THE WILBERFORCE SOCIETY

Cyber-wars: Russian disinformation and the war in Ukraine: emboldening freedom of the press in an era of digital revolution

Editor:

Mihaela Revencu

Writers:

Anne Levai, Ben Brent, Edward Barlow, Matthew Christie, Teodor Grama

Abstract

The conflict in Ukraine, which began in 2014, escalated significantly on 24 February 2022 with Ukraine now fully engaged in a war against Russia. The war has seen an increase in censorship and media disinformation as Russia attempts to shape the narrative of the invasion, both domestically and abroad. This paper analyses how Russia has attempted to achieve this aim, and how other authoritarian states have followed Russia's example. After analysing the censorship and disinformation attempts made by authoritarian states like Russia, China and Iran, this paper proposes policies to mitigate the spread of misinformation and limit the opportunities for state leaders to control their citizens' access to (accurate) information.

Executive Summary

This policy paper focuses on the increasing use of media disinformation and censorship across the world and analyses the view that there is an ambition of authoritarian states to control global information production and distribution. This argument is investigated in the current Russia and Ukraine war, as well as the ongoing Iranian and Chinese state involvement in domestic and foreign media. To portray this message the policy paper is structured in three sections: Russia and Ukraine War; Other Authoritarian Regimes and Policy Proposal, each of these will further cover domestic and foreign disinformation and censorship attempts made by the state.

Section 1: Russia and Ukraine War

Section I of this paper situates the questions of censorship and disinformation within the context of the Russo-Ukrainian war from the Russian Federation's 2014 annexation of Crimea onwards. By means of both theoretical and case study-centric approaches, it explores the processes behind Russian censorship and disinformation both at home and abroad. It prepares the ground for the following consideration of other authoritarian regimes, as well as policy suggestions focused on countering the impacts of state-sponsored censorship and disinformation.

Section 2: Other Authoritarian States

Section II employs a comparative approach between China, Iran and Russia to assess whether current developments constitute a global aspiration for information control. It will argue that irrespective of its ubiquity across authoritarian states and their use of similar policies and techniques, these have not arisen in uniformity or coherence. Instead, each state has developed programmes in reflection of their own self-interest, itself shaped by distinctive contexts. Differentiating between domestic and foreign policies it will highlight how, through a multi-pronged approach, the use of censorship and disinformation have conspired to achieve control. A secondary phenomenon that can be observed through this foundational dominance is the establishment and exacerbation of epistemological insecurity. In the international sphere, these techniques have aided geopolitical ambitions.

Section 3: Policy Proposal

Section III of this policy brief explores existing and potential policy responses to state-sponsored disinformation and emerging digital authoritarianism. A review of the existing policy frameworks reveals that approaches centred around multi-stakeholder engagement, targeted export controls and increased

political pressure on social media platforms have gone some way towards addressing the threats identified in the other two sections. Our policy recommendations suggest that current policy approaches should be built upon rather than scrapped. Governments should seek to play a more active role in incentivising social media platforms to adequately report on and respond to disinformation operations, whilst also expanding their own efforts in the field. Consolidating existing multilateral fora that seek to play a central role in promoting digital freedom should also represent a priority. Lastly, high-tech export controls and an increased emphasis on corporate due diligence are likely to prove effective tools in undermining mass surveillance under authoritarian regimes and weak democracies.

Contents

Introduction

The brief as a whole aims to describe the existence of censorship and disinformation in numerous states, seeking to emphasise the policies needed to resolve such issues. To better understand censorship this paper defines it as a "system in which an authority limits the ideas that people are allowed to express" and "prevents books, films, works of art, documents or other kinds of communication from being seen or made available to the public"; [1]mostly because they include or support certain ideas that the governing authority disagrees with. Even further, disinformation has been defined as non-accidentally misleading information and even if it has a limited impact on the creation of false beliefs, it will still be deemed disinformation as long as it has the potential to cause *false* views.[2]

[1] Cambridge University Press & Assessment 2024. Censorship | English meaning. Cambridge Dictionary.

[2] Fallis, D. (2015). What is Disinformation? Library Trends, 63(3), 401-426

1. Russian Disinformation and the Conflict in Ukraine

1.1 Domestic censorship and disinformation within Russia

Within Russia's internal structures, institutions, and wider society, the use of censorship and disinformation plays a vital role in maintaining the status quo of Putin's authoritarian regime. Censorship ensures that only specific narratives are discussed within the public sphere. Whereas previously censorship was directed at independent (that is, non-state-aligned) organisations and independent media outlets, since the February 2022 invasion of Ukraine it has increasingly applied to individuals, too. By silencing dissenting voices, censorship serves to preserve the narratives which are created through the strategic use of disinformation by state actors.

Broadly, the centrality of disinformation is reflected in the Russian government's insistence that the invasion of Ukraine is not a war but rather a special military operation. More specifically, though, it appears that Russia has enacted three 'narrative frames' of disinformation in relation to the war, which will be examined further in this brief. Firstly, much focus exists on the Russo-Ukrainian war as an existential threat to Russia's existence, secondly, the war is presented as 'liberating' and thirdly actions are imposed to downplay Russia's actions abroad. Censorship helps to preserve the existing conditions set by disinformation. A further crucial narrative has been made to create the impression that the attack on Ukraine is legally legitimate as Russia responded to NATO's alleged violation of the 1990 Treaty, possibly visible in its talks with Ukraine. Through the dissemination of confusion and false information, such narratives have had certain degrees of support since February until now. This section first examines the modus operandi of domestic censorship, before outlining some of the key disinformation narratives that it aims to maintain. Then, it further presents the case of foreign censorship and disinformation.

1.1.1 Domestic censorship

Legally, censorship in the Russian Federation is prohibited under Article 29 of the Constitution. The same article also guarantees freedom of the press.[3] The reality is very different, however. While censorship has long been a central element of managing the Russian political space, a severe clampdown on dissenting and opposition voices has taken place following Russia's invasion of Ukraine in 2022. This section outlines the conceptualisation of censorship practices in contemporary Russia. It then briefly traces domestic censorship since the start of the conflict in 2014; having done so, it then turns to focus on the mechanisms through which it has been exercised post-February 2022.

[3] Kovalev, A. (2021). 'The political economics of news making in Russian media: Ownership, clickbait and censorship'

There are three 'avenues' through which domestic censorship in Russia is enacted: directly; indirectly; and voluntarily (self-censorship). 'Direct' censorship refers to the practice of material being deliberately and explicitly censored due to demands from political or business 'higher-ups'. In this way, informal rules are written from the top of the hierarchal structures of authority limiting the freedom of independent journalists to write about the truth. Secondly, 'indirect' censorship occurs when media outlets are pushed out of the media market through the Kremlin's market dominance.[4] Finally, 'self-censorship' involves individuals choosing to censor what they say in order to comply with unspoken or unofficial 'rules' about what can, and cannot, be said. This form of censorship is also known as *adekvatnost*' (literally, 'adequacy'; knowing 'what is enough').[5] While the literature on such a conceptualisation of censorship indeed predates the Russian invasion of Ukraine, the next paragraphs trace the use of censorship; in so doing, it becomes apparent that while the focus may have moved more strongly onto direct censorship, the overarching framework remains incredibly similar.

Prior to February 2022, the majority of, albeit not all, censorship took place indirectly and in the form of self-censorship. A prime example of the former is the infamous 'foreign agents' law which was originally passed in 2012 targeting non-profit organisations[6] before later being amended in 2017 to cover media outlets too.[7] Having to declare their status before any broadcasted material made media production more costly, and the need to declare full details of their finances limited opportunities for funding. Rules were also applied more harshly to independent media outlets that did not always align with the Kremlin's take on events: in 2018, the radio station *Ekho Moskvy* was fined 20,000 rubles for content which, while linked to on a blog hosted on the station's website, bore no official connection to it.[8] Censorship on a personal level was further visible: a lack of culture in Russia of speaking out and journalists' fears of unexpected circumstances led to *adekvatnost'* being considered 'a virtue and expression of professionalism'.[9] Be that as it may, the presence of independent news outlets and journalists was still important, though, for it gave the (now no longer) impression of press freedom.[10]

Since the invasion, the intensification of censorship has been increasingly prominent through the 'direct' channel, as well as through self-censorship. As the Kremlin cracks down on press freedom, previously implicit threats have become explicit. On the 26th of February, less than a week following the invasion of Ukraine, Roskomnadzor (the federal executive body 'responsible for overseeing the media',[11]

[4] Kovalev, A. (2021).
[5] Schimpfossl, E., & Yablokov, I. (2014). 'Coercion or conformism? Censorship and self-censorship among Russian media personalities and reporters in the 2010s.'
[6] 'Российские НКО не хотят быть 'иностранными агентами'. (2012, November 21). *BBC News Русская Служба*.
[7] Mischke, J. (2017, November 10). 'Russia to amend law to classify media as 'foreign agents'. POLITICO.
[8] 'Echo of Moscow fined for linked content in blog on its website'. (2018, April 27). Reporters Without Borders.
[9] Schimpfossl, E., & Yablokov, I. (2014), pp. 304-310.
[10] Kovalev, A. (2021), p. 2907.
[11] *Federal Service for Supervision of Communications, Information Technology and Mass Media.* Government of the Russian Federation.

unofficially known as the 'ministry of censorship'[12]) ordered a number of media outlets to delete the words "war" and "invasion" from their coverage.[13] The criminal code was later amended in March 2022 to make it illegal to spread 'false information' about the Russian army with regards to not solely the war in Ukraine, but rather any of its actions.[14] The punishment for 'discrediting' the Russian army: from a fine of up to 1.5 million rubles, to 15 years of prison time.[15] In March alone already the authorities initiated criminal proceedings against 9 journalists under the offence that they were "disseminating false information about the Russian Armed Forces" [16] (Article 207.3 of the Criminal Code) .

Such explicit, yet arbitrary, limitations on what can and cannot be said have led to both individuals and organisations keeping quiet more than ever before. With war reporting codified as illegal, the foreign news agencies Bloomberg and CNN pulled out of Russia almost immediately. As the main editor of Bloomberg, John Micklethwait put it, the changes designed to 'turn any independent reporter into a criminal' made reporting all but impossible.[17] Some news agencies have increasingly exercised self-censorship. Those that did not, however, have paid the price. Due to its supposed 'failure' to recognise two non-profit organisations as 'foreign agents' earlier on in the year, *Novaya Gazeta*'s license to act as a mass media outlet was withdrawn in September 2022 at the request of the Supreme Court of the Russian Federation.[18]

Direct censorship has also been targeted at individuals through invalid imprisonment and long periods of solitary detentions. The opposition politician Ilya Yashin was initially detained in July 2022 for 15 days for having disobeyed a police officer. Yet, just as he was supposed to be released from prison, he was hit with further charges of knowingly spreading 'fake information', based on a video he posted on YouTube speaking out about the Bucha massacre.[19] His detention was extended until September 2022; in December of the same year, he was officially sentenced to eight and a half years in jail for his actions.[20]

To summarise the above, domestic censorship within the Russian Federation is not a new phenomenon. In spite of its increase following the invasion of Ukraine in 2022, the avenues through which it is exercised have largely continued to exist in the same forms: direct, indirect, and self-censorship. Yet, its

[12] Kovalev, A. (2021), pp. 2911-2912.
[13] 'Do not call Ukraine invasion a 'war', Russia tells media, schools'. (2022, March 2). *Al Jazeera*.
[14] 'Russia Criminalizes Independent War Reporting, Anti-War Protests'. (2022, March 7). *Human Rights Watch*.
[15] 'Путин подписал закон о больших сроках за публикацию альтернативного мнения про военных РФ'. (2022, March 5). *Roskomsvoboda*.
[16] 'Russian Journalists Are Being Silenced to Stifle Reporting of Protests', Amnesty International, 24 November 2022, https://www.amnesty.org/en/latest/news/2022/11/russia-journalists-and-independent-monitors-beingsilenced-to-stifle-reporting-of-protests-new-report/
[17] 'Bloomberg и CNN приостанавливают работу в России'. (2022, March 5). *Mediazona*.
[18] 'Верховный суд прекратил деятельность сайта «Новой газеты» в качестве СМИ'. (2022, September 15). *Roskomsvoboda*.
[19] 'Russian opposition politician kept in prison under 'fake information' investigation'. (2022, July 13). *Reuters*.
[20] 'Russia: Opposition politician Ilya Yashin sentenced to eight and half years in jail for denouncing Russia's war crimes in Ukraine'. (2022, December 9). *Amnesty International*.

focus and efforts have changed. While still heavily reliant on self-censorship like before, an even greater emphasis has been placed on direct censorship through state institutions. As the boundaries of what can, and cannot, be expressed have become increasingly clear, so have the punishments for breaking these norms and by now laws.

1.1.2 Domestic disinformation

Since the start of the conflict in 2014, domestic disinformation within Russia has historically served two purposes. 'Defensive' disinformation aims to defend Russian domestic sentiment and status quo from external threats; the objective of 'offensive' disinformation, on the other hand, is to undermine the legitimacy of other states[21]. However, the line between these two types of disinformation has become blurred: given the offensive nature of Russia's invasion of Eastern Ukraine in February 2022, the ensuing ramping up of domestic disinformation has needed to simultaneously 'defend' and 'offend'[22]**.** Over the last year especially, disinformation has been used to create confusion and present issues in a biased, and factually incorrect, manner. Its ultimate aim is to push the Kremlin's desired narrative and maintain (or build) the regime's public support[23].

Russian disinformation operates through a series of 'frames'. Regardless of how disinformation is disseminated, be it through (social) media or official political communications, it is purposely distorted to fit into one (or more) of the narratives that have been created by the Kremlin. The most common narratives around which disinformation is organised include undermining the political sovereignty of other nation-states, as well as presenting Russia as an 'innocent victim'. In the context of the Russia-Ukraine war, this section highlights the salience of three frames in particular: portraying the war as necessary for Russia's existence; depicting it as a war of 'liberation' which is supported by Ukrainians; and 'ввв8' the Russian military's actions. Through each of these, the workings of domestic disinformation become clear.

Firstly, Russian disinformation narratives frame the state's very existence on the war with Ukraine. In doing so, they play on the nation's cultural memory of the collapse of the USSR in an attempt to increase support for the war. In his Address to the Federal Assembly on 21st February 2023, President Putin portrays the war as an existential threat to Russia. He does this both explicitly and implicitly, claiming

[21] Baranovsky-Dewey, (2019), "Determinants of the Timing and Intensity of Propaganda Attacks", *St Antony"s Review*, vol.14, issue.2, p.120

[22] Diepeveen, S., Borodyna, O., & Tindall, T. (2022, March 11). *A war on many fronts: Disinformation around the Russia-Ukraine war*. ODI. https://odi.org/en/insights/a-war-on-many-fronts-disinformation-around-the-russia-ukraine-war/ (Accessed 12 January 2023)

[23] Bodrunova, S. S. (2021). Information disorder practices in/by contemporary Russia. In H. Tumber & S. Waisbord (Eds.), *The Routledge Companion to Media Disinformation and Populism* (pp. 279–289). Routledge. Pp. 280

that the ultimate (and unhidden) goal of Western elites is the strategic destruction of Russia. As a result, there is a greater outside threat for all Russians, in greater amounts bringing in social cohesion- "the matter in question is the existence of our country"[24].

Even further, as has been a common feature of post-2022 Russian disinformation and propaganda, Putin draws on religious parallels to make his point[25]. He refers to Western priests who are "forced to bless same-sex marriages" as well as "the destruction of the family, [and] cultural and national identity" to present a dangerous threat which goes as far as paedophilia: one from which children need to be "saved". Such framings based around 'destruction' and 'existence' are powerful in Russia, potentially because they hark back to the chaos of the 1990s: a period during which Russia saw what had, in practice, been the world's largest 'great' empire replaced with economic and political uncertainty[26]. This form of manipulation and influence from the Kremlin on society is a clear example of disinformation,

Domestic propaganda also frames the war as 'liberating'. According to this line of argument, the war serves to 'liberate' the Ukrainian nation from the corrupt, Western-led 'regime' in Kyiv [27]. In June 2022, the Russian government exploited a video of a Ukrainian woman, Anna Ivanova, which later went viral and resulted in her being known as "Babushka Z". The video supposedly shows Ivanova valiantly resisting the arrival of Ukrainian soldiers by waving a USSR flag, which a soldier subsequently stamps on. She then rejects assistance from the soldier, retorting that her grandparents died for the flag[28]. Despite Ivanova being opposed to the Russian invasion, the Kremlin used the footage to its advantage greatly. It aligned near-perfectly with the narrative frame that Russia's 'Special Military Operation' was being well-received by Ukrainians who, regretting the collapse of the USSR, were grateful for Russia 'saving' them. Within days, "Babushka Z" appeared all over state media as well as social media; a statue of her was even erected in the captured city of Mariupol. Despite pro-Kremlin disinformation's attempts to present Ukrainians as grateful for the invasion, the reality is still that 97% of Ukrainians see the invasion as a threat to their country's security, and over 7 million refugees had already fled into Europe within the war's first two months [29].

Finally, disinformation aims to downplay Russia's role in the war. It argues that Russia is only acting as far as is necessary; accuses other actors of wrongdoing; and denies evidence suggesting it has committed

[24] Scarr, F., & Ahmedzade, T. (2023, April 7). The talk-show hosts telling Russians what to believe. BBC. https://www.bbc.co.uk/news/resources/idt-4af5a2e0-10d4-4d4f-b3bb-41e2d1fe35dd
[25] Ibdem.
[26] Petrov, N., Lipman, M., & Hale, H. E. (2014). Three dilemmas of hybrid regime governance: Russia from Putin to Putin. Post-Soviet Affairs, 30(1), pp. 24.
[27] olianska, A. (2022, September 2). A History of Defamation: Key Russian Narratives on Ukrainian Sovereignty. EUvsDisinfo. https://euvsdisinfo.eu/a-history-of-defamation-key-russian-narratives-on-ukrainian-sovereignty-2/
[28] Bettiza, S., & Khomenko, S. (2022, June 15). Babushka Z: The woman who became a Russian propaganda icon. *BBC.* https://www.bbc.co.uk/news/world-europe-61757667
[29] Diepeveen, S., Borodyna, O., & Tindall, T. (2022, March 11). *A war on many fronts: Disinformation around the Russia-Ukraine war*. ODI. https://odi.org/en/insights/a-war-on-many-fronts-disinformation-around-the-russia-ukraine-war/ (Accessed 12 January 2023)

war crimes. On an episode of the NTV talk show 'Your Own Truth' entitled 'Rabid Russophobia', the State Duma member Boris Chernyshov made claims that the Ukrainian population is ultimately responsible for the war, for it could stop it if "normal people" finally took to the streets to put an end to Zelensky's "Nazist regime". Chernyshov later speaks of the nature of war: for him, war should be waged according to the rules. However, the "criminals time and again cross these red lines".[30] Such framing implies that Russia is not the enemy. Not only is Russia apparently following the rules of war, but it is supposedly the only side to be doing so. Of course, such claims are in stark contrast to the realities of the war. Responsibility for the Bucha massacre in April 2022 was widely denied across both state-run and social media outlets. In reality, testimony of the killings suggests that they "may amount to the war crime of wilful killing, a grave breach of the Geneva Conventions"[31].

To summarise, domestic disinformation during the Russia-Ukraine war has served the simultaneous functions of 'offending' and 'defending'. It undermines other states and their actions, while also 'defending' against evidence-backed accusations made against Russia. The deliberate use of narrative frames culminates in a certain domestic presentation of the war, according to which it is a morally justified and existentially necessary act of 'liberation'.

1.2 Russian disinformation efforts abroad

1.2.1 Why Disinformation?

Russian disinformation efforts must be understood in the context of a deep-seated concern over the loss of status following the end of the Cold War and the ascent of Putin in the late 1990s. The state's core strategic objective of regaining great-power status came to be seen as a civilisational struggle which necessarily would be pursued in the informational space. Russian strategists believed that regaining great-power status was endangered by alleged Western informational subversion of Russia and other post-Soviet republics. The consequent understanding of informational subversion being a prerequisite for geostrategic security developed alongside a strategic culture of aggressive pre-emption entrenched by the rise of the siloviki is explained further below. The result of this was an understanding that competition with the West must be informational, concerned with political-cultural values and use pre-emptive tools such as disinformation.

[30] Своя правда. Выпуск от 18.11.2022. ОГОЛТЕЛАЯ РУСОФОБИЯ. (2022, November 18). https://www.youtube.com/watch?v=BJJBT_NUorg

[31] "Protect, Respect and Remedy" Framework" <https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf> accessed 12 November 2022

The concern with great-power status and antagonism to the West stood in a tense juxtaposition with an acute awareness of economic and military-industrial vulnerability. The 1998 economic crisis led the 2000 National Security Concept (NSC) to assert that 'Russia's national interests may be only assured on the basis of sustainable economic development'[32]. The 2000 NSC defined economic recovery as the most pressing short-term goal and recognised the necessity of economic integration for the purpose of modernisation.[33] The 2000 NSC also drew attention to the continued importance of military strength (conditional on economic vitality) and the need to seize the 'new opportunities for ensuring its security' [34]. The need for integration to strengthen the Russian economy had to be squared with an increasingly nationalist-revisionist domestic climate post-1995. This tension between integration and revisionism was explicitly articulated in the 2000 NSC, which identified 'two mutually exclusive trends' between the need to integrate into the global economy to improve Russia's standing and the need to revise the "international relations structure based on domination by developed Western countries"[35].

The consequence of this insoluble tension was an attempt to redefine the terms on which the socially constructed character of status was defined. Claims to status are embedded in a framework of socially constituted international structures. Thus, authority can only occur within the parameters of a collectively accepted international architecture and to become authoritative 'actors must pass intersubjective legitimacy tests that demonstrate their eligibility and ability to enact the new status given to them'[36]. Russia could not meet revisionist and nationalist demands at home and, at the same time, pass these intersubjective legitimacy tests within the Liberal International Order that would facilitate integration. It is from this position that Russian strategists embarked on a method of what Clunan describes as 'aspirational constructivism' articulating a desire to redefine 'Russia's Eurasian identity' as 'positive and superior to that of the West' [37] to revise the international order away from Western status criteria.

As a result, political-cultural distinctiveness became regarded as the basis of Russian strength because it acted as the axiom of an alternative status criteria which facilitated the revisionism central to addressing status concerns. This can be seen in the 2000 Foreign Policy Concept published under Putin which articulated this strategy of pragmatic competition and social creativity. Putin's understanding of Russian status 'rested squarely on what he termed "belief in Russian greatness"'[38]. Political-cultural

[32] Office of the President of the Russian Federation, Decree of the President of the Russian Federation of no.24, (2000), Article 2
[33] Idem.,
[34] Idem.,
[35] Office of the President of the Russian Federation, Decree of the President of the Russian Federation of no.24, (2000), Article 1
[36] Anne Clunan, 'Why Status Matters in World Politics', in Thazha Paul, Deborah Larson, William Wohlforth (eds), *Status in World Politics*, (Cambridge: Cambridge University Press, 2014), p.276
[37] Anne Clunan, 'Historical Aspirations and the Domestic Politics of Russia's Pursuit of International Status', *Communist and Post-Communist Studies*, vol.47, (2014), p.284
[38] Clunan, 'Historical Aspirations and the Domestic Politics of Russia's Pursuit of International Status', p.287

distinctiveness came to be understood as the basis of Russian status, and as such distinctiveness needed to be guarded from the hegemonic ideology of the US-led order. Status, under conditions of contradictory domestic and international demand,s could only be achieved through ensuring the sovereignty of a distinct political-cultural identity. Such understanding emphasises that status and sovereignty were, therefore, mutually constitutive for much of the Russian political elite.

To recognise the reason for Russia's turn towards disinformation it is important to analyse the colour revolutions of the 2000s.[39] These revolutions, which were seen by many in the West as 'the result of individuals living under oppression standing up for their political rights'[40] across former Soviet states – were viewed very differently from the Kremlin. They were seen as the product of Western *information warfare* targeting core civilisational tenets. It was this perceived shift into an informational field of conflict which stimulated the Russian grand strategy to take on a character not just opposed to integration into the US-led order, but intent on insulating Russian civilisation from exogenous political influence. The colour revolutions across Ukraine, Georgia and Kyrgyzstan were understood as embodying the blueprint for Western subversion of this traditional Russian spiritual-moral through informational channels dubbed by some researchers a "geo-informational threat"[41]. The fear of this has subsequently occupied a prominent role in the formulation of Russian grand strategy.

The Chief of the General Staff, Gerasimov (making him the most senior military officer in Russia), at the 2014 Moscow Conference on International Security, articulated this belief. He asserted that "colour revolutions are becoming the main means of [Western countries] achieving [their] political ambitions"[42] Moscow, therefore, views itself as the victim of Western information warfare, suspecting any use "of political, economic, informational, humanitarian and other non-military measures"[43] by Western actors to be subversive informationally-driven efforts aimed at undermining Russian civilisation. Many Russian policymakers subsequently came to regard Russia as being engaged in a "counter-struggle"[44], setting Russian civilisational values against the penetration of liberal ideology that would undermine political-cultural attributes and instigate instability. The Russian dictionary of informational-psychological operations refers to 'information confrontation'. This is defined as "rivalry between social systems in the information sphere"[45]. The dictionary specifies that informational-psychological confrontation may take any form of social and political competition, reflecting a belief that Western

[39] The 'colour revolutions' refer to a series of protest movements and changes in government in Belarus, Georgia, Ukraine and Kyrgyzstan throughout the early 2000s.
[40] Ben Sohl, 'Discolored Revolutions: Information Warfare in Russia's Grand Strategy', *The Washington Quarterly*, vol.45, issue.1, (2022), p.99
[41] Katri Pynnöniemi, 'Information-Psychological Warfare in Russian Security Strategy', in Roger Kanet (eds), *Routledge Handbook of Russian Security*, (Abingdon: Routledge, 2021), p.221
[42] Sohl, 'Discolored Revolutions: Information Warfare in Russia's Grand Strategy', p.99
[43] Valery Gerasimov, 'The Value of Science in Foresight', *Military Review*, (2016), p.24
[44] The term 'Protivoborstvovat'.
[45] Pynnöniemi, 'Information-Psychological Warfare in Russian Security Strategy', p.216

states' alleged use of informational subversion is perpetual and all-encompassing – that every facet of life is vulnerable to an attempt at subversion.

The impact of 'information confrontation' on Russian grand strategy is also connected to regime preservation. Colour revolutions give rise to the fear of a fifth column being artificially injected to usurp an incumbent elite - unsurprisingly an especially acute anxiety amongst Russia's political elite. This can be seen in Shchelin's comparison of the 2009 and 2015 US National Security Strategy (NSS). The 2009 Strategy sets out the ambition of transforming Russia into "one of the leading powers judging by the level of technological progress, quality of life …and influence on global processes"[46] In contrast, the 2015 NSS has "no clear image of any future goals"[47] focusing instead on the internal political stability, reflecting an awareness of the potential of popular movements to topple the government, as was the case in Serbia and Ukraine. One might, therefore, argue that while political stability is described as primarily under threat from Western injections of a fifth column, the strategic attitude to colour revolutions must be understood as a nexus of domestic and foreign policy concerns. One might, therefore, argue that while political stability is described as primarily under threat from Western injections of a fifth column, the strategic attitude to colour revolutions must be understood as a nexus of domestic and foreign policy concerns.

An important intersecting factor in explaining why Russia uses disinformation can be found in the rise of the siloviki. The term 'siloviki' derives from 'silovye struktury' which translates as 'force wielding'. It refers to structures such as the military, security services, intelligence agencies and other members of Russia's security establishment[48]. Regardless of specific institutional affiliation, "all siloviki have in common a special type of training that sets them apart from civilians"[49] and harbour an acute hawkishness. Since the turn of the last century the siloviki have occupied an increasingly prominent role in policymaking, and their unique strategic culture has had a profound impact on how Russian grand strategy assesses and responds to threat. Felgenhauer believes that the siloviki "seem to be in the process of taking over Russia's domestic and foreign policy decision-making completely"[50].

The rise of the siloviki has informed the policymaking process but was also connected to the entrenchment of a particular strategic culture. Covington lays out the central principles of Russian strategic culture. The most important of which is the underlying assumption of *uniqueness* – that Russia's geographic, political, economic and strategic position gives rise to "unique vulnerabilities [which produce] a strategically unique approach to defence that Russians sometimes refer to as an asymmetric

[46] Office of the President of the Russian Federation, 'National Security Strategy of the Russian Federation until 2020', Article 24
[47] Pavel Shchelin, Russian National Security Strategy: Regime Security and Elite's Struggle for 'Great Power' Status, *Slovo*, vol.28, issue.2, (2016), p.87
[48] Peter Rutland, 'The Political Elite in Post-Soviet Russia', in Heinrich Best and John Higley (eds), *The Palgrave Handbook of Political Elites,* (Basingstoke, Palgrave Macmillan, 2017)
[49] Andrei Illiarionov, 'Reading Russia: The Siloviki in Charge', *Journal of Democracy*, vol.20, issue.2, (2009), p.69
[50] Anderson, 'The Chekist Takeover of the Russian State', *International Journal of Intelligence and* Counterintelligence, p.239

approach"[51]. Within this understanding of uniqueness is an awareness of geostrategic and technological *vulnerability* in addition to a susceptibility to surprise that contributes toward an anxiety as to whether Russia is truly defendable. The belief in Russia's strategic uniqueness motivates the military to seek opportunistic deployment of force while simultaneously acknowledging Russia to be strategically vulnerable and susceptible to surprise. Leading to an approach designed to "minimise vulnerability to anticipated surprise by maximising the counter-surprise power of Russian military actions"[52].

In sum, the preponderance of the siloviki in Russia's foreign policy and security establishments has not just entrenched a particularly hawkish and revanchist attitude, it has also privileged a strategic culture of aggressive, pre-emptive action. In the context of information confrontation, Russia's strategic culture has instigated a disposition towards not just strategic paranoia, but also the use of methods that pre-emptively seek to counter-surprise Western states utilising informational tools precisely because that is how they believe the West seeks to destabilise Russia. The frame of the contest, therefore, *must* be informational. Further, because of the character of the perceived Western threat and the tendency towards pre-emptive aggression embedded in Russian strategic culture, informational contests must use disinformation to damage the confidence of target populations in their core political and cultural institutions.

1.2.2 The Content of Disinformation

Having explained why Russia uses disinformation it becomes clear what narratives must be used in order to achieve this central strategic goal of informational reflexive control over its adversaries. To achieve the reflexive control necessitated by its strategic outlook Russia must effectively destabilise and disorient target populations to stymie the effective political discourse that might impede Russian revisionism. To demonstrate how destabilisation and disorientation may occur one should look to English-language examples of how Russia has undertaken disinformation outside of Ukraine.

The narratives deployed in Russian disinformation present to Western audiences a vision of their political systems as irreparably broken, their societies as rootless (i.e., lacking the distinct civilisational identity so valued by the Kremlin) and from this in need of sudden, radical change. Much of the existing scholarship draws on how in English-language Russian media outlets, such as Russia Today (RT) or Sputnik the West is cast as inherently dysfunctional and disordered. In Ramsey and Robertshaw's study of 952 articles about UK domestic issues across 11th May-7th June 2017 and 4th-31st March 2018, 1,361

[51] Covington, 'The Culture of Strategic Thought Behind Russia's Modern Approaches to Warfare', p.7
[52] Covington, 'The Culture of Strategic Thought Behind Russia's Modern Approaches to Warfare', p.14

instances of frames relating to political dysfunction were found[53]. Within this category, reports of conflict between ethnic, religious or social groups, including tensions related to immigration were most common[54]. Assertions of chronic instability and a loss of social cohesion resulting from inter-group tensions were furthered by the persistent conflation of immigration, Islamic fundamentalism and terrorism. Ramsey and Robertshaw found that discussions of migration as a breeding ground for Islamic radicalism that destabilises Europe must be linked to the overarching narrative of Europe as a place of chaos.

Critical framing of NATO as aggressive, illegitimate or incompetent appeared in 280 of the sampled articles (45% of the total). These frames depicted the alliance as having aggressively encroached upon Russia's sphere of influence and unnecessarily threatened its security. A Sputnik article following the NATO summit in 2017 entitled "Russia Has Little Reason to Trust NATO After It Absorbed Whole of Eastern Europe"[37]. Similarly, numerous articles have been published by RT, accessible to Russians and Ukrainians in the region, encouraging Ukraine not to join NATO on these grounds. One article describes Ukraine's bid to join as a "pipe dream" with the efforts contributing towards NATO's "steady expansion to the East", the conclusion being that Russia "reserves the right to protect Russia's national security"[38]. As mentioned in the first section, this rhetoric continues to be a justification for the invasion of Ukraine. The presentation of NATO as expansionist works alongside its presentation as duplicitous and engaging in illegal action. Equally, RT has claimed that the accession of Montenegro to NATO was carried out against the people's will. It was described as "the finalizing of one big, undemocratic process"[39]. Framing the alliance as being aggressive and expansionist serves to undermine readers' faith in NATO being a defensive organisation, replacing it with an image of an imperialist bloc that is a far less attractive option. In doing so the intention is not to spur exits of the organisation, but rather to weaken support for unified action when Russia interferes on its borders. Thus, through Russian disinformation, it hopes to weaken support within target countries' populations for institutions such as NATO that seek to contain Russian ambitions.

In portraying NATO membership as unattractive (and at worst illegitimate) to those outside of the alliance and a US-dominated system seeking to vassalize the smaller members, Russian disinformation seeks to discredit its sole geostrategic competitor. In doing so, weakening the internal coherence of the alliance and the legitimacy of its actions.

The portrayal of Western dysfunction not only serves to disguise Russian vulnerabilities not dissimilar to those it attributes to the West but is accompanied by the projection of Russian strength. Russian outlets, such as RT and Sputnik, frequently publish English-language articles that amount to little more

[53] Gordon Ramsey and Sam Robertshaw, 'Weaponising News, RT, Sputnik and targeted disinformation', *King's College London Centre for the Study of Media, Communication & Power*, (2018), p.73
[54] Ramsey and Robertshaw, 'Weaponising News, RT, Sputnik and targeted disinformation', p.73

than fact-files of Russian military specifications laced with fearmongering. Sputnik publishes numerous articles given over to 'detailed specification of military hardware',[55] listing details of weapons, carefully explaining their specifications and capabilities. The material is clearly designed to provide an eye-catching, easily accessible impression of the alleged potency of the Russian military. These planted articles often find their way into British outlets having received remarkably little editing. For example, one article published by *The Daily Express* on 30th May 2017 entitled 'Preparing for WAR? Russia to upgrade rocket artillery by 2020 as tensions with NATO rise' featured extensive weapons specifications[56]. The very wording of the article was close to a verbatim reproduction of the Sputnik original. Hence, this reality suggests the integration of disinformation tools in Russia's foreign affairs efforts.

These narratives, persistently maligning the viability of open societies, are intended to demoralise target populations, and thereby instigate political instability in the West. To undermine or paralyse the political systems of target states benefits Russian revisionism: that is to say, the more tangible efforts by Russia to revise the international order may be expected to meet with less resistance if states that would likely oppose their actions cannot function domestically. Thus, Russian disinformation attempts to achieve the informational reflexive control that is necessitated by its grand strategy as well as maligning the Western political model.

Russian disinformation campaigns in other Western states provide a model to understand how it may be effectively countered in Ukraine. In seeking to inject artificial discord into Ukraine, as was particularly notable following the 2014 Maidan protests, Russia has sought to drive Ukraine and other states to the point of collapse from the inside out by either exacerbating existing divisions or generating novel cleavages. The Kremlin's attempts to do so hinge on its ability to disseminate narratives that erode confidence either in the state itself or in democratic values. It is for this reason that Ukraine must make further attempts to reinforce the political culture of democratic values and prevent Russian disinformation that seeks to portray democratic values as inherently dysfunctional.

1.2.3 How Disinformation is Disseminated

Turning our minds to Russian disinformation efforts in Ukraine, it becomes clear that Russia identified and exploited vulnerabilities both informational and civic to spread anti-Western disinformation. One might argue that Ukraine was "a nearly perfect target that was unprepared to formulate a coherent

[55] Idem, pp. 67
[56] Idem, pp. 60

information strategy and quickly lost the information war with Russia"[57]. Baranovsky-Dewey highlights the polarised/contentious political environment as increasing the likelihood of an information intervention by another state. She argues that a polarised domestic environment leads to gridlock in government, and leaves the electorate sceptical of the government's capacity to govern. From this they become sceptical of not just the government, but institutions more broadly; such as the press. When citizens "do not trust the media they consume to cover news fairly, this increases their demand for marginal, less known, or less established sources"[58], which presents a hospitable environment for disinformation. The effects of disinformation were compounded by the sluggish pace with which Ukraine in 2014 was able to mobilise its public relations resources. In comparison, following the 2008 invasion of Georgia, Tbilisi "approached foreign firms for help in crafting a global image"[59]. Ukraine, on the other hand, lacked an international voice or identity and thus was a target less capable of resisting the information onslaught.

Attempts to destabilise the Ukrainian informational environment were also revealed in the Surkov leaks. These were leaks of three tranches of emails belonging to Kremlin official and Putin's close advisor Vladislav Surkov. To further infiltrate the Ukrainian informational space Russia successfully took-over media outlets. In one email Pavlo Broyde, a PR expert from the Eastern Ukrainian city of Zaporizhzhia, contacted Surkov identifying Ukrainian Media Holding (UMH) as the most promising media company for achieving "an informational pro-Russian breakthrough in the Ukrainian media space"[60]. Broyde classified the UMH outlets as "moderate re-translators of anti-Russian messages". The aim was not to have UMH directly spoon-feed the messaging of the Russian Ministry of Foreign Affairs per se, but to reorient their output so that it promoted Russian interests in Ukraine. Further emails revealed that the Kremlin also considered gaining control over the Odesa media outlets Timer and STV. In November 2014, Surkov's deputy Ardzinba received an analysis of the two outlets" potential as conduits of Kremlin messaging and of the risks of involvement.

This allowed Russia to persistently undermine Western influence amongst Ukrainians. Similar to the above narratives on the disadvantages of joining NATO, and reflective of the expansion of Western institutions, the Russian Ministry of Foreign Affairs has consistently pushed the narrative that "We again see that the United States … are in fact attempting to impose a "Western vector" on their development dictating to the authorities of a sovereign country what they should do"[61]. This notion of exterior control

[57] Baranovsky-Dewey, (2019), "Determinants of the Timing and Intensity of Propaganda Attacks", *St Antony's Review*, vol.14, issue.2, p.121
[58] Ibid, p.127
[59] Ibid, p.129
[60] Shandra and Seely, (2019), "The Surkov Leaks, The Inner Workings of Russia"s Hybrid War in Ukraine", *RUSI*, p.17
[61] Boyte, (2017), "An Analysis of the Social-Media Technology, Tactics, and Narratives Used to Control Perception in the Propaganda War Over Ukraine", *Journal of Informational Warfare*, vol.16, issue.1, p.95

was furthered by the assertion that far-right groups within the country are NATO puppets and that Russian involvement has been an attempt at both "de-Nazification" and to dislodge Western influence.

The efforts to subvert Ukrainian sovereignty were not limited to the informational space, they also too advantage of civic weakness. On 10th July 2014, Surkov was emailed proposals by Broyde, about how the organised "racket" created by President Yanukovych's Party of Regions might be used to Russia's advantage. Under Yanukovych, those state and regional organs responsible for monitoring political processes including the "secret services, parts of local government, police and local political parties, which had already fallen under the de facto control of business groups and clans after Ukrainian independence – were corralled further into "shadow verticals of power"[62]. These organs were intimately tied to the criminal underworld and Ukraine's shadow economy. The subsequent weakness and corruption of state organs acted as a barrier to effective civic action. A neutered civil society facilitated destabilisation campaigns and entrenched a system of criminal fiefdoms with ties to the Kremlin.

In conclusion, Russian disinformation efforts outside of its border must be characterised as a method to destabilise states such as Ukraine from the inside with the intention of taking them to the point of crisis and the polity itself disintegrating; and in doing so opening itself to Russian intervention and occupation. This is achieved through high-volume, multi-channel dissemination aimed at exploiting the heuristics of a crowded media environment highly susceptible to the reproduction of falsehoods aimed at highlighting or fabricating perceived weaknesses in the political, social and security settings of rival states. When working alongside the exploitation of instability in Ukraine through several channels[63], the result is a highly potent and effective means to not just unsettle the political environments of target states, but also to vivisect the epistemological groundings of these democracies. Moreover, by addressing the underlying strategic causes of Russian disinformation we see that it is unlikely to stop soon, and states such as Ukraine must invest considerable resources to prevent further Russian penetration.

[62] Shandra and Seely, (2019), "The Surkov Leaks, The Inner Workings of Russia"s Hybrid War in Ukraine", ***RUSI***, p.17
[63] As revealed by the Surkov leaks

2. Other Authoritarian States

As the "scale, scope and sophistication of online censorship worldwide" [64]has been increasing in the last years, a question can be raised of whether or not authoritarian regimes use similar tactics of censorship, misinformation and foreign influence. As a result, this section will investigate the existence of an aspiration for information control by discussing the domestic and foreign policies of China and Iran and comparing this to Russia's actions in Ukraine. Though evidence suggests that China and Iran, as well as Russia, use similar tactics and policies to achieve their goals of domestic censorship, misinformation and foreign influence, there is a lack of evidence supporting the view to fulfil the interest of their government, both domestically and abroad. Though objectives overlap, the motives are consistently related to each state, not a union of authoritarian states.

2.1 Domestic censorship and misinformation

2.1.1 Domestic Censorship and Misinformation in China

The People's Republic of China has a population of 1,4 billion people, over one billion of which use the Internet, representing almost 20% of the 4.95 billion Internet users worldwide in 2022.[65] Freedom House's annual report on online freedoms has named China "the world's worst abuser of internet freedom" for 8 consecutive years, and many scholars agree that China has the most sophisticated and complex system of online censorship and domestic control in the world.[66] The extensive system of Chinese information control is continually evolving, extremely complex and sensitive to changes in the country's political climate, not just the decisions of its leadership. Lu Wei, the former Deputy Head of the Propaganda Department of the Chinese Communist Party, sometimes referred to as "the gatekeeper of the Chinese Internet", once said that China "generates 30 billion pieces of information each day. It is not possible to apply censorship to this enormous amount of data. Thus, censorship is not the correct word choice. But no censorship does not mean no management".[67] This statement not only points to the façade that the Chinese leadership promotes regarding the extent of their involvement in access to information in China, but it also sheds light on the nuanced view China's leaders have of censorship within the country's borders which is reflected in the varied techniques and complex policies which characterise China's system of domestic censorship and misinformation.

---

[64] Palfrey, John. OpenNet Initiative

[65] Global Times (2022) "China has 1.032 billion internet users, 73.0% penetration rate"
S. Kemp (2022) "Digital 2022 – Global Overview Report"

[66] Freedom House (2022) "China – Freedom of the Net 2022 Country Report"

[67] Lu Wei as quoted in M.E. Roberts (2018) *Censored – Distraction and Diversion Inside China's Great Firewall*

Although the Chinese Communist Party (CCP) has employed authoritarian censorship for decades, the severity has increased in recent years, most importantly as a result of the consolidation of personal power and multiple restrictive reforms implemented by the current president Xi Jinping. This has resulted in increasing state control over the country's media.[68] The most famous feature of the extensive Chinese online censorship system is "the Great Firewall" which regulates and censors Chinese domestic Internet activity and blocks Chinese access to the global Internet and foreign platforms, often replacing these sources with domestic alternatives of misinformation and effectively creating "an alternative Internet infrastructure" for the Chinese population.[69]

According to GreatFire.org, a platform which tracks online censorship of websites in China, some of the blocked international websites include Google, Yahoo and Wikipedia, as well as social media platforms such as Facebook, Twitter, Instagram and WhatsApp and commonly referenced international news platforms such as the British Broadcasting Corporation (BBC), the New York Times and the Wall Street Journal.[70] As most international social media platforms are banned in China, the Chinese communication platforms WeChat and Weibo have been developed, but these are also subject to extensive censorship and are used to manipulate public opinion. Weibo has for example been used to either directly promote the state's agenda through "state mouthpieces" or indirectly through information manipulation by fake accounts.[71] It has been estimated that the Chinese state "fabricates almost half a billion inauthentic pro-government comments a year" on social media platforms through fake accounts and state-paid commentators.[72] Chinese companies are required to censor their own and their user's content, with the content being regularly removed before publication or immediately afterwards.[73] All Internet companies also have to give the Chinese government access to information about users online activities, and together with the fact that what is considered prohibited information is continually evolving, much of the Chinese population resort to self-censoring their online activities, overcompensating to make sure that they do not fail to comply with any censorship or surveillance laws and can be subjected to criminal punishment.[74]

Despite these extensive measures of censorship, the Chinese state is however unable to completely control its population and this has led to further developments in the state's methods of censorship.[75] It is for example possible to circumvent "the Great Firewall" through VPNs, something which has become increasingly common in the last few years, even though state restrictions on this have also been

[68] Freedom House (2022) "China – Freedom of the Net 2022 Country Report"
[69] S. Woolley & P.N. Howard Eds. (2018) *Computational Propaganda*
[70] GreatFire.org (2022) "Censorship of Alexa Top 1000 Domains in China"
Freedom House (2022) "China – Freedom of the Net 2022 Country Report"
[71] S. Woolley & P.N. Howard Eds. (2018) *Computational Propaganda*
[72] D. Kliman Et al. (2020) "Digital Influence Tools Used by China and Russia"
[73] S. Woolley & P.N. Howard Eds. (2018) Computational Propaganda
[74] J. Hassid (2008) "Controlling the Chinese Media – An Uncertain Business"
Freedom House (2022) "China – Freedom of the Net 2022 Country Report"
[75] M.E. Roberts (2018) *Censored – Distraction and Diversion Inside China's Great Firewall*

intensified in parallel with this since 2017, especially around important political events.[76] During Xi Jinping's rule, the CCP has extended their control over Chinese press, film, radio and television, increasingly subordinating Chinese media to the CCP's Central Propaganda Department.[77] Lorentzen makes the argument that this is precisely a result of this growing tendency of the Chinese population accessing censored information through the Internet which leads the Chinese state to intensify their control of traditional media to maintain control over information flows in the country.[78]

Because of this, Roberts has also described China as developing into a 'porous censorship' where censored information is available given enough time, knowledge and money, leading to a social divide between a well-educated and affluent elite with access to more censored information and the majority of the population who does not have the resources to gain such access. Roberts argues that this leads to the majority of the population consuming the abundant and more easily accessible state-approved information, without being fully aware of the extent of censorship they are being submitted to, and enabling targeted repression and censorship through fear of the minority, resulting in minimal dissent and a divided population less likely to form coordinated opposition.[79] Some political speech has also been allowed in China to monitor public opinion, manage possible developments towards dissent and keep local government effective, but this is restricted to only local problems unrelated to national politics.[80] As the Chinese people are endeavouring to circumvent CCP's policies of censorship and misinformation, the policies keep changing and becoming more sophisticated to maintain control over information flows in China, and by extension the Chinese population.

2.1.2 Domestic Censorship and Disinformation in Iran

Although the common authoritarian desire for information control is not coordinated in uniformity amongst differing authoritarian states, Iranian policies of censorship and misinformation, nonetheless, are in keeping with the ubiquitous bid for hegemonic information control demonstrated by China. Birthed through the revolution of 1978-79, the Islamic Republic of Iran has consistently sought to exert control over the flow of information to its citizens. This has not only impeded the manifestation of dissent but has aided in its repression when it does arise. Whilst a culture of journalistic repression has existed since its conception, the policies of information control have expanded and matured in accordance with the twenty-first century's digital evolution. Indeed, in 2001, judicial rulings transferred

[76] The Economist (2022) "As Censorship in China increases, VPNs are becoming more important"
Freedom House (2022) "China – Freedom of the Net 2022 Country Report"
[77] Freedom House (2022) "China – Freedom of the Net 2022 Country Report"
[78] P. Lorentzen (2014) "China"s Strategic Censorship"
[79] M.E. Roberts (2018) *Censored – Distraction and Diversion Inside China"s Great Firewall*
[80] S. Woolley & P.N. Howard Eds. (2018) *Computational Propaganda*
P. Lorentzen (2014) "China"s Strategic Censorship"

control of the country's Internet Service Providers (ISPs) over to the state,[81] subjecting them to stricter monitoring standards in contrast to Article 24 of the constitution which had guaranteed press freedom. This expanded "elicit" material to incorporate anything that "endangered the Islamic Republic" and or "offended the clergy and the Supreme Leader" and was furthered following the 2009 Green Movement. As will be explored below, this was viewed as an existential challenge to the state's sovereign authority and has led to Iran ranking 178th out of 180 countries for journalist freedom,[82] with imprisonments deterring journalist reporting alongside the increasingly substantial network of online censorship.

This network of control, incorporating internet blocks, firewalls and filters, has become increasingly sophisticated, with local variation carefully targeting regionally distinctive themes. For example, just 45 per cent of English-language sites were (as of 2008) censored, compared to 80 per cent of the Farsi-language websites.[83] Thus, the filtration system retains the capacity to adapt its information control towards contentious themes amongst aggrieved communities. A year later, any remanence of internet liberty was dismantled in the aftermath of the 2009 Green Movement. Following a reformist challenge in the 2009 elections, led by former President Mir Hossein Mousavi, electoral fraud led to spontaneous protests across the country.[84] In part, this was coordinated through the internet (specifically social media applications) and, accordingly, proved a catalyst for information control having illustrated the digital potential to undermine state authority. The aforementioned trends for controlling ISPs were furthered as the state bought a controlling stake in the Telecommunication Company of Iran and, more drastically, blocked Facebook and Twitter.[85]

Aware of the internet's potential for undermining political authority and legitimacy of the state, the decade that has followed the Green Movement has witnessed the continued trend towards complete censorship control. Indeed, at the time of writing this report, protests across Iran, following the death of Mahsa Zhina Amin for not complying with the country's veiling laws, have led to the banning of Instagram and WhatsApp, furthering the absence of international social media platforms.

Yet, the evolution towards information control proves more complicated than commonly presumed. Over 23.5 million of the country's population use VPNs (virtual private networks) to bypass government

[81] Atlantic Council: Iranian digital influence efforts: Guerrilla broadcasting for the twenty-first century: Emerson Brooking and Suzanne Kianpour: 11 February 2022: https://www.atlanticcouncil.org/in-depth-research-reports/report/iranian-digital-influence-efforts-guerrilla-broadcasting-for-the-twenty-first-century/.
[82] Reporters Without Borders: Iran: https://rsf.org/en/country/iran.
[83] Ronald J. Deibert. 14 Aug 2008, The geopolitics of internet control from: Routledge Handbook of Internet Politics Routledge, p. 329.
[84] Güneş Murat Tezcür (2012) Democracy promotion, authoritarian resiliency, and political unrest in Iran, Democratisation, 19:1, p. 130.
[85] Atlantic Council: Iranian digital influence efforts: Guerrilla broadcasting for the twenty-first century: Emerson Brooking and Suzanne Kianpour: 11 February 2022: https://www.atlanticcouncil.org/in-depth-research-reports/report/iranian-digital-influence-efforts-guerrilla-broadcasting-for-the-twenty-first-century/.

censorship.[86] Moreover, prior to the recent prohibition of Instagram, Iran was formally the 7th largest user of the platform, revealing a dichotomous tension between usage and restriction.[87]

However, arguments that highlight the weakness of Iranian social media restrictions do not correlate to suggestions that the desire for information control has faulted. If anything, the exposed limitations have catalysed increasingly draconian activity. Beginning in 2011, the "National Internet Project" has effectively sought to create a closed intranet that provides domestic services to reduce the need for access to the global system. Correspondingly, during the 2019 fuel protests, Iran was able to shut off the entire internet, with over 95% of the population affected,[88] in what has been described as the "largest Internet shut-down in history" both in terms of scale and effectiveness.[89] Similarly, during the 2022 "veil" protests, the internet was completely shut down in Iranian Kurdistan (the protest's epicentre), denoting a willingness to repeatedly use the draconian policy. Thus, the combination of banning uncontrolled social media outlets, with the retention of authority over the remaining sources of information reflects a culmination in Iran's aspiration for information control. Indeed, their nearly hegemonic position over the internet, a policy being replicated across authoritarian states, has enabled the prevention of dissent through the removal of seditious literature. When dissent has arisen, their control limits its efficacy by impeding the coordination of protests.

Notably, this is not to suggest that censorship has left the Iranian population void of information. Indeed, domestic misinformation proves a complementary strand in the assumption of epistemological control, with official state rhetoric arising alongside the denial of alternative sources of information. This paper understands misinformation to constitute the employment of false or inaccurate information, arguing that, unlike Russia which uses a subtly different policy of disinformation, the Iranian state has centralised a formal process of perpetuating informational insecurity. The importance of misinformation can be best relayed through the fact that the head of the state's propaganda agency (the Islamic Republic of Iran Broadcasting (IRIB)) is appointed directly by Iran's Supreme Leader. Moreover, irrespective of their increasing economic hardship that has, in part, followed US sanctions, the IRIB continues to retain an annual budget of over $750 million.[90] Reflecting a prioritisation of information control, the budget has funded the establishment of "cyber battalions", comprising an estimated 8000-strong unit designated to peddling a distorted truth that aligns with state rhetoric. At the start of 2020, Facebook had identified

[86] The Internet as a Global/Local Site of Contestation: The Case of Iran. In Celikates, R., J. de Kloet, E. Peeren & T. Poell (Eds.) 2017. Global Cultures of Contestation. London: Palgrave MacMillan, p. 6.
[87] Fikra Forum Policy Analysis: Threats to Iranian Instagram: Analysing Iran"s Internet Landscape: 24 November 2021: https://www.washingtoninstitute.org/policy-analysis/threats-iranian-instagram-analyzing-irans-internet-landscape).
[88] Freedom House: The true depth of Iran"s online repression: 2 December 2019: Amy Slipowitz: https://freedomhouse.org/article/true-depth-irans-online-repression.
[89] Atlantic Council: Iranian digital influence efforts: Guerrilla broadcasting for the twenty-first century: Emerson Brooking and Suzanne Kianpour: 11 February 2022: https://www.atlanticcouncil.org/in-depth-research-reports/report/iranian-digital-influence-efforts-guerrilla-broadcasting-for-the-twenty-first-century/.
[90] Atlantic Council: Iranian digital influence efforts: Guerrilla broadcasting for the twenty-first century: Emerson Brooking and Suzanne Kianpour: 11 February 2022: https://www.atlanticcouncil.org/in-depth-research-reports/report/iranian-digital-influence-efforts-guerrilla-broadcasting-for-the-twenty-first-century/.

766 pages which were followed by 5.4 million users and indirectly run by the Iranian regime.[91] This reflects the mutually reinforcing nature of censorship and misinformation, with the latter helping to mitigate the issue caused by the use of VPNs.

Not only, has misinformation enhanced a pro-regime narrative, but on the flip side, it has undermined external actors including both neighbouring and western states. For instance, to detract from their shortcomings in responding to the Covid-19 Pandemic, Iran's Fars News Agency reported that the Pfizer vaccine "kill[ed] six people in America".[92] Yet, this neglected that, in actuality, four of the deaths occurred in participants who had received the placebo. Again, this narrative was aided by censorship's limiting of alternative information avenues. At best this works to ensure unity of thought, in line with the official narrative but, at the very least, misinformation campaigns have ensured epistemological insecurity. Indeed, additional and contrasting reporting that the coronavirus was part of a US-led bio attack against Iran,[93] dilutes the consistency of information, whilst still pertaining to the general pro-state argument. These practices of "truth-subversion" have limited consensus and, in turn, hindered the establishment of nationally uniformed movements of opposition.[94]

2.1.3 Comparison: A global authoritarian aspiration for information control

China and Iran use similar techniques of domestic censorship and misinformation. Both promote an official state narrative of events, prevent alternative sources of information from reaching their respective populations and undermine epistemological security to combat dissent and maintain control. These measures of information control have manifested across authoritarian states, but their shared desire for such control is related to the political situation in their own countries and does not point towards a coordinated or uniform aspiration for global authoritarian information control. Similar techniques are instead used to achieve the objectives of individual state leaders. China and Iran have for example both sought to create their own independent and restricted strands of the Internet to enhance control in their respective countries. Though there is a common authoritarian desire for information control, this desire does not rise in uniformity and is instead the result of individual state goals.

[91] Atlantic Council: Iranian digital influence efforts: Guerrilla broadcasting for the twenty-first century: Emerson Brooking and Suzanne Kianpour: 11 February 2022: https://www.atlanticcouncil.org/in-depth-research-reports/report/iranian-digital-influence-efforts-guerrilla-broadcasting-for-the-twenty-first-century/.
[92] Alliance for securing democracy: How Russia, China, and Iran have shaped and manipulated coronavirus vaccine narratives: 6 March 2021: Bret Schafer, et al., https://securingdemocracy.gmfus.org/russia-china-iran-covid-vaccine-disinformation/.
[93] Oxford Internet Institute: Understanding Online Misinformation in Iran, the Epicentre of the Coronavirus in the Middle East: 24 June 2020: Mahsa Alimardani and Mona Elswah: https://www.oii.ox.ac.uk/news-events/news/understanding-online-misinformation-in-iran-the-epicentre-of-coronavirus-in-the-middle-east/.
[94] Adler, E., & Drieschova, A. (2021). The Epistemological Challenge of Truth Subversion to the Liberal International Order. International Organization, 75(2), p. 375.

There are interesting parallels in the policies of censorship and misinformation implemented in authoritarian regimes, not only between China and Iran, but between these two states and Russia, as well. Just like many other authoritarian regimes, both China and Russia have for example made the realisation "that absolute control over information [...] is neither possible nor necessary", and have implemented more sophisticated policies of information control to maintain their authority while simultaneously adapting to an environment with changing accessibility to information given the development of the Internet.[95] One such policy development, which has taken place in China, Iran and Russia, in response to the greater tendency of citizens to circumvent state restrictions has been described as "porous censorship" where states make access to more money, time or other resources necessary to circumvent information restrictions, leading to a social divide between an elite with more information who can be subjected to targeted repression and the majority of the population without such access being left in the dark.[96]

However, these similar policies are again used to promote individual state goals rather than one unified goal shared between the three states. For example, although Russian and Iranian rhetoric often aligns along anti-western axes, this reflects their respective self-interest and is not evidence of a common and coherent discursive construction. Therefore, just as China and Iran's use of similar policies does not represent a unified ambition, neither does the aligned rhetoric of Iran and Russia, or the use of similar policies of censorship in the three states. Instead, this proves a transactional consequence of their respective geopolitical self-interest and a by-product of their established misinformation policy of anti-western discourse.

2.2 Foreign misinformation and influence

2.2.1 Chinese Foreign Misinformation and Influence

China is not only one of the leading countries regarding domestic censorship and misinformation, but also one of the most prevalent actors on the international stage of misinformation and foreign influence. China's policies for international influence focus on improving opinions of the country abroad through exporting many of the techniques they use domestically and increasing control over local media in other countries, as well as promoting Chinese interests through economic and political networks of dependence and influence, especially in developing countries.

[95] D. Tapscott & A.D. Williams as quoted in K. Kyriakopoulou (2011) "Authoritarian States and Internet Social Media – Instruments of Democratisation or Instruments of Control?"
[96] M.E. Roberts (2018) *Censored – Distraction and Diversion Inside China's Great Firewall*

In the same way, Chinese domestic censorship and misinformation have increased since the beginning of Xi Jinping's rule, China's foreign influence has also expanded in recent years. Chinese media narratives are reaching audiences across the world, censorship of information which the CCP disapproves of is spreading and media outlets in other countries have been co-opted to contribute to this development.[97] Chinese foreign influence focuses on controlling international narratives about the country, in what Louis Lim and Julia Bergin describe as a determination "to combat what it [China] sees as decades of unchallenged Western media imperialism", through changing, co-opting and censoring information about China across the world.[98]

Furthermore, not only is Chinese influence increasing globally, but China's campaign to gain foreign influence affects every continent in the world with Southeast Asia and Africa being the most affected in the last few decades.[99] The most common and important method for China to spread their authoritarian influence abroad has been through their "Digital Silk Road"; an infrastructure of online surveillance and censorship, which is being adopted by governments across the world.[100]

Since 2009, it is estimated that China has spent $6.6 billion to improve its media presence internationally through hosting exchange programs and training for foreign reporters in China as well as providing free state media content in foreign newspapers.[101] China has also been known to use advertisements that promote state-sponsored information or positive propaganda about China to change public opinions in other countries.[102] The country has for example increasingly spread disinformation in Taiwanese media aimed at discrediting the Taiwanese government and promoting ideas of unification.[103] Though social media platforms such as Facebook and Twitter are banned domestically, China uses these platforms, as well as media networks such as China Central Television (CCTV) and China Daily, to influence foreign public opinion abroad, which was for example done through the establishment of the first CCTV overseas production centre in Nairobi, as China aimed to increase its influence in Africa, which has since been expanded.[104] There are debates about the extent to which these campaigns can achieve their aim of influencing foreign public opinion, but this is a developing part of Chinese policy for spreading the state's narratives abroad.[105]

---

[97] S. Cook (2022) "Beijing"s Global Media Influence 2022 – Authoritarian Expansion and the Power of Democratic Resilience"

[98] L. Lim & J. Bergin as quoted in R. Kumar (2021) "How China uses the News Media as a Weapon in its Propaganda War against the West"

[99] S. Cook (2022) "Beijing's Global Media Influence 2022"
D. Kliman Et al. (2020) "Digital Influence Tools Used by China and Russia"

[100] D. Kliman Et al. (2020) "Digital Influence Tools Used by China and Russia"
R. Kumar (2021) "How China uses the News Media as a Weapon in its Propaganda War against the West"

[101] R. Kumar (2021) "How China uses the News Media as a Weapon in its Propaganda War against the West"

[102] D. Kliman Et al. (2020) "Digital Influence Tools Used by China and Russia"

[103] Freedom House (2022) "Beijing"s Global Media Influence 2022 – Taiwan"

[104] K. Batchelor & X. Zhang Eds. (2017) *China-Africa Relations – Building Images through Cultural Cooperation, Media Representation and Communication*

[105] K. Batchelor & X. Zhang Eds. (2017) *China-Africa Relations – Building Images through Cultural Cooperation, Media Representation and Communication*

A large part of Chinese influence in other countries is also through intimidation or pressure. It has for example been argued that countries that rely heavily on trade with China, even democracies, show developments of higher levels of media censorship.[106] China has been known to use economic pressures on foreign companies (for example Zara, American Airlines, Disney, ESPN and Marriott) to censor information that is considered damaging to China.[107] It has also been reported that local media in regions with high levels of Chinese media influence are afraid to report anything that the Chinese state would disapprove of, or are pressured not to do so if they want to keep revenues from Chinese state-sponsored advertisements.[108] Developing countries with less effective local governments have been a great target as they often do not have their own stable media infrastructure, facilitating Chinese influence in the process of developing local media.[109]

Since 1999, through their "Going Out" policy, China has invested greatly in developing Chinese state-owned media in Africa with for example the Chinese-owned TV operator StarTimes Group spreading Chinese narratives in thirty African countries.[110] Media connected to the Chinese state often experience domestic Chinese censorship models, which for example happened when a weekly column in a South African newspaper was cancelled after it attempted to publish an article about the persecution of Uighur Muslims in China, allegedly because the companies that owned the newspaper had links to the Chinese state.[111] China's growing economic and political influence in many countries has become connected to the advancement and spread of authoritarian values of censorship and the desire for information control.[112] This is further worsened by other authoritarian states also being seen to adopt these Chinese models of information control in their own countries.[113]

2.2.2 Iranian Foreign Misinformation and Influence

Additionally and in a similar light, Iran's aforementioned instruments of misinformation can also be employed on foreign audiences in accordance with Iranian interests. This secondary employment of information control constitutes a strand of the exertion of "soft power", which, coined by Joseph Nye, seeks to gain advantage through "persuasion". Indeed, foreign misinformation is commonly used by Iran for specific ends and, more broadly, the peddling of anti-American sentiment within its near-abroad. Operating 30 radio channels and the news agency Pars Today which broadcasts 32, the IRIB has created an "information-laundering apparatus" capable of evading US sanction regulations.[114] This proves capable of misinforming foreign audiences with

[106] J. Gamso (2021) "Is China exporting Media Censorship? China"s Rise, Media Freedoms, and Democracy"
[107] D. Kliman Et al. (2020) "Digital Influence Tools Used by China and Russia"
[108] D. Kliman Et al. (2020) "Digital Influence Tools Used by China and Russia"
[109] R. Kumar (2021) "How China uses the News Media as a Weapon in its Propaganda War against the West"
[110] A. Essa (2018) "China is Buying African Media"s Silence",
[111] A. Essa (2018) "China is Buying African Media"s Silence",
[112] J. Gamso (2021) "Is China exporting Media Censorship? China"s Rise, Media Freedoms, and Democracy"
[113] M.E. Roberts (2018) *Censored – Distraction and Diversion Inside China's Great Firewall*
[114] Atlantic Council: Iranian digital influence efforts: Guerrilla broadcasting for the twenty-first century: Emerson Brooking and Suzanne Kianpour: 11 February 2022: https://www.atlanticcouncil.org/in-depth-research-reports/report/iranian-digital-influence-efforts-guerrilla-broadcasting-for-the-twenty-first-century/.

information published through apparently unconnected mediums and is necessary given the long-established suspicion of Iranian-branded media.[115] For example, "Nile Net Online", a media outlet with 115,000 followers, was exposed as part of Iran's misinformation network, posing as an Egyptian media source and challenging their support of America.[116] Not only does Iranian misinformation seek to undermine the U.S. but, within its near abroad, it challenges Sunni Arab powers.[117] This aims to undermine neighbouring and regional stability and reflects a belief that the discontent of a hostile state is beneficial in enhancing one's position within the balance of power.

Lastly, foreign misinformation has also been used by Iran to achieve spatial and temporally specific aspirations. For example, Iran perpetuated a Lebanese conspiracy that the West, specifically the U.S., had created ISIS, aiming to undermine American influence within Lebanon and, in turn, embolden the soft power of Hezbollah, an Iranian-backed militia group.[118] Thus, Iran not only seeks to retain information control within its sovereign borders but, externally, its pursuit of foreign misinformation represents an effort in information subversion, manipulating foreign audiences for their self-interest.

2.2.3 Comparison of authoritarian tools

In recent years China and Iran have developed a relationship of increasing cooperation, solidified with their 25-year cooperation agreement signed in 2021.[119] Despite their diverging policies on many issues, Chinese-Iranian cooperation is based on an agreed authoritarian opposition to what the two countries see as an international system dominated by the West and has resulted in China becoming Iran's primary trading partner of oil and they have developed a closer relationship through China's aid in developing the Iranian military and most notably their nuclear program.[120] This however seems to be a part of Chinese foreign influence efforts in the Middle East rather than any coordinated plan for increasing Iranian and Chinese joint influence abroad. Indeed, although Iranian foreign information in service of specific ambitions mirrors China's "Digital Silk Road", the substance and aim of these policies are unaligned. Put another way, authoritarian cooperation and common usage of misinformation, albeit ubiquitous, are not in uniformity.

[115] Atlantic Council: Iranian digital influence efforts: Guerrilla broadcasting for the twenty-first century: Emerson Brooking and Suzanne Kianpour: 11 February 2022: https://www.atlanticcouncil.org/in-depth-research-reports/report/iranian-digital-influence-efforts-guerrilla-broadcasting-for-the-twenty-first-century/.
[116] Reuters: Special Report: How Iran spreads disinformation around the world: 30 November 2018: Jack Stubbs and Christopher Bing: https://www.reuters.com/article/us-cyber-iran-specialreport-idUSKCN1NZ1FT.
[117] Atlantic Council: Iranian digital influence efforts: Guerrilla broadcasting for the twenty-first century: Emerson Brooking and Suzanne Kianpour: 11 February 2022: https://www.atlanticcouncil.org/in-depth-research-reports/report/iranian-digital-influence-efforts-guerrilla-broadcasting-for-the-twenty-first-century/.
[118] Atlantic Council: Iranian digital influence efforts: Guerrilla broadcasting for the twenty-first century: Emerson Brooking and Suzanne Kianpour: 11 February 2022: https://www.atlanticcouncil.org/in-depth-research-reports/report/iranian-digital-influence-efforts-guerrilla-broadcasting-for-the-twenty-first-century/.
[119] N.A. Moonakal (2022) "The Impact and Implications of China"s Growing Influence in the Middle East"
[120] S.W. Harold & A. Nader (2012) "China and Iran – Economic, Political and Military Relations"

Similarly, both China and Russia are endeavouring to expand their spheres of influence abroad and have in recent years cooperated to a greater extent in this process of gaining international control over information. Both countries have been known to use similar strategies of censorship and disinformation. The use of fake accounts and paid commentators, for example, promoting the respective state's narratives and the common techniques which they have developed domestically to influence other countries and train them to use similar tactics.[121] However, not only are their respective policies unaligned, but even within techniques, disparities arise. Both China and Russia have different approaches to increasing their foreign influence. China generally has a broader focus of spreading disinformation to the largest audience possible, while Russia has a more specific approach of targeting specific parts of a population with disinformation, and the two countries use similar techniques in different ways, for example in the use of fake accounts which China primarily uses to promote China's image and Russia primarily uses to dilute the information available.[122] In this way, the two states employ many of the same techniques to expand their influence abroad, but in slightly different ways and generally with different aims.

Importantly, however, this has changed with the recent Russian war in Ukraine. As reported by the Russian newspaper Tass, Xi Jinping and Vladimir Putin have recently given a joint statement indicating that the two states call for the "internationalisation of Internet governance", with both states promoting equal sovereign rights for each country "to regulate national segments of the Internet".[123] A strong argument has been made by commentators that "this collaboration should be seen as part of a broader project to reshape the global information landscape to favour the Kremlin and Beijing's authoritarian political projects".[124] This should most definitely raise international concern, but it does not yet necessarily represent a unified global authoritarian aspiration for information control. As the Diplomat argues, this Chinese and Russian new vision of Internet governance "is about the security of their regimes".[125] Thus, though this is a unified call, the objective seems to be for both China and Russia to respectively strengthen their regimes, not the category of authoritarian regimes globally.

It seems to instead be a case of a coincidingly common goal leading to this cooperation, rather than a unified Chinese and Russian foreign policy. Some scholars have for example argued that though China and Russia are "jointly advancing their shared interests in the international arena" "the asymmetry of cooperation in favour" of China is increasingly at "odds with Russia's national goals in digital technology". These difficulties are further increased by the fact that Sino-Russian cooperation is "based on shared interests rather than ideology or shared values" with "differences in resources and standpoints (...) reflected in the implementation of digital surveillance".[126] This furthers the argument that such an alliance is likely one of coinciding national goals rather

[121] D. Kliman Et al. (2020) "Digital Influence Tools Used by China and Russia"
[122] D. Kliman Et al. (2020) "Digital Influence Tools Used by China and Russia"
[123] Tass (2022) "Russia and China Call for Internationalization of Internet Governance Statement"
[124] D. Bandurski (2022) "China and Russia are Joining Forces to Spread Disinformation"
[125] C. Mok (2022) "China and Russian Want to Rule the Global Internet"
[126] S. Kirchberger, S. Sinjen, N. Wörmer Eds. (2022) *Russia-China Relations – Emerging Alliance or Eternal Rivals*

than a united authoritarian stance. This recent Sino-Russian call for cooperation is also closely connected to the Russian War in Ukraine. Though China has contributed to promoting Russian propaganda and disinformation related to the war, their "interests diverge in important ways" and China has "avoided fully backing the incursion".[127] This hesitancy can for example be seen in how China abstained from voting on the UN Security Council Resolution condemning Russian annexation of parts of Ukraine.[128] Therefore, the Sino-Russian call for "the internationalisation of internet governance" is as much a question of national interests as a shared vision between two authoritarian states. Though very much worthy of concern, it not seem to be a coordinated authoritarian vision for global information control.

2.3 Conclusion

In summation, despite the aspiration for information control proving ubiquitous amongst global authoritarian states, their pursuit of it does not occur in uniformity of coherence. Though evidence exists that China, Iran and Russia each employ similar mechanisms and policies for ascertaining epistemological dominance, namely that of domestic censorship and misinformation at home and abroad, this does not evidence a unified goal. Instead, these are employed in alignment with each state's own respective self-interest. Whilst these have, on occasion, manifested in consistency with one another, they, nevertheless, continuously relate to each authoritarian state.

On the issue of censorship, authoritarian states have, albeit not with complete success, pursued absolute control. China's "Great Firewall" has been replicated in both the Iranian's use of filters and their gradual outlawing of social media company operations. Going forward, both are seeking to separately construct a "new" internet. Both employ an increased arbitrariness to what constitutes "elicit" and "supervise" material. Moreover, both have grappled with the limitations posed by the use of VPNs. Not only does this offer insight into the population's relationship with digital information and, implicitly, the state and one another, but, practically, it has ensured that censorship proves just one of a multi-pronged approach to information control. Indeed, censorship does not reflect an aspiration for an absence of information but, instead, provides the grounding through which misinformation can arise. Using guerrilla information broadcasting techniques, to disguise misinformation as allegedly neutral content, each of the aforementioned states seeks to present themselves in a positive light. Even without this success, misinformation and censorship servs to create epistemological insecurity to dissuade dissent. Thus, domestic policies reveal a common pursuit of information control through the avenues of censorship and misinformation.

That said, the developments traced throughout this section reveal that their respective progression toward control mirrored domestic events and considerations. Consequently, the aspiration did not arise in cooperation

[127] D. Bandurski (2022) "China and Russia are Joining Forces to Spread Disinformation"
[128] S. Lewis & T. Gardner (2022) "Russia Vetoes UN Resolution on Proclaimed Annexations, China Abstains"

with one another. Again, although anti-western rhetoric has permeated throughout these developments interlinks of support prove transactional in their nature, mirroring self-interest. Lastly, and on a similar front, authoritarian state's exertion of information control into the international sphere has not arisen in coherence. For instance, China's "Digital Silk Road" pursues a global policy in contradiction to Iran's emphasis on their "near abroad" and Russia's more targeted approach.

Therefore, in spite of common policies, techniques and rhetoric, reflecting a ubiquitous aspiration for information control, authoritarian states have not pursued this in coordination with one another. Instead, the development of their respective approaches reflects their own context and self-interest.

3. Policy Proposal to ensure secure access to free, independent and plural media worldwide

The rise in digital authoritarianism, which has come into stark focus in the context of the war in Ukraine, and the precarious state of media freedom in many countries across the world raises the issue of what the international community might be able to do to contain the threats associated with these developments. An effective approach to present challenges should seek to build on, rather than circumvent or replace, present instruments and policy frameworks, utilising existing networks of stakeholders, which include governments, businesses and civil society actors. With such support it will become possible to proliferate the best practices in the field and create incentives for authoritarian states and weak democracies to adjust their conduct.

Recent examples of concerted efforts involving both local and international actors, such as those targeting internet shutdowns, provide a workable roadmap for future action seeking to promote media pluralism. A large literature has also emerged in relation to the issue of state-sponsored online disinformation, which has become politically salient, particularly in the aftermath of the 2016 US presidential election. What follows is a review of the existing policy ecosystem, as well as a set of policy recommendations aiming to provide the groundwork for a coherent and effective strategy for combatting digital authoritarianism and upholding freedom of information globally.

3.1 Policy status-quo

3.1.1 Action by social media platforms

Social media platforms have increasingly become a major news source over the last decade. Whilst the ability of users to post and circulate content through channels like Facebook or Twitter has brought about many benefits, the difficulties associated with reviewing the factual accuracy of social media content have turned these platforms into prime vehicles for the spread of state-sponsored disinformation. Fortunately, public outcry has pressured social media companies into attempting to develop more robust content review protocols and identifying other ways to curb the spread and impact of disinformation. What follows is a review of the policies put in place by three of the largest social media platforms – Facebook, Twitter and TikTok – to counter-respond to the proliferation of false information.

Facebook

In 2017, Facebook (now Meta) committed to fighting the spread of misinformation by "disrupting economic incentives", "building new products to curb the spread of false news" and "helping people make more informed decisions when they encounter false news".[129] Some of the measures it has pursued include restricting the ability of purveyors of false news to buy ads on Facebook, intensifying efforts to detect fake accounts and streamlining the community-based reporting process of false news stories.[130] A prominent strategy of dealing with disinformation entails "providing more context" by submitting reported stories to independent third-party fact-checking organisations; if found to be false, the stories are then flagged as disputed and annotated with a link to an article that contextualises the information featured in the story – while also appearing lower in users" news feeds.[131]

Increasing public and political pressure, particularly in the context of disinformation related to the COVID-19 pandemic, has seemingly led to a more aggressive deployment of the tools at its disposal by Facebook, as well as to a more extensive drive to publicise its efforts.[132] In the aftermath of Russia's invasion of Ukraine, as pressure yet again increased on Meta to address the issue of disinformation, Facebook and Instagram reported having taken down a fairly small but coordinated disinformation

[129] Adam Mosseri, "Working to Stop Misinformation and False News" (*Working to Stop Misinformation and False News | Meta for Media*, April 2017) <https://www.facebook.com/formedia/blog/working-to-stop-misinformation-and-false-news> accessed 12 November 2022.
[130] Idem
[131] Idem
[132] Guy Rosen, "How We're Tackling Misinformation Across Our Apps" (*Meta*, 22 March 2021) <https://about.fb.com/news/2021/03/how-were-tackling-misinformation-across-our-apps/> accessed 12 November 2022.

network targeting Ukrainians, whilst also blocking access to Russia Today and Sputnik across the European Union.[133] Under conditions of intense public and political scrutiny with regard to the threat of disinformation, Meta has demonstrated increased interest in developing tools to monitor and tackle the issue. There are grounds for scepticism, however – misinformation still spreads at an alarming rate on the platform, with one study suggesting that pages known for spreading inaccurate information received up to six times more interactions than trustworthy news sources on Facebook.[134]

Twitter

Not unlike Facebook, Twitter has also come under increased scrutiny in terms of its approach to tackling the spread of false information. Twitter policy differentiates the toolkit deployed in responding to "misleading information" depending on "potential for offline harm", pursuing one of three strategies in tackling this type of content: removal, "if offline consequences could be immediate and severe", limiting amplification or informing and contextualising.[135] The latter is done through a series of tools, including labelling content by offering a notice sharing additional context and alerting users that a Tweet has violated Twitter policy when attempting to share it.[136] A feature that allows users to report Tweets for containing misinformation is still in a limited testing phase and thus available in only a handful of countries[137] - such reports "are reviewed and acted on independently from other Tweet reporting flows (e.g. for abuse)".[138]

Another feature available in limited testing, Community Notes, allows users to write a note with additional information that is attached to a Tweet in order to offer potentially useful community-sourced additional context.[139] State-sponsored disinformation in particular is partly addressed through the government and state-affiliated media account labels on Twitter, which prevent the dissemination of state-sponsored narratives without users being aware of connections between certain accounts and foreign governments. In spite of Twitter's expressed commitments to combatting misinformation and the use of bots on the platform, however, there are still grounds for concern – for instance, one study, commissioned by the Knight Foundation, found that 83% of the most prominent accounts involved in

[133] Dan Milmo and Dan Milmo Global technology editor, "Facebook Takes down Ukraine Disinformation Network and Bans Russian-Backed Media" *The Guardian* (28 February 2022) <https://www.theguardian.com/technology/2022/feb/28/facebook-takes-down-disinformation-network-targeting-ukraine-meta-instagram> accessed 12 November 2022.
[134] Elizabeth Dwoskin, 'Misinformation on Facebook Got Six Times More Clicks than Factual News during the 2020 Election, Study Says' *Washington Post* (10 September 2021) <https://www.washingtonpost.com/technology/2021/09/03/facebook-misinformation-nyu-study/> accessed 28 November 2022.
[135] "How We Address Misinformation on Twitter" (*Twitter Help Center*) <https://help.twitter.com/en/resources/addressing-misleading-info> accessed 12 November 2022.
[136] Idem
[137] Certain users in Australia, Brazil, the Philippines, South Korea, Spain and the US can access this feature.
[138] Idem
[139] Idem

spreading fake and conspiracy news during the 2016 election were still active on the platform as of November 2022.[140]

TikTok

With a global reach gained over the last few years, TikTok has become one of the largest social media platforms in the world and has, accordingly, been subject to increased pressures to develop effective tools to counter disinformation. TikTok has committed to act to "remove accounts that seek to mislead people or use TikTok to deceptively sway public opinion".[141] Misinformation is addressed by a specialised team of moderators in conjunction with a series of independent fact-checking organisations, all accredited by the International Fact-Checking Network.[142] Upon establishing that information contained in a video is false, the video may either be removed from the platform or made ineligible for recommendation into For You feeds,[143] a standard penalty for violations of Community Guidelines that greatly reduces the video's reach, restricting it to the followers of the account that has posted it or search results. A series of recent investments made by TikTok in the area of tackling misinformation include the creation of a database of previously fact-checked claims that can help streamline the decision-making process of misinformation moderators and a proactive detection program with fact-checkers who flag evolving claims seen on the internet, allowing TikTok to search for such claims and remove violations – according to TikTok's Newsroom website, "[s]ince starting this program last quarter, [it] identified 33 new misinformation claims, resulting in the removal of 58,000 videos from the platform".[144] Once again, in spite of these efforts, research indicates that misinformation is still spreading at an alarming rate on TikTok. For instance, an experiment conducted by Global Witness and the Cybersecurity for Democracy team at NYU Tandon showed that TikTok's anti-disinformation policies targeted towards political ads could be circumvented significantly more easily than those of the other tested platforms (Facebook and YouTube).[145]

Social media companies have been placed under increased scrutiny in the last few years over their handling of disinformation, state-sponsored or otherwise. A flurry of new commitments to effectively combatting the spread of false information, particularly pertaining to political topics, has ensued. However commendable, there are grounds for believing that newly implemented policies do not adequately address the problem. An issue that hampers the understanding of policymakers and other

[140] Matthew Hindman and Vladimir Barash, 'Disinformation, "Fake News" and Influence Campaigns on Twitter' (*Knight Foundation*) <https://www.knightfoundation.org/features/misinfo> accessed 28 November 2022.
[141] Cormac Keenan, "An Update on Our Work to Counter Misinformation" (*Newsroom / TikTok*, 28 September 2022) <https://newsroom.tiktok.com/en-us/an-update-on-our-work-to-counter-misinformation> accessed 12 November 2022.
[142] Cormac Keenan, "An Update on Our Work to Counter Misinformation" (*Newsroom / TikTok*, 28 September 2022) <https://newsroom.tiktok.com/en-us/an-update-on-our-work-to-counter-misinformation> accessed 12 November 2022.
[143] Idem
[144] Idem
[145] Global Witness, 'TikTok and Facebook Fail to Detect Election Disinformation in the US, While YouTube Succeeds' (*Global Witness*, October 2022) <https:///en/campaigns/digital-threats/tiktok-and-facebook-fail-detect-election-disinformation-us-while-youtube-succeeds/> accessed 28 November 2022.

interested parties with respect to the problem of disinformation is that companies are generally secretive about its full extent. Publicly available data from social media platforms is oftentimes lacking, making it difficult to develop effective public policy strategies to counter state-sponsored disinformation.

Restrictions on media outlets linked to authoritarian regimes

Within democratic states, the practice of severely restricting or banning media outlets by virtue of their connection to foreign states (be they authoritarian or not) is generally limited in scope, as it is often considered to conflict with constitutional and other legal safeguards for press freedom. As such, the recent EU-imposed sanctions on RT and Sputnik have constituted a departure from standard practice in dealing with state-sponsored disinformation. The Council of the European Union introduced the restrictive measures in early March 2022, "urgently susp[ending] the broadcasting activities of Sputnik" and RT/Russia Today (RT English, RT UK, RT Germany, RT France, and RT Spanish) in the EU, or directed at the EU, until the aggression to Ukraine is put to an end, and until the Russian Federation and its associated outlets cease to conduct disinformation and information manipulation actions against the EU and its member states".[146] [147] The goal of combatting Russian-sponsored disinformation was also featured prominently in the justification for the EU's decision.[148] The General Secretary of the European Federation of Journalists expressed concern over the decision, on the grounds that the EU did not have the legal competence to introduce restrictions on media outlets and that the precedent set by the EU's decision would be problematic: "In our liberal democracies, it is independent regulators, never the government, that are allowed to manage the allocation of licences. The EU"s decision is a complete break with these democratic guarantees. For the first time in modern history, Western European governments are banning media".[149] These criticisms have been echoed across civil society.[150] [151] [152]

[146] "EU Imposes Sanctions on State-Owned Outlets RT/Russia Today and Sputnik"s Broadcasting in the EU" (*Council of the European Union*, 2 March 2022) <https://www.consilium.europa.eu/en/press/press-releases/2022/03/02/eu-imposes-sanctions-on-state-owned-outlets-rt-russia-today-and-sputnik-s-broadcasting-in-the-eu/> accessed 13 November 2022.

[147] The move was framed as part and parcel of the EU's efforts to respond to the Russian invasion of Ukraine. Sputnik and Russia Today's association to the Kremlin made them, according to the Council, "essential and instrumental in bringing forward and supporting the military aggression against Ukraine, and for the destabilisation of its neighbouring countries' (idem)

[148] Idem

[149] Idem

[150] "Understandable, but Still Wrong: How Freedom of Communication Suffers in the Zeal for Sanctions" (*Media@LSE*, 10 June 2022) <https://blogs.lse.ac.uk/medialse/2022/06/10/understandable-but-still-wrong-how-freedom-of-communication-suffers-in-the-zeal-for-sanctions/> accessed 13 November 2022.

[151] Toby Sterling, "Dutch Journalists, Rights Group File Lawsuit Challenging EU Ban on RT, Sputnik" *Reuters* (25 May 2022) <https://www.reuters.com/business/media-telecom/dutch-journalists-rights-group-file-lawsuit-challenging-eu-ban-rt-sputnik-2022-05-25/> accessed 13 November 2022.

[152] Mark MacCarthy, "Why a Push to Exclude Russian State Media Would Be Problematic for Free Speech and Democracy" (*Brookings*, 14 April 2022) <https://www.brookings.edu/blog/techtank/2022/04/14/why-a-push-to-exclude-russian-state-media-would-be-problematic-for-free-speech-and-democracy/> accessed 13 November 2022.

3.1.2 Notable multilateral initiatives and policy instruments

As issues pertaining to human rights and media freedom have become more entangled with the Internet, a series of multilateral initiatives and policy instruments have sprung up attempting to address the issue. The result of this development has been a proliferation of recommendations, best practices and guidelines with broad legitimacy, derived from multi-stakeholder collaboration. The willingness of participating stakeholders to translate them into actual policy practice remains the key variable that has determined and will continue to determine the practical success of these multilateral efforts.

Internet Governance Forum

Created in 2006, the Internet Governance Forum (IGF) is a multi-stakeholder platform set up as part of the United Nations ecosystem in order "to bring people together from various stakeholder groups as equals, in discussions on public policy issues relating to the Internet".[153] The IGF is undoubtedly one of the largest international fora focused on digital policy. In 2022, a variety of events have taken place under its auspices discussing optimal policy responses to combatting disinformation,[154] the usage of unconditional bans and "de-platforming" as a tool of content moderation[155] or the widespread and adverse impacts of internet shutdowns on marginalised communities such as refugees.[156] The last IGF Forum (Poland, 2021) focused on 6 issue-area tracks covering topics such as data protection, universal access, Internet connectivity and digital cooperation.[157] The 2022 IGF Forum – its 17th edition – set the goal of avoiding internet fragmentation as one of its key themes - suggesting that developments relating to internet shutdowns or government censorship have gained enough salience to constitute a cause of concern for the international community.

United Nations Guiding Principles on Business and Human Rights

The UN Guiding Principles on Business and Human Rights were developed by the Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises and endorsed by the UN Human Rights Council in 2011.[158] The

[153] "About Us | Internet Governance Forum" (*Internet Governance Forum*) <https://www.intgovforum.org/en/about#about-us> accessed 12 November 2022.
[154] "IGF 2022 Open Forum #108 Combatting Disinformation without Resorting to Online Censor | Internet Governance Forum" (*Internet Governance Forum*) <https://intgovforum.org/en/content/igf-2022-open-forum-108-combatting-disinformation-without-resorting-to-online-censor> accessed 12 November 2022.
[155] "IGF 2022 WS #52 De-Platforming as Censorship Means in the Digital Era | Internet Governance Forum" <https://www.intgovforum.org/en/content/igf-2022-ws-52-de-platforming-as-censorship-means-in-the-digital-era> accessed 12 November 2022.
[156] "IGF 2022 Launch / Award Event #11 The Impact of Internet Shutdown on Refugees and Host Communities in Uganda. | Internet Governance Forum" (*Internet Governance Forum*) <https://intgovforum.org/en/content/igf-2022-launch-award-event-11-the-impact-of-internet-shutdown-on-refugees-and-host> accessed 12 November 2022.
[157] "IGF 2021 Summary" <https://www.intgovforum.org/en/filedepot_download/223/20706> accessed 12 November 2022.
[158] Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises and Office of the High Commissioner on Human Rights, "Guiding Principles on Business and Human

objective of the Guiding Principles is that of "enhancing standards and practices with regard to business and human rights so as to achieve tangible results for affected individuals and communities, and thereby also contributing to a socially sustainable globalization", without however creating any new legally binding obligations.[159] The Guiding Principles have been previously invoked as a useful framework in the context of human rights promotion efforts on the Internet[160] primarily as a result of their elaboration of business enterprises' responsibility to carry out human rights due diligence by "assessing actual and potential human rights impacts, integrating and acting upon the findings, tracking responses, and communicating how impacts are addressed".[161] Principle 17 sets the key parameters for human rights due diligence, while Principles 18 through 21 develop a clearer account of what the process might entail.[162] The Guiding Principles thus represent a widely accepted and authoritative international standard that can serve as a centrepiece for the development of new policy strategies aimed at combatting digital authoritarianism.

Freedom Online Coalition

The Freedom Online Coalition (FOC) is a multilateral forum set up in 2011 by the Dutch Foreign Ministry and encompasses 34 national governments (to date, Iran, Russia and China have not joined the initiative). The Founding Declaration of the FOC defines its purpose as being "to share, as appropriate, information between our States on potential violations and other measures that undermine the enjoyment of freedom of expression and other human rights on the Internet" and "to consider measures needed to protect and advance these rights, working in close engagement with all relevant stakeholders".[163] It also affirms the FOC's Participating States' commitment to "support – both politically and through project aid – the ability of individuals, particularly those operating in repressive environments, to exercise their human rights through the Internet and connection technologies".[164] Since its creation, the FOC has held yearly conferences hosted across the world by the holders of the rotating Chairship.

Rights. Implementing the United Nations "Protect, Respect and Remedy" Framework" <https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf> accessed 12 November 2022.

[159] Idem

[160] See, for instance, Adrian Shabhaz, Allie Funk and Kian Vesteinsson, "Freedom on the Net 2022: Policy Recommendations" (*Freedom House*, 2022) <https://freedomhouse.org/report/freedom-net/2022/countering-authoritarian-overhaul-internet/policy-recommendations> accessed 10 November 2022.

[161] Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises and Office of the High Commissioner on Human Rights, "Guiding Principles on Business and Human Rights. Implementing the United Nations "Protect, Respect and Remedy" Framework" <https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf> accessed 12 November 2022.

[162] Idem

[163] Freedom Online Coalition, "Founding Declaration of the Freedom Online Coalition" <https://freedomonlinecoalition.com/document/the-founding-declaration-freedom-online-joint-action-for-free-expression-on-the-internet/> accessed 11 November 2022.

[164] Idem

Accordingly, in its latest program of action, elaborated in 2022 by the current Chair, Canada, the FOC has committed to coordinating action to promote its core values within such international fora as the UN General Assembly, the UN Human Rights Council, the UN Open Ended Working group, the Internet Governance Forum, the Organization of American States and the Council of Europe's Committee on Artificial Intelligence,[165] recognising the importance of such organisations in shaping international norms on state conduct and engaging with them accordingly.[166] Lastly, the FOC undertakes to intensify its attempts to raise awareness around human rights violations on the Internet, including through social media and other outreach initiatives.[167]

In a similar vein, in October 2022, the FOC also issued a Joint Statement on Internet Shutdowns in Iran, calling "on the Government of Iran to immediately lift restrictions intended to disrupt or prevent their citizens from accessing and disseminating information online and from communicating safely and securely"[168]. The FOC has therefore proven to be effective in aggregating calls for upholding human rights online and conveying them to a wider global audience in a way that eschews politicisation.

Tech for Democracy

Tech for Democracy (TFD) is a multi-stakeholder initiative launched by the Danish Foreign Ministry, bringing together democratic governments (therefore not including China, Russia and Iran), companies and civil society organisations which have joined the Copenhagen Pledge on Tech for Democracy, committing to "applying [their] shared democratic values and a human rights-based approach in the design, development, deployment, and use of digital technologies".[169] As part of the TFD initiative, multiple Action Coalitions have been set up to "target specific issues in the intersection of tech, democracy and human rights", with Coalition partners committing to "engage in concrete activities and deliver concrete solutions in line with the Copenhagen Pledge".[170] For instance, the Trustworthy Information Online Action Coalition unites the Danish Ministry of Foreign Affairs, Salesforce, Witness, Global Voices and the Wikimedia Foundation and seeks to "[d]evelop capacities for effective information governance, including globally-relevant systems, tools and capabilities to identify, detect and address false and misleading information".[171] In addition to the work of the Action Coalitions, TFD

[165] Freedom Online Coalition, "Freedom Online Coalition Program of Action 2022. Digital Inclusion: A Democratic and Human Rights-Based Vision for the Digital Age" <https://freedomonlinecoalition.com/wp-content/uploads/2022/01/FOC_ProgramofAction_2022_ENG.pdf> accessed 12 November 2022.
[166] Idem
[167] Freedom Online Coalition, "Freedom Online Coalition Program of Action 2022. Digital Inclusion: A Democratic and Human Rights-Based Vision for the Digital Age" <https://freedomonlinecoalition.com/wp-content/uploads/2022/01/FOC_ProgramofAction_2022_ENG.pdf> accessed 12 November 2022.
[168] Freedom Online Coalition, "FOC Issues Joint Statement on Internet Shutdowns in Iran" (*Freedom Online Coalition*, 20 October 2022) <https://freedomonlinecoalition.com/foc-issues-joint-statement-on-internet-shutdowns-in-iran/> accessed 12 November 2022.
[169] "Sign the Pledge" (*Tech for Democracy*) <https://techfordemocracy.dk/join-the-initiative/> accessed 12 November 2022.
[170] "Coalitions" (*Tech for Democracy*) <https://techfordemocracy.dk/coalitions/> accessed 12 November 2022.
[171] "Trustworthy Information Online" (*Tech for Democracy*) <https://techfordemocracy.dk/action-coalitions/trustworthy-information-online/> accessed 12 November 2022.

organised an international conference in Copenhagen on 18 November 2021, entailing six sessions covering key issues in the promotion of democracy and human rights in the digital age.[172]

Declaration for the Future of the Internet

In April 2022, the US State Department launched the Declaration for the Future of the Internet, which it branded "a political commitment among Declaration partners to advance a positive vision for the Internet and digital technologies"[173]. The US was joined in endorsing the Declaration by 61 other national governments, as well as the European Commission, and it "remains open to all governments or relevant authorities willing to commit its vision and principles".[174] The Declaration lays out a vision for Digital Internet that, *inter alia*, includes "foster[ing] societies where … [t]echnology is used to promote pluralism and freedom of expression, sustainability, inclusive economic growth, and the fight against global climate change".[175]

Relevant to the topic of the current analysis, the Declaration Partners "[r]eaffirm [their] commitment that actions taken by governments, authorities, and digital services including online platforms to reduce illegal and harmful content and activities online be consistent with international human rights law", to "[r]efrain from government-imposed internet shutdowns or degrading domestic Internet access, either entirely or partially" and to "[r]efrain from blocking or degrading access to lawful content, services, and applications on the Internet, consistent with the principles of Net Neutrality subject to applicable law, including international human rights law".[176] The European Commission has emphasised the importance of the Declaration in the context of the war in Ukraine, which highlights both the risks raised by service shutdowns, as well as the threat by some governments (in this case, Russia's) to create a parallel digital ecosystem, separate from the "global open Internet, which is a driving force for the economies and societies worldwide"[177].

Whilst the Declaration has been primarily framed in news coverage in terms of a confrontation with Russia and China, it is highly unlikely to affect their behaviour in a meaningful way – an initiative set up by the US can very easily be rejected by states unwilling to cooperate on political grounds (unsurprisingly, neither China, Russia, nor Iran have signed up to it). However, the Declaration may

[172] "The Conference" (*Tech for Democracy*) <https://techfordemocracy.dk/watch-now/> accessed 12 November 2022.
[173] US State Department, "Declaration for the Future of the Internet" <https://www.state.gov/declaration-for-the-future-of-the-internet/> accessed 12 November 2022.
[174] Idem
[175] US State Department, "A Declaration for the Future of the Internet" <https://www.state.gov/wp-content/uploads/2022/04/Declaration-for-the-Future-for-the-Internet.pdf> accessed 10 November 2022.
[176] Idem
[177] "Declaration for the Future of the Internet" (*European Commission*) <https://ec.europa.eu/commission/presscorner/detail/en/IP_22_2695> accessed 12 November 2022.

very well play a role in advancing a set of global norms that shape the conduct of weak democracies with wavering commitments to media pluralism and internet freedom.[178] [179]

Since the creation of the Internet Governance Forum, a wide variety of institutions and organisations have been set up to deal specifically with issues related to digital communications. Over time, they have proven to be effective arenas of dialogue and contestation over human rights and freedom on the Internet. However, as with most international organisations and initiatives, the extent to which their findings, conclusions and calls for action are reflected in policy reality is largely dependent on the decisions made by individual Member States. Additionally, robust and sustained diplomatic coordination is required on the part of advocates of Internet freedom in order to effectively promote their objectives within these fora. Multilateral initiatives are what states make of them – and those concerning digital media freedom are no exception.

High-tech export controls

Supply chains in tech manufacturing are highly globalised in nature. As such, export controls introduced by any state included in these supply chains can disrupt the manufacturing of hardware and technological equipment. This has a wide range of implications for any economy, but, for authoritarian states in particular, disruptions in tech supply chains also impact the ability of the government to covertly monitor its citizens. The Biden administration's recent decision to introduce a ban on semiconductor exports to China is undoubtedly the most high-profile instance of high-tech export controls in recent history. Motivated by geopolitical considerations going far beyond any concerns for the lack of media freedom in China, the move is expected to severely impact China's tech manufacturing sector, which remains reliant on semiconductor imports.[180] Crucially, semiconductors are essential in powering the surveillance tech used by the Chinese government[181], meaning that the export ban instituted by the Biden administration has the potential to undermine China's efforts to crack down on free journalism within its borders. The key role played by the high-tech sector in the Chinese economy will likely lead to a proportionate response from Chinese authorities[182]; additionally, the US strategy faces important limitations insofar as European states have not joined in imposing similar export bans, which could, in

[178] Alex Engler, "The Declaration for the Future of the Internet Is for Wavering Democracies, Not China and Russia" (*Brookings*, 9 May 2022) <https://www.brookings.edu/blog/techtank/2022/05/09/the-declaration-for-the-future-of-the-internet-is-for-wavering-democracies-not-china-and-russia/> accessed 10 November 2022.

[180] Michael Bluhm, "Biden"s Hugely Consequential High-Tech Export Ban on China, Explained by an Expert" (*Vox*, 5 November 2022) <https://www.vox.com/world/2022/11/5/23440525/biden-administration-semiconductor-export-ban-china> accessed 13 November 2022.

[181] Idem

[182] Idem

the long run, undermine the competitiveness of US tech manufacturers as well as greatly diminishing the pressure exerted on China.[183]

Nevertheless, similar measures were imposed by the US earlier this year on Russia following the invasion of Ukraine[184], on Iran as part of wider sanctions packages[185] and important steps have been taken in bolstering international collaboration on the matter through the US-led Export Controls and Human Rights Initiative, launched in 2021[186]. Trade policy, particularly in the tech sector, has therefore increasingly come to the fore of the debate about changing the conduct of authoritarian states, with important implications for media freedom. As the Chinese example highlights, the extent to which international coordination remains a crucial component of policy action in the area has the potential to determine the success of export controls in achieving their declared objectives.

3.2 Policy recommendations

Recent policy developments around combatting digital authoritarianism and promoting media freedom on the Internet have been broadly positive. Enhanced multi-stakeholder cooperation and a renewed policy toolkit have succeeded in charting a clearer pathway for the advancement of human rights online. Yet more is needed, particularly considering sustained efforts in resisting calls for democratisation on the Internet by authoritarian states such as Russia, China and Iran. What follows is a series of policy recommendations selected after a careful review of existing literature, divided into two sub-sections: first, on ways to combat authoritarian-sponsored disinformation within democracies, and, second, on ways to promote digital media freedom under authoritarian regimes and weak democracies.

[183] Reuters, "Biden Administration Imposes Sweeping Tech Restrictions on China" *The Guardian* (7 October 2022) <https://www.theguardian.com/us-news/2022/oct/07/biden-administration-tech-restrictions-china> accessed 13 November 2022.
[184] Idem
[185] US Bureau of Industry and Security, 'Iran' (*US Bureau of Industry and Security*) <https://www.bis.doc.gov/index.php/policy-guidance/country-guidance/sanctioned-destinations/iran> accessed 28 November 2022.
[186] House, "Fact Sheet: Export Controls and Human Rights Initiative Launched at the Summit for Democracy" (*The White House*, 10 December 2021) <https://www.whitehouse.gov/briefing-room/statements-releases/2021/12/10/fact-sheet-export-controls-and-human-rights-initiative-launched-at-the-summit-for-democracy/> accessed 13 November 2022.

3.2.1 Policies to combat authoritarian-sponsored disinformation within democracies

Governments should create more incentives for social media companies to double down on their efforts in identifying disinformation operations carried out through bots and false accounts, as well as in tracking their sources and reporting on their findings. Further action needs to be taken to dismantle said operations and prevent the development of others in the future, by governmental bodies. Failure to fulfil this duty should be accompanied by legal scrutiny and sanctions, including fines on the companies.[187]

In parallel, governments should also set up arms-length bodies (reporting directly to elected officials and media regulators) to identify foreign influence networks sponsored by authoritarian regimes and publicise their findings. Intelligence agency involvement in this process should be limited as far as possible without compromising its effectiveness to prevent the legitimacy of the findings from being undermined by association. In particular, governments should heavily limit intelligence agency involvement in communications with the public on the subject. Such communications should be reduced to facts-based reports of the findings with little to no editorialising.[188]

Government agencies should reach out to and foster collaboration with civil society actors holding expertise on disinformation, including but not limited to media organisations, networks of journalists and academics, by formalising their involvement in the data collection and policymaking processes.

Limiting censorship

Governments should refrain as much as possible from using censorship as a tool for combatting disinformation. *Ceteris paribus*, governments should resort to combatting disinformation by working with social media platforms to empower independent third-party fact-checkers to provide context for false or misleading information.

When censorship is thought unavoidable on national security grounds, governments should ensure that such censorship is (1) targeted (i.e. affects only misleading or false content and not entire media organisations) and (2) time-bound (i.e. is not permanent but conditional on the removal of offending content from the material being censored or otherwise contains sunset provisions[189]). Governments should refrain as much as possible from directly involving themselves in the process of regulating media

[187] See Erol Yayboke and Sam Brannen, "A Strategic Approach to Digital Authoritarianism".
[188] See Emerson T Brooking and Suzanne Kianpour, "Iranian Digital Influence Efforts: Guerrilla Broadcasting for the Twenty-First Century" (*Atlantic Council*, 11 February 2020) <https://www.atlanticcouncil.org/in-depth-research-reports/report/iranian-digital-influence-efforts-guerrilla-broadcasting-for-the-twenty-first-century/> accessed 13 November 2022.
[189] For a discussion of the failure of the EU RT/Sputnik ban to fulfil these procedural criteria, see Adrian Shabhaz, Allie Funk and Kian Vesteinsson, "Freedom on the Net 2022: Countering an Authoritarian Overhaul of the Internet" (*Freedom House*, 2022) <https://freedomhouse.org/report/freedom-net/2022/countering-authoritarian-overhaul-internet> accessed 10 November 2022.

content and uphold the independence of media regulators while extending their jurisdiction over social media where this has not already happened to ensure their effectiveness in the digital age.

Fact-checking and multi-stakeholder cooperation

Social media companies should increase their commitment to collaborating with independent third-party fact-checkers by fast-tracking and investing more resources into the development of new and effective procedures to streamline the fact-checking process. This should be carried out in an equitable manner by making the content screening process and any features providing additional context or flagging false or misleading content available in as many jurisdictions simultaneously as early as possible.

Governments should engage with civil society actors and businesses through international fora such as the Freedom Online Coalition and the Tech for Democracy initiative to create and circulate an International Digital Content Moderation Code of Conduct (IDCMCC) laying out best practices in content moderation on digital platforms, which would provide a yardstick by which to evaluate the practices of social media operators. In elaborating the IDCMCC, all parties should refer to existing international human rights instruments, including the UN Guiding Principles on Business and Human Rights. Social media companies declining to commit to incorporating and following the IDCMCC in their internal procedures should be pressured to do so through political means, including public statements by the FOC or parliamentary and congressional hearings.

Social media companies should refrain from automating the content moderation process. To ensure due process, streamlining internal content moderation procedures should lead to a speedier referral of flagged content to content moderators or independent fact-checkers and not to automated removal or "shadow banning" of content.

Increased media literacy

Governments should work with civil society groups, academics and journalists do devise programmes to improve media literacy and increase awareness about the most common types of state-sponsored online disinformation. Governmental involvement should be limited to providing resources to and guaranteeing a platform for these media literacy programmes, while eschewing any substantive role in order to pre-empt accusations of politicisation.

Similarly, social media companies should engage with civil society stakeholders to devise new features and resources that can be easily integrated into and accessed by users on social media platforms. Policymakers should carefully track developments in this area to ensure speedy execution. Tools of political pressure, such as statements by the FOC or parliamentary and congressional hearings, could prove useful in ensuring that social media companies live up to their responsibilities.

3.2.2 Promoting digital media freedom under authoritarian regimes and weak democracies

Gauging the size of the problem, enhancing data collection and improving awareness

Governments should require businesses exporting surveillance and censorship technologies at risk of being employed to restrict human rights under authoritarian regimes and weak democracies to report annually on the impacts of their exports.[190] This obligation should be grounded in the UN Guiding Principles on Business and Human Rights, more specifically, in the due diligence obligations of businesses. These reports should include an assessment of the likely contribution that the exported technologies may have had in allowing governments to conduct surveillance and enact censorship, as well as a review of the measures put in place by businesses to mitigate the risks associated with the supply of said technologies.

Lastly, these reports should constitute the subject of parliamentary and congressional hearings and debates to ensure adequate scrutiny. Parallel assessments of the impacts of such technological exports should be carried out by governmental bodies in situations deemed to be of particular importance to national security or where there are serious suspicions of inaccuracy with respect to the reports issued by businesses themselves. Social media companies should document government demands for service shutdowns across the world and make the public aware of such demands through notices displayed on their platforms, particularly in countries where government transparency is lacking.[191]

Promoting multilateralism and supporting civil society

Governments should dedicate more institutional and financial resources to the consolidation of international fora committed to the promotion of media freedom on the Internet, such as the Freedom Online Coalition and the Tech for Democracy initiative, while also coordinating with partners with shared values to advance the fight against digital authoritarianism in the UN ecosystem, particularly within the Internet Governance Forum. In particular, governments should seek to increase the name recognition and global notoriety of the FOC, TFD and other similar initiatives by publicising their activity to a wider public on social media and by organising more outreach events. Additionally, governments should pursue the expansion of the membership of these fora as a key objective, with the

[190] See Adrian Shabhaz, Allie Funk and Kian Vesteinsson, "Freedom on the Net 2022: Policy Recommendations" (*Freedom House*, 2022) <https://freedomhouse.org/report/freedom-net/2022/countering-authoritarian-overhaul-internet/policy-recommendations> accessed 10 November 2022.
[191] Idem

aim of including more states in the institutional architecture of organisations that are likely to shape their conduct with respect to human rights in a positive manner. However, this should only be done after adequate consultation with relevant stakeholders already involved in the initiatives and with a view to ensuring that new members will prove an asset for institutional development.[192]

More generally, like-minded governments should seek to act in concert and consultation with one another rather than pursuing differentiated national strategies in the fight against digital authoritarianism. The US, the EU, the UK, Japan and others should ensure that their individual policy responses do not run counter to the interests of their allies and that they can expect to receive support in their separate efforts, in order to prevent conflict and maximise effectiveness.[193] Governments should also support civil society organisations engaging in strategic litigation in weak democracies in order to hold governments accountable for service shutdowns and other infringements of human rights on the Internet, whilst working to strengthen judicial independence abroad as an autonomous check on government abuses.[194]

Promoting responsible usage of technology and the development of new technological solutions to current problems

Governments should strengthen policies concerning encryption and encourage tech companies to double down on their commitment to secure private communications so as to minimise vulnerabilities that can be weaponised by authoritarian governments and weak democracies in monitoring their citizens. To this end, governments should avoid requiring the introduction of "back doors" or the traceability of messages[195] for ostensible national security and law enforcement purposes.

Governments should also invest in public and private countermeasures to digital repression, including AI, privacy-preserving machine learning and explainable algorithms.[196]Governments should also introduce best practices with respect to Internet protocol security in procurement rules to incentivise large market players seeking government contracts to change their behaviour and subsequently generate a virtuous cycle in the tech sector.[197]

Policymakers should introduce or strengthen high-tech export controls to countries with a track record of human rights abuses on the Internet to undermine governments' capacity to carry out surveillance. In conjunction with this, governments should introduce sanctions on businesses that supply surveillance

[193] See also Erol Yayboke and Sam Brannen, "A Strategic Approach to Digital Authoritarianism".
[193] See also Erol Yayboke and Sam Brannen, "A Strategic Approach to Digital Authoritarianism".
[194] See Adrian Shabhaz, Allie Funk and Kian Vesteinsson, "Freedom on the Net 2022: Policy Recommendations" (*Freedom House*, 2022) <https://freedomhouse.org/report/freedom-net/2022/countering-authoritarian-overhaul-internet/policy-recommendations> accessed 10 November 2022.
[195] See also Erol Yayboke and Sam Brannen, "A Strategic Approach to Digital Authoritarianism".
[196] Idem
[198] See Alina Polyakova and Chris Meserole, "Exporting Digital Authoritarianism: The Russian and Chinese Models".

or dual-use equipment to countries officially designated as "digital authoritarian"[198] and fail to exercise adequate due diligence, in accordance with the UN Guiding Principles on Business and Human Rights. Designating states as "digital authoritarian" should be done in accordance with a clear set of criteria established in consultation with civil society and should, as far as possible, be done in an equitable manner, without exceptions or ad hoc waivers of the sanctions for friendly states. Consistently applying the designation is a necessary step to avoid accusations of politicisation. Lastly, governments should avoid unilaterally pursuing export controls without prior consultation with allies, in order to ensure that the objectives of said export controls are not undermined by the lack of coordination.

Articulating and promoting an alternative vision of the Internet

Governments should intensify efforts to articulate and promote a positive alternate vision of the Internet that is sensitive to the human rights implications of digital communications, while being open to inputs from the private sector and civil society. Diplomacy should play an important role in promoting this vision, particularly in weak democracies, in order to counter the propagation of digital authoritarianism. Central to this vision should be an ethos of leading by example, specifically by eschewing tactics and policy instruments associated with digital authoritarian states such as censorship or mass surveillance.[199]

3.3 Conclusion

The existing policy framework aimed at combatting state-sponsored disinformation and the spread of digital authoritarianism offers some promising tools for the promotion of media freedom and an open, decentralised Internet. The authors believe that, by pursuing the policy recommendations laid out above, sustained progress can be made towards achieving these objectives. Multi-stakeholder engagement, coordination between states with shared values and the continued investment of institutional and financial resources are essential to realising a positive vision of the Internet that acknowledges and upholds its potential to expand human rights in the digital age.

[198] See Alina Polyakova and Chris Meserole, "Exporting Digital Authoritarianism: The Russian and Chinese Models".
[199] See also Erol Yayboke and Sam Brannen, "A Strategic Approach to Digital Authoritarianism".

Bibliography

Adler, E., & Drieschova, A. (2021). The Epistemological Challenge of Truth Subversion to the Liberal International Order. *International Organization, 75*(2), 359-386.

AFP. (2022, April 5). Satellite Images Show Bodies in Bucha for Weeks, Rebutting Moscow Claim. The Moscow Times. https://www.themoscowtimes.com/2022/04/05/satellite-images-show-bodies-in-bucha-for-weeks-rebutting-moscow-claim-a77211

AFP. (2022, March 1). *Russia Blocks 2 Independent Media Sites Over War Coverage*. The Moscow Times. https://www.themoscowtimes.com/2022/03/01/russia-blocks-2-independent-media-sites-over-war-coverage-a76693

AlJazeera: "Rooted in NATO": Iran responds to Russia"s Ukraine attack: Maziar Motamedi: 24 February 2022:https://www.aljazeera.com/news/2022/2/24/rooted-in-nato-inside-irans-response-to-the-ukraine-crisis-2

Al-Jazeera: Centre for Studies: "The role of Iran"s regional media in its soft war policy": 16 February 2017: https://studies.aljazeera.net/en/reports/2017/02/role-irans-regional-media-soft-war-policy-170216114010915.html

Al-Jazeera: Iran"s Khamenei: "Mafia regime" of US created Ukraine crisis: Maziar Motamedi: 1 March 2022: https://www.aljazeera.com/news/2022/3/1/iran-khamenei-ukraine-war-russia-us-policies-nato

Al-Jazeera: Do not call Ukraine invasion a 'war', Russia tells media, schools. (2022, March 2) https://www.aljazeera.com/news/2022/3/2/do-not-call-ukraine-invasion-a-war-russia-tells-media-schools

Alliance for securing democracy: How Russia, China, and Iran have shaped and manipulated coronavirus vaccine narratives: 6 March 2021: Bret Schafer, et al., https://securingdemocracy.gmfus.org/russia-china-iran-covid-vaccine-disinformation/

Amnesty International. 'Russian Journalists Are Being Silenced to Stifle Reporting of Protests', 24 November 2022. https://www.amnesty.org/en/latest/news/2022/11/russia-journalists-and-independent-monitors-being-silenced-to-stifle-reporting-of-protests-new-report/.

An Analysis of the Social-Media Technology, Tactics, and Narratives Used to Control Perception in the Propaganda War Over Ukraine: KJ Boyte: Journal of Information Warfare , Vol. 16, No. 1 (Winter 2017), pp. 88-111

Anderson, J. (2006) "The Chekist Takeover of the Russian State", *International Journal of Intelligence and CounterIntelligence,* 19:2, pp. 237-288

Atlantic Council: As the world shuns Russia over its invasions of Ukraine, Iran strengthens its ties with Moscow: 7 March 2022: Nicole Grajewski: https://www.atlanticcouncil.org/blogs/iransource/as-the-world-shuns-russia-over-its-invasion-of-ukraine-iran-strengthens-its-ties-with-moscow%EF%BF%BC/

Atlantic Council: Iranian digital influence efforts: Guerrilla broadcasting for the twenty-first century: Emerson Brooking and Suzanne Kianpour: 11 February 2022: https://www.atlanticcouncil.org/in-depth-research-reports/report/iranian-digital-influence-efforts-guerrilla-broadcasting-for-the-twenty-first-century/

Atlantic Council: The Ukraine war has made Iran and Russia allies in economic isolation: Alam Saleh and Zakiyeh Yazdanshenas: 25 August 2022: https://www.atlanticcouncil.org/blogs/iransource/the-ukraine-war-has-made-iran-and-russia-allies-in-economic-isolation-heres-how/

Authoritarian states and internet social media: instruments of democratisation or instruments of control? *Kalliopi kyriakopoulou: human affairs* 21, pp. 18–26, 2011

Axios: Iran"s protests spark wider adoption of anti-censorship tools: 30 September 2022: https://www.axios.com/2022/09/30/iran-protests-vpn-google-jigsaw-outline

Ayalew YE, "From Digital Authoritarianism to Platforms" Leviathan Power: Freedom of Expression in the Digital Age under Siege in Africa" (2021) 15 Mizan Law Review 455

Bandurski, D. (2022) “China and Russia are Joining Forces to Spread Disinformation”, Brookings, URL: https://www.brookings.edu/techstream/china-and-russia-are-joining-forces-to-spread-disinformation/ (14/11/2022)

Baranovsky-Dewey, A. (2019). Determinants of the Timing and Intensity of Propaganda Attacks: Russia"s Information Offensives in Georgia and Ukraine. *St Antony"s International Review*, *14*(2), 121–137.

Batchelor & Zhang Eds. (2017) *China-Africa Relations – Building Images through Cultural Cooperation, Media Representation and Communication*, Routledge

Bettiza, S., & Khomenko, S. (2022, June 15). Babushka Z: The woman who became a Russian propaganda icon. *BBC*. https://www.bbc.co.uk/news/world-europe-61757667

Bloomberg и CNN приостанавливают работу в России. (2022, March 5). Mediazona. https://zona.media/news/2022/03/04/bloomberg_cnn

Bluhm M, "Biden"s Hugely Consequential High-Tech Export Ban on China, Explained by an Expert" (*Vox*, 5 November 2022) <https://www.vox.com/world/2022/11/5/23440525/biden-administration-semiconductor-export-ban-china> (Accessed 13 November 2022)

Bodrunova, S. S. (2021). Information disorder practices in/by contemporary Russia. In H. Tumber & S. Waisbord (Eds.), *The Routledge Companion to Media Disinformation and Populism* (pp. 279–289). Routledge.

Boyte, (2017), "An Analysis of the Social-Media Technology, Tactics, and Narratives Used to Control Perception in the Propaganda War Over Ukraine", *Journal of Informational Warfare*, vol.16, issue.1

Boyte, K. (2017). An Analysis of the Social-Media Technology, Tactics, and Narratives Used to Control Perception in the Propaganda War Over Ukraine. *Journal of Information Warfare*, *16*(1), 88–111.

Brooking ET and Kianpour S, "Iranian Digital Influence Efforts: Guerrilla Broadcasting for the Twenty-First Century" (*Atlantic Council*, 11 February 2020) <https://www.atlanticcouncil.org/in-depth-research-reports/report/iranian-digital-influence-efforts-guerrilla-broadcasting-for-the-twenty-first-century/> (Accessed 13 November 2022)

Burns, A, and Eltham, B. 2009. Twitter Free Iran: An Evaluation of Twitter"s Role in Public Diplomacy and Information Operations in Iran’s 2009 Election Crisis. *Communications Policy & Research Forum 2009*. Sydney: University of Technology.

Celikates, de Kloet, Peeren and Poell eds.Global Cultures of Contestation (London: Palgrave MacMillan. 2017)

Chadwick, A. &. Howard, P.N Eds. (2008) *Routledge Handbook of Internet Politics*, Routledge

Christensen, C. (2011) Twitter Revolutions? Addressing Social Media and Dissent, The Communication Review, 14:3, 155-157: https://www.tandfonline.com/doi/full/10.1080/10714421.2011.597235

Cook, S. (2022) “Beijing"s Global Media Influence 2022 – Authoritarian Expansion and the Power of Democratic Resilience”, *Freedom House*, URL: https://freedomhouse.org/report/beijing-global-media-influence/2022/authoritarian-expansion-power-democratic-resilience (15/10/2022)

Covington, SR. (2016). “The Culture of Strategic Thought Behind Russia’s Modern Approaches to Warfare”. *Harvard Kennedy School Belfer Centre.* Pp. 1-64

Dehghan, Saeed Kamali. 2016. Telegram: The Instant Messaging App Freeing up Iranians" Conversations. *The Guardian*, 8 February. https://www.theguardian.com/world/2016/feb/08/telegram-the-instant-messaging-app-freeing-up-iranians-conversations.

Diepeveen, S., Borodyna, O., & Tindall, T. (2022, March 11). *A war on many fronts: Disinformation around the Russia-Ukraine war*. ODI. https://odi.org/en/insights/a-war-on-many-fronts-disinformation-around-the-russia-ukraine-war/ (Accessed 12 January 2023)

Dryzek, J. S., & Holmes, L. T. (2002). Post-Communist Democratization. Cambridge University Press.

Dwoskin E, ‘Misinformation on Facebook Got Six Times More Clicks than Factual News during the 2020 Election, Study Says’ *Washington Post* (10 September 2021) <https://www.washingtonpost.com/technology/2021/09/03/facebook-misinformation-nyu-study/> accessed 28 November 2022

E.C. Economy (2018) “The Great Firewall of China – Xi Jinping"s Internet Shutdown”, *the Guardian*, URL: https://www.theguardian.com/news/2018/jun/29/the-great-firewall-of-china-xi-jinpings-internet-shutdown (08/11/2022)

Echo of Moscow fined for linked content in blog on its website. (2018, April 27). Reporters Without Borders. https://rsf.org/en/echo-moscow-fined-linked-content-blog-its-website

Engler A, "The Declaration for the Future of the Internet Is for Wavering Democracies, Not China and Russia" (*Brookings*, 9 May 2022) <https://www.brookings.edu/blog/techtank/2022/05/09/the-

declaration-for-the-future-of-the-internet-is-for-wavering-democracies-not-china-and-russia/> accessed 10 November 2022

Essa, A. (2018) "China is Buying African Media"s Silence", *Foreign Policy*, URL: https://foreignpolicy.com/2018/09/14/china-is-buying-african-medias-silence/ (12/10/2022)

European Council on Foreign Relations: Suspicious bind: Iran"s relationship with Russia: Faezeh Foroutan: 2 September 2022: https://ecfr.eu/article/suspicious-bind-irans-relationship-with-russia/

EUvsDisinfo. (2016, September 30). *Nine Ways to Confuse Us About MH17*. https://euvsdisinfo.eu/nine-ways-to-confuse-us-about-mh17/

EUvsDisinfo. (2023, March 31). The Bucha massacre: Mapping a year of Kremlin denial. EUvsDisinfo. https://euvsdisinfo.eu/the-bucha-massacre-mapping-a-year-of-kremlin-denial/

Federal Service for Supervision of Communications, Information Technology and Mass Media. (n.d.). Government of the Russian Federation. Retrieved 6 June 2023, from http://government.ru/en/department/58/

Fikra Forum Policy Analysis: Threats to Iranian Instagram: Analysing Iran"s Internet Landscape: 24 November 2021: https://www.washingtoninstitute.org/policy-analysis/threats-iranian-instagram-analyzing-irans-internet-landscape

Foreign Policy: Kourosh Ziabari: 9 March 2022: https://foreignpolicy.com/2022/03/09/iran-support-russia-war-ukraine/

Freedom House (2022) "Beijing"s Global Media Influence 2022 – Country Reports", URL: https://freedomhouse.org/report/beijing-global-media-influence/2022/authoritarian-expansion-power-democratic-resilience/country-reports (12/11/2022)

Freedom House (2022) "Beijing"s Global Media Influence 2022 – Taiwan", URL: https://freedomhouse.org/country/taiwan/beijings-global-media-influence/2022 (12/11/2022)

Freedom House (2022) "China – Freedom of the Net 2022 Country Report", URL: https://freedomhouse.org/country/china/freedom-net/2022 (08/11/2022)

Freedom House: Iran: Transnational repression origin country case study: Special report 2021: https://freedomhouse.org/report/transnational-repression/iran

Freedom House: The true depth of Iran"s online repression: 2 December 2019: Amy Slipowitz: https://freedomhouse.org/article/true-depth-irans-online-repression

Freedom Online Coalition, "Founding Declaration of the Freedom Online Coalition" <https://freedomonlinecoalition.com/document/the-founding-declaration-freedom-online-joint-action-for-free-expression-on-the-internet/> accessed 11 November 2022

Galeotti, (2021), *New National Security Strategy Is a Paranoid"s Charter*, The Moscow Times, [https://www.themoscowtimes.com/2021/07/05/new-national-security-strategy-is-a-paranoids-charter-a74424]

Gamso, J. (2021) Is China exporting Media Censorship? China"s Rise, Media Freedoms, and Democracy, *European Journal of International Relations*, Vol. 27, No. 3

Galeotti, M. (2019). *We Need to Talk About Putin: How the West Gets Him Wrong*. Ebury Press:London

Gavin, J. (2022). *Information and Misinformation in the Russia Ukraine War*. Vision of Humanity. https://www.visionofhumanity.org/information-and-misinformation-in-the-russia-ukraine-war/

Geranmayeh, Ellie, and Kadri Liik. THE NEW POWER COUPLE: RUSSIA AND IRAN IN THE MIDDLE EAST. European Council on Foreign Relations, 2016. https://www.jstor.org/stable/resrep21586?searchText=iran+media&searchUri=%2Faction%2FdoBasicSearch%3FQuery%3Diran%2Bmedia&ab_segments=0%2Fbasic_search_gsv2%2Fcontrol&refreqid=fastly-default%3A5b5a37db89f9acc44a5bd705ed6ddabe#metadata_info_tab_contents

Gerasimov, V. (2016) "The Value of Science in Foresight", *Military Review*, pp.24-29

Gill, G. and Young, J., *Routledge Handbook of Russian Politics and Society* (London: Routledge, 2012)

Global Affairs Canada, "Statement on Behalf of Canada, Chair of the Freedom Online Coalition: A Call to Action on State-Sponsored Disinformation in Ukraine" (*Freedom Online Coalition*, 2 March 2022) <https://freedomonlinecoalition.com/statement-on-behalf-of-canada-chair-of-the-freedom-online-coalition-a-call-to-action-on-state-sponsored-disinformation-in-ukraine/> accessed 12 November 2022

Global Times (2022) "China has 1.032 billion internet users, 73.0% penetration rate", URL: https://www.globaltimes.cn/page/202202/1253226.shtml (08/11/2022)

Global Witness, 'TikTok and Facebook Fail to Detect Election Disinformation in the US, While YouTube Succeeds' (*Global Witness*, October 2022) <https:///en/campaigns/digital-threats/tiktok-and-facebook-fail-detect-election-disinformation-us-while-youtube-succeeds/> accessed 28 November 2022

Godzimirski (2000) Russian national security concepts 1997 and 2000: A comparative analysis, European Security, 9:4

GreatFire.org (2022) "Censorship of Alexa Top 1000 Domains in China", URL: https://en.greatfire.org/search/alexa-top-1000-domains (09/11/2022)

Güneş Murat Tezcür (2012) Democracy promotion, authoritarian resiliency, and political unrest in Iran, Democratization, 19:1, 120-140

Harold & Nader (2012) "China and Iran – Economic, Political and Military Relations", *Rand Corporation*

Hassid, A. (2008) "Controlling the Chinese Media – An Uncertain Business", *Asian Survey*, Vol. 48, No. 3

Hindman M and Barash V, 'Disinformation, "Fake News" and Influence Campaigns on Twitter' (*Knight Foundation*) <https://www.knightfoundation.org/features/misinfo> accessed 28 November 2022

House, "Fact Sheet: Export Controls and Human Rights Initiative Launched at the Summit for Democracy" (*The White House*, 10 December 2021) <https://www.whitehouse.gov/briefing-room/statements-releases/2021/12/10/fact-sheet-export-controls-and-human-rights-initiative-launched-at-the-summit-for-democracy/> accessed 13 November 2022

Illiarionov, A. (2009) "Reading Russia: The Siloviki in Charge", *Journal of Democracy*, 20:2, pp.69-72

Ilya Yablokov, Open Democracy. 'Russian Journalism's Double White Lines'. Accessed 16 December 2022. https://www.opendemocracy.net/en/odr/russian-media-s-double-white-lines/

Institute for Economics & Peace. (2022). *World Risk Poll: Spotlight on Ukraine and Russia* (The Institute for Economics & Peace Briefing Series). https://www.visionofhumanity.org/wp-content/uploads/2022/06/GPI-2022-Briefing-WRP-Ukraine-Russia-web-1.pdf

Iran and the West: Mahmood Sariolghalam: Horizons: Journal of International Relations and Sustainable Development , No. 16, Pandemics & Geopolitics: The Quickening (SPRING 2020), pp. 160-167: https://www.jstor.org/stable/48573757#metadata_info_tab_contents

Iranian Media: Centralised Control and Tattered Accountability. In Karmasin, M, T. Eberwein, & S. Fengler (Eds.) 2021. Global Handbook for Media Accountability. London: Routledge

Kalathil & Boas (2001) "The Internet and State Control in Authoritarian Regimes – China, Cuba and the Counterrevolution", *First Monday*, Vol. 6, Carnegie Endowment for International Peace

Keenan C, "An Update on Our Work to Counter Misinformation" (*Newsroom | TikTok*, 28 September 2022) <https://newsroom.tiktok.com/en-us/an-update-on-our-work-to-counter-misinformation> accessed 12 November 2022

Kemp, S. (2022) "Digital 2022 – Global Overview Report", *Datareportal*, URL: https://datareportal.com/reports/digital-2022-global-overview-report (08/11/2022)

Khorrami, N. (2022) "How China Boosts Iran"s Digital Crackdown", *the Diplomat*, URL: https://thediplomat.com/2022/10/how-china-boosts-irans-digital-crackdown/ (14/11/2022)

Kirchberger, Sinjen, Wörmer Eds. (2022) *Russia-China Relations – Emerging Alliance or Eternal Rivals*, Springer

Kliman, Kendall-Taylor, Lee, Fitt & Nietsche (2020) "Digital Influence Tools Used by China and Russia", *Center for a New American Security*

Kovalev, A. (2021). The political economics of news making in Russian media: Ownership, clickbait and censorship. *Journalism*, *22*(12), 2906–2918.

Kovalev, Alexey. 'In Putin's Russia, the Hollowed-out Media Mirrors the State'. *The Guardian*, 24 March 2017, sec. Opinion. https://www.theguardian.com/commentisfree/2017/mar/24/putin-russia-media-state-government-control.

Kumar, R. (2021) "How China uses the News Media as a Weapon in its Propaganda War against the West", *Reuters Institute for the Study of Journalism*, URL: https://reutersinstitute.politics.ox.ac.uk/news/how-china-uses-news-media-weapon-its-propaganda-war-against-west (15/10/2022)

Kusa, I. (2022) "China"s Strategic Calculations in the Russia-Ukraine War", Wilson Center, URL: https://www.wilsoncenter.org/blog-post/chinas-strategic-calculations-russia-ukraine-war (14/11/2022)

Kyriakopoulou, K. (2011) "Authoritarian States and Internet Social Media – Instruments of Democratisation or Instruments of Control?", *Human Affairs*, Vol. 21

Kyza EA and others, "Combating Misinformation Online: Re-Imagining Social Media for Policy-Making" (2020) 9 Internet Policy Review <https://policyreview.info/articles/analysis/combating-misinformation-online-re-imagining-social-media-policy-making> accessed 10 November 2022

Landen, X. (2022, February 26). *Russia Tells Media to Delete Stories Mentioning Ukraine "Invasion"*. Newsweek. https://www.newsweek.com/russia-tells-media-delete-stories-mentioning-ukraine-invasion-1682973

Lewis, Williams and Franklin, (2008), "Four Practices and An Explanation", *Journalistic Practice*, vol.2, issue.1

Lewis & T. Gardner (2022) "Russia Vetoes UN Resolution on Proclaimed Annexations, China Abstains", *Reuters*, URL: https://www.reuters.com/world/us-act-un-friday-russias-proclaimed-annexations-ukraine-blinken-2022-09-30/ (14/11/2022)

Lorentzen, P. (2014) "China"s Strategic Censorship", *American Journal of Political Science*, Vol. 58, No. 2

Lunden, I. (2014a, April 1). *Pavel Durov Resigns As Head Of Russian Social Network VK.com, Ukraine Conflict Was The Tipping Point*. TechCrunch. https://techcrunch.com/2014/04/01/founder-pavel-durov-says-hes-stepped-down-as-head-of-russias-top-social-network-vk-com/

Lunden, I. (2014b, April 22). *Durov, Out For Good From VK.com, Plans A Mobile Social Network Outside Russia*. https://techcrunch.com/2014/04/22/durov-out-for-good-from-vk-com-plans-a-mobile-social-network-outside-russia/?guccounter=1

MacCarthy M, "Why a Push to Exclude Russian State Media Would Be Problematic for Free Speech and Democracy" (*Brookings*, 14 April 2022) <https://www.brookings.edu/blog/techtank/2022/04/14/why-a-push-to-exclude-russian-state-media-would-be-problematic-for-free-speech-and-democracy/> accessed 13 November 2022

MacFarlane (2003), "Russian Perspectives on Order and Justice", in Foot, Gaddis and Hurrell, ed., *Order and Justice in International Relations,* (Oxford University Press)

Meedan 2020. 2020 Misinfodemic Report: COVID-19 in Emerging Economies

Metzger and Flanigan, Credibility and trust of information in online environments: The use of cognitive heuristics, *Journal of Pragmatics*, vol.59, (2013)

Milmo D and editor DMG technology, "Facebook Takes down Ukraine Disinformation Network and Bans Russian-Backed Media" *The Guardian* (28 February 2022) <https://www.theguardian.com/technology/2022/feb/28/facebook-takes-down-disinformation-network-targeting-ukraine-meta-instagram> accessed 12 November 2022

Mischke, J. (2017, November 10). Russia to amend law to classify media as 'foreign agents'. POLITICO. https://www.politico.eu/article/russia-to-amend-law-to-classify-media-as-foreign-agents/

Mok, C. (2022) "China and Russian Want to Rule the Global Internet", the Diplomat, URL: https://thediplomat.com/2022/02/china-and-russia-want-to-rule-the-global-internet/ (14/11/2022)

Moonakal, N.A. (2022) "The Impact and Implications of China"s Growing Influence in the Middle East", *The Diplomat*, URL: https://thediplomat.com/2022/07/the-impact-and-implications-of-chinas-growing-influence-in-the-middle-east/ (14/11/2022)

Morozov, E. Net Delusion: The Dark Side of Internet Freedom.

Mosseri A, "Working to Stop Misinformation and False News" (*Working to Stop Misinformation and False News | Meta for Media*, April 2017) <https://www.facebook.com/formedia/blog/working-to-stop-misinformation-and-false-news> accessed 12 November 2022

Mpoke B. M. (2022, September 13). *Russia invaded Ukraine more than 200 days ago. Here is one key development from every month of the war.* The New York Times. https://www.nytimes.com/article/ukraine-russia-war-timeline.html

Mueller and the US Department of Justice, *Report On The Investigation Into Russian Interference In The 2016 Presidential Election*, (2019)

Myers, M. (2018) "China"s Belt and Road Initiative – What Role for Latin America?", *Journal of Latin American Geography*, Vol. 17, No. 2

Nguyen M, Subramanya R and Garson M, "Moving Away from Fight or Flight: Key Lessons from China"s Tech Regulation" (*Institute for Global Change*, 13 October 2022) <https://institute.global/policy/moving-away-fight-or-flight-key-lessons-chinas-tech-regulation> accessed 10 November 2022

Olga Razumvoskaya 'Russian News Editor Fired Over Ukrainian Nationalist Interview - WSJ', March 2014, Accessed 15 December 2022. https://www.wsj.com/articles/BL-NEB-7445.

Oxford Internet Institute: Understanding Online Misinformation in Iran, the Epicentre of the Coronavirus in the Middle East: 24 June 2020: Mahsa Alimardani and Mona Elswah:

https://www.oii.ox.ac.uk/news-events/news/understanding-online-misinformation-in-iran-the-epicentre-of-coronavirus-in-the-middle-east/
Paul and Matthews, "The Russian "Firehose of Falsehood" Propaganda Model", *Rand Corporation*, (2016)
Petrov, N., Lipman, M., & Hale, H. E. (2014). Three dilemmas of hybrid regime governance: Russia from Putin to Putin. Post-Soviet Affairs, 30(1), 1–26.
Poell, Thomas, et al. 2016. Protest Leadership in the Age of Social Media. *Information, Communication & Society* 19(7): 994-1014.
Polianska, A. (2022, September 2). A History of Defamation: Key Russian Narratives on Ukrainian Sovereignty. EUvsDisinfo. https://euvsdisinfo.eu/a-history-of-defamation-key-russian-narratives-on-ukrainian-sovereignty-2/
Political Self-Censorship in Authoritarian States: The Spatial-Temporal Dimension of Trouble: Charles Chang and Melanie Manion: Comparative Political Studies 2021, Vol. 54(8) 1362–1392
Politico: Russia eyes Iran as sanctions-busting backdoor for oil sales: 23 August 2022: Mathew Karnitsching: https://www.politico.eu/article/russia-eyes-iran-as-sanctions-busting-backdoor-for-oil-sales/
Polyakova A and Meserole C, "Exporting Digital Authoritarianism: The Russian and Chinese Models"
Press-Freedom Watch: Repression Goes Digital: Joel Simon: https://sites.uni.edu/fabos/thc/cjrarticle.pdf
Pynnöniemi, K., (2021) 'Information-Psychological Warfare in Russian Security Strategy', in Roger Kanet (eds), *Routledge Handbook of Russian Security*, (Abingdon: Routledge)
Ramsey and Robertshaw, "Weaponising News, RT, Sputnik and targeted disinformation", *King"s College London Centre for the Study of Media, Communication & Power*, (2018)
Ramsey, G. and Robertshaw, S. (2018). 'Weaponising News, RT, Sputnik and targeted disinformation', *King's College London Centre for the Study of Media, Communication & Power*, pp. 1-140
Reporters Without Borders: Iran: https://rsf.org/en/country/iran
Reuters, "Biden Administration Imposes Sweeping Tech Restrictions on China" *The Guardian* (7 October 2022) <https://www.theguardian.com/us-news/2022/oct/07/biden-administration-tech-restrictions-china> accessed 13 November 2022
Reuters: Special Report: How Iran spreads disinformation around the world: 30 November 2018: Jack Stubbs and Christopher Bing: https://www.reuters.com/article/us-cyber-iran-specialreport-idUSKCN1NZ1FT
Rid, T., *Active Measures* (Profile Books, 2020).
Roberts, M.E. (2018) *Censored – Distraction and Diversion Inside China"s Great Firewall*, Princeton University Press
Ronald J. Deibert. 14 Aug 2008, *The geopolitics of internet control from:* Routledge Handbook of Internet Politics Routledge
Ronan, G. (2020), *Tomas Schuman Yuri Bezmenov LA 1983 YouTube*, https://www.youtube.com/watch?v=Or9CeuqcfMY, [Accessed 20/7/22]
Rosen G, "How We"re Tackling Misinformation Across Our Apps" (*Meta*, 22 March 2021) <https://about.fb.com/news/2021/03/how-were-tackling-misinformation-across-our-apps/> accessed 12 November 2022
RUSI: Friends with benefits: Iran and Russia after the Ukraine invasion: Dr Aniseh Bassiri Tabrizi: 22 July 2022: https://rusi.org/explore-our-research/publications/commentary/friends-benefits-iran-and-russia-after-ukraine-invasion
Russia Criminalizes Independent War Reporting, Anti-War Protests. (2022, March 7). Human Rights Watch. https://www.hrw.org/news/2022/03/07/russia-criminalizes-independent-war-reporting-anti-war-protests
Russia: Opposition politician Ilya Yashin sentenced to eight and half years in jail for denouncing Russia's war crimes in Ukraine. (2022, December 9). Amnesty International. https://www.amnesty.org/en/latest/news/2022/12/russia-opposition-politician-ilya-yashin-sentenced-to-eight-and-half-years-in-jail-for-denouncing-russias-war-crimes-in-ukraine/
Rutland, P. (2017) 'The Political Elite in Post-Soviet Russia', in Heinrich Best and John Higley (eds), *The Palgrave Handbook of Political Elites,* (Basingstoke, Palgrave Macmillan)
Scarr, F., & Ahmedzade, T. (2023, April 7). The talk-show hosts telling Russians what to believe. BBC. https://www.bbc.co.uk/news/resources/idt-4af5a2e0-10d4-4d4f-b3bb-41e2d1fe35dd
Schimpfossl, E., & Yablokov, I. (2014). Coercion or conformism? Censorship and self-censorship among Russian media personalities and reporters in the 2010s. Demokratizatsiya: The Journal of Post-Soviet Democratization, 22(2), 295–311.

Schimpfossl, E., & Yablokov, I. (2014). Coercion or conformism? Censorship and self-censorship among Russian media personalities and reporters in the 2010s. *Demokratizatsiya: The Journal of Post-Soviet Democratization*, *22*(2), 295–311.

Seibt, S. (2022, May 6). How "Babushka Z" became the unlikely icon of Russian propaganda. *France 24*. https://www.france24.com/en/europe/20220506-how-babushka-z-became-the-unlikely-icon-of-russian-propaganda

Seibt, S. (2022, May 6). How 'Babushka Z' became the unlikely icon of Russian propaganda. France 24. https://www.france24.com/en/europe/20220506-how-babushka-z-became-the-unlikely-icon-of-russian-propaganda

Shabhaz A, Funk A and Vesteinsson K, "Freedom on the Net 2022: Countering an Authoritarian Overhaul of the Internet" (*Freedom House*, 2022) <https://freedomhouse.org/report/freedom-net/2022/countering-authoritarian-overhaul-internet> accessed 10 November 2022

Shandra and Seely, (2019), "The Surkov Leaks, The Inner Workings of Russia"s Hybrid War in Ukraine", *RUSI*

Shchelin, P (2016) "Russian National Security Strategy: Regime Security and Elite's Struggle for 'Great Power' Status", *Slovo*, 28:2, pp.80-90

Sherman J, "The Politics of Internet Security: Private Industry and the Future of the Web" (*Atlantic Council*, 5 October 2020) <https://www.atlanticcouncil.org/in-depth-research-reports/report/the-politics-of-internet-security-private-industry-and-the-future-of-the-web/> accessed 10 November 2022

Smirnova, "Russian TV: Contesting European Values", *University of Oxford*, (2016)

Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises and Office of the High Commissioner on Human Rights, "Guiding Principles on Business and Human Rights. Implementing the United Nations "Protect, Respect and Remedy" Framework" <https://www.ohchr.org/sites/default/files/documents/publications/guidingprinciplesbusinesshr_en.pdf> accessed 12 November 2022

Sterling T, "Dutch Journalists, Rights Group File Lawsuit Challenging EU Ban on RT, Sputnik" *Reuters* (25 May 2022) <https://www.reuters.com/business/media-telecom/dutch-journalists-rights-group-file-lawsuit-challenging-eu-ban-rt-sputnik-2022-05-25/> accessed 13 November 2022

Summary Executions and Attacks on Individual Civilians in Kyiv, Chernihiv, and Sumy Regions in the Context of the Russian Federation's Armed Attack against Ukraine. (2022). Office of the United Nations High Commissioner for Human Rights. https://www.ohchr.org/sites/default/files/2022-12/2022-12-07-OHCHR-Thematic-Report-Killings-EN.pdf

Tass (2022) "Russia and China Call for Internationalization of Internet Governance Statement", URL: https://tass.com/economy/1398177 (14/11/2022)

Tech for Democracy, "Together for an Equal, Just and Democratic Digital World. Action Programme for Tech for Democracy - Civil Society Recommendations" <https://globaltfokus.dk/images//TechForDemocracy/TFD_Action-Programme.pdf> accessed 12 November 2022

The Economist (2022) "As Censorship in China increases, VPNs are becoming more important", URL: https://www.economist.com/china/2022/06/28/as-censorship-in-china-increases-vpns-are-becoming-more-important (10/11/2022)

The United States Institute of Peace: The Iran Primer: "Iran blames US, West for Ukraine war: Garrett Nada: 19 July 2022: https://iranprimer.usip.org/blog/2022/mar/03/iran-blames-us-west-ukraine-war

Tselyu ukrainskoy rakety mog byt" camolet Vladimira Putina [Vladimir Putin"s Plane May Have Been The Target of Ukrainian Missile]. (2014, July 17). *Lifenews*. https://life.ru/p/136833

U.S. Department of State. (2022, January 20). Russia's Top Five Persistent Disinformation Narratives. https://www.state.gov/russias-top-five-persistent-disinformation-narratives/

U.S. Department of State. (2022a, January 20). *Russia"s Top Five Persistent Disinformation Narratives*. https://www.state.gov/russias-top-five-persistent-disinformation-narratives/

U.S. Department of State. (2022b, August 24). *Russia"s War on Ukraine: Six Months of Lies, Implemented*. https://www.state.gov/disarming-disinformation/russias-war-on-ukraine-six-months-of-lies-implemented/

US Bureau of Industry and Security, 'Iran' (*US Bureau of Industry and Security*) <https://www.bis.doc.gov/index.php/policy-guidance/country-guidance/sanctioned-destinations/iran> accessed 28 November 2022

US State Department, "A Declaration for the Future of the Internet" <https://www.state.gov/wp-content/uploads/2022/04/Declaration-for-the-Future-for-the-Internet.pdf> accessed 10 November 2022

Vinokour, Maya. 'Russia's Media Is Now Totally in Putin's Hands'. *Foreign Policy* (blog). Accessed 16 December 2022. https://foreignpolicy.com/2022/04/05/russia-media-independence-putin/.

Vasu, Ang, Teo, Jayakumar, Faizal & Ahuja (2018) "Fake News – National Security in the Post-Truth Era", *S. Rajaratnam School of International Studies*

VOA News: Journalist Arrested in Iran, Warned About Protest Coverage: Jessia Jerreat: 23 September 2022: https://www.voanews.com/a/journalists-arrested-in-iran-warned-about-protest-coverage/6760774.html

Vorobyov, N. (2022, January 31). How are Russian media outlets portraying the Ukraine crisis? *Al Jazeera*. https://www.aljazeera.com/news/2022/1/31/how-are-russian-media-outlets-portraying-the-ukraine-crisis

Wang, Y. (2020) "In China, the "Great Firewall" Is Changing a Generation", *Politico*, URL: https://www.politico.com/news/magazine/2020/09/01/china-great-firewall-generation-405385 (08/11/2022)

Washington Post: What the West should learn from the protests in Iran: Karim Sadjadpour: 24 September 2022: https://www.washingtonpost.com/opinions/2022/09/24/mahsa-amini-hijab-west-biden-iran/

Woolley & Howard Eds. (2018) *Computational Propaganda – Political Parties, Politicians and Political Manipulation on Social Media*, Oxford University Press

Xu B and Albert E, "Media Censorship in China" (*Council on Foreign Relations*, February 2017) <https://www.cfr.org/backgrounder/media-censorship-china> accessed 10 November 2022

Yayboke E and Brannen S, "A Strategic Approach to Digital Authoritarianism"

…

Верховный суд прекратил деятельность сайта «Новой газеты» в качестве СМИ. (2022, September 15). Roskomsvoboda. https://roskomsvoboda.org/post/sayt-novoy-ne-smi/

Послание Президента Федеральному Собранию. (2023, February 21). Президент России. http://kremlin.ru/events/president/news/70565

Путин подписал закон о больших сроках за публикацию альтернативного мнения про военных РФ. (2022, March 5). Roskomsvoboda. https://roskomsvoboda.org/post/15-let-za-kritiku-vsrf/

Российские НКО не хотят быть 'иностранными агентами'. (2012, November 21). BBC News Русская Служба. https://www.bbc.com/russian/russia/2012/11/121121_russia_ngo_agents_debate

Своя правда. Выпуск от 18.11.2022. ОГОЛТЕЛАЯ РУСОФОБИЯ. (2022, November 18). https://www.youtube.com/watch?v=BJJBT_NUorg