

Beyond Disinformation

Identarian Narratives meet Authoritarian Practices, Lawfare & Marketcraft

Table of Contents

<i>Executive Summary</i>	2
<i>Introduction – Situating Disinformation Studies</i>	5
<i>DOMAIN 1 – Identity, Dominance, and Diaspora</i>	6
The Contradictions of Identarian Isolation and Dominance	7
Censorship and Self-Censorship among Diasporas.....	12
Disinformation targeting diasporas.....	15
<i>DOMAIN 2 – Lawfare</i>	18
Domestic Legislation and the Dispossession of Rights	18
The Market and Infrastructure of Digital Lawfare	22
Export of Authoritarian Tools & Narratives.....	23
<i>DOMAIN 3 – Digital Authoritarianism & Non-State Actors</i>	25
Systemic Industrialized Persuasion	25
State Use of Non-State Actors	29
<i>DOMAIN 4 – Marketcraft & Platform Power</i>	31
Data Colonialism and Digital Sovereignty	32
Domestic Platform Regulation.....	35
<i>Conclusion – Best Practices for Responsible Digital Resilience</i>	37
<i>References</i>	39

Faculty Investigators

Dr. Kenzie Burchell, University of Toronto, Principal Investigator¹

Dr. Jennifer Ross, University of Toronto, Co-Investigator

Professor Vera Tolz, University of Manchester, Co-Investigator

Dr. Sherry Yu, University of Toronto, Co-Investigator

Graduate Research Team

John Amundson (Toronto), Ling Ding (Toronto) Haley Forgacs (Toronto), Valérie Kindarji (Toronto), Ruty Korotaev (Toronto), Maksim Markelov (Manchester), Sebastian Rodriguez (Oxford), Sorcha Scarff (Manchester) & Anastasia Zabalueva (Toronto)

With additional support from Dr. Dara Conduit, University of Melbourne
& Professor Stephen Hutchings, University of Manchester

¹Corresponding Author: Kenzie.Burchell@utoronto.ca “Beyond Disinformation” is funded by the Social Sciences and Humanities Research Council in partnership with UK Research and Innovation Arts and Humanities Research Council / “Beyond Disinformation” est financé par le Conseil de Recherches en Sciences Humaines en partenariat avec UK Research and Innovation Arts and Humanities Research Council.

Executive Summary

What lies Beyond Disinformation?

Disinformation is now the status quo. Beyond the facts of the matter—false claims to be fact-checked or governmental narratives to be debunked—broader forces are shaping our everyday informational landscape. These forces reweight and reorder opportunities to speak, engage, express and represent oneself, limiting our capacity to know, understand, and participate in the world around us.

Identity matters as much to this landscape as facts. Repressive legal templates and restrictive economic interventions redefine how we individually or collectively participate in digital life. These changes leave only narrow openings—apertures that permit limited ways of belonging to collective, interpretive communities—while foreclosing so many other possibilities for public life.

By linking these domains of identity, authoritarianism, law and economics, this report demonstrates how such interventions reduce opportunities for local, transnational and global experiences of collective engagement to the strategic needs of governments or the competing commercial imperatives of platform and data economies.

About the Beyond Disinformation Research Cluster

We are media scholars and journalists, area-experts and disinformation specialists – each faculty researcher and graduate team member brings a different set of skills and experiences to bear down on one of the most pressing issues facing fact-based journalism and democratic governance today. We seek to understand rapidly declining institutional trust in liberal democratic institutions and surging populism worldwide while examining the fragmentation of the informational landscape and the polarization of public opinion, ultimately seeking to understand what underlies these shifts—What lies beyond disinformation?

This report is the product of the “Beyond Disinformation” international research cluster, developed through a joint institutional partnership between the Universities of Manchester, Melbourne and Toronto.² Over the Spring and Summer of 2024, our faculty specialists worked with four teams of graduate researchers – examining the impact of identity and diaspora, of authoritarian techniques and templates, of censorship laws, as well as market and platform regulation. We also looked at the role of communication specialists who themselves seek to combat disinformation and establish a context where fact-based certainty and trust flourishes among and across diverse communities. We have contributed to shorter, public, rapid response analyses in collaboration with the AHRC funded “(Mis)Translating Deceit” project and the Centre for Digital Trust and Society at the University of Manchester and the Munk School of Global Affairs and Public Policy at the University of Toronto.³ In October 2024, we came together with our wider network partners to workshop and present our findings at the University of Toronto through a two-day symposium hosted by the

² The wider partnership “Beyond Disinformation: Assessing Digital Communications Strategies of Hybrid Neo-Authoritarian Empires” is led by Dr. Kenzie Burchell (Toronto), Dr. Dara Conduit (Melbourne), and Prof. Stephen Hutchings (Manchester) and funded by the Joint Institutional Partnership program of the participating universities.

³ See “[Workshop on ‘Big Disinfo’ at the University of Manchester](#)” (May 2024) and “[What Trump’s Victory means for Europe and Eurasia](#)” (November 2024).

Munk School's Center for European and Eurasian Studies on the first day and the Faculty of Information on the second.⁴ In January 2025, our key findings were presented to the “Evolving Narratives of Culture and Histories” Knowledge Mobilization Forum for stakeholders and policymakers hosted by the Canadian Government. This report is the product of these successive collaborative efforts, and our work continues.

Key Findings

Identity – Across today's information and media landscape shaped by polarizing political entertainment rather than genuine public discourse—and by social media platforms that amplify conflict while overwhelming spaces for political deliberation—identity is increasingly perceived in terms of isolation and disconnection. We compare how this environment has fostered new forms of collective victimhood that, while empowering and populist, are often rooted in dominant classes, including ethnonationalist majorities and gender, with “manhood” emerging forcefully as a perceived aggrieved identity.

For contrast, we provide a survey of diaspora communities worldwide – examining first how the very definition of diaspora and their difference from others reproduce a politics of nationalism(s) rather than a politics grounded in everyday experiences. Where such social forces are entangled with disinformation, we find communities seeking to forge communicative spaces that reflect their identities, yet often seeking refuge in self-censorship. This constrains the effectiveness of how we speak about and represent ourselves, preventing local experiences and shared cultural memories from translating into opportunities for just and democratic participation.

Lawfare – Globally, there has been a rise in the use of laws, or more precisely, legal templates, as tools for authoritarian experimentation, entrenchment, and export. They are increasingly used to identify and isolate particular communities from participation in political and public life, targeted in a way that mobilizes and incites parts of the wider electorate. This tactic reduces political accountability and suppresses opportunities for public expression while further disenfranchising already marginalized and at-risk individuals, making them targets of abuse and repression by police, security forces and the broader public.

The ambiguity of laws and the quasi-legal rhetoric of government officials plays a significant role in populist politics by legitimizing wider state-led actions targeting marginalized communities. This situation creates opportunities for authoritarian legislative changes, the imposition of harsh criminal penalties, their inconsistent and arbitrary application across all levels of society, allowing public responses to such actions to act as pretexts for additional laws.

Authoritarian Practices – Repressive legal techniques often spread regionally and are shared among aligned illiberal regimes. However, they also circulate globally, initially through the rhetorical templates of disinformation actors in the media and then through the digital tactics of non-state actors working closely with governments to conduct surveillance, harassment and silencing of dissent.

Our analysis of several case studies shows that conventional labels such as “democratic” or “autocratic” can obscure how authoritarian practices operate across the political spectrum worldwide, undermining any attempts for accountability and resulting in a convergence of authoritarian and democratic strategies for legalized surveillance, information manipulation, and repression.

⁴ Many thanks to Dr. Daniel McCarthy (Melbourne) and Dr. Alejandro Paz (Toronto) for their participation and insights.

Marketcraft –Although terms such as “sanctions”, “supply chains”, and “digital sovereignty” have only recently entered popular economic discourse—particularly since the COVID-19 pandemic and following the full-scale invasion of Ukraine in 2022— they represent just a few types of marketcraft. These tools are used to stop and dam the flow of economic power by legally crafting domestic industries to serve geopolitical goals.

In the race to dominate digital, data, and AI-driven economies, increasingly assertive policies are being implemented to impose controls and create divisions. This is fragmenting the global economy and producing various divergent information landscapes. Disinformation flourishes in the gaps between these emerging digital worlds—spaces increasingly defined by competition between states rather than connection between their citizens.

Policy Implications

- Political engagement and informed participation are not one only tied only to elections. They are everyday issues represented in social isolation at the scale individual and socio-economic life, which much be addressed through interpersonal, community and employment opportunities – and by recognizing the impacts when such opportunities are lacking.
- Informational literacy must be mobilized at the national level as part of a comprehensive effort to build digital resilience that connects people beyond their individual information-seeking behaviours or labour market needs.
- Responsible newsmakers, fact-based content creators, educators and community leaders must expand their commitment to accountability. Disinformation flourishes when we fail to identify how persuasion, publicity, and the packaging of information erode trust across the diverse domains of economic and political life – while also recognizing the agenda-setting impact of disinformation when it monopolizes the news cycle.
- Rather than mirroring illiberal practices of repression and censorship, democratic governments must take seriously the creative and participatory potential of our diverse, digital lives— as essential to protecting public participation. When geopolitical, isolationist and market-driven regulatory practices across digital platforms permit non-state actors to limit the nature of public expression and engagement, authoritarian regimes are emboldened, and their techniques are more effective.

Preferred Citation:

Burchell, K., Ross, J., Tolz, V., Yu, S., Amundson, J., Ding L., Forgacs, H., Kindarji, V., Korotaev, R., Markelov, M., Rodriguez, S., Scarff, S. & Zabalueva, A. with Hutchings S. and Conduit, D. (2025). Beyond Disinformation: Identarian Narratives meet Authoritarian Practices, Lawfare & Marketcraft. A Knowledge Synthesis and Policy Report. Universities of Toronto and Manchester.

Introduction – Situating Disinformation Studies

The Internet as an open space with equitable opportunities for participation in public discussion has been repeatedly challenged by various actors exploiting it for their political or commercial gain. These coordinated efforts span multiple countries globally – binary view contrasting “authoritarian” to “liberal democratic” and “hostile actors” to “ordinary users” seems no longer tenable (cf., e.g. Benkler et al., 2018; Hutchings, 2024). Likewise, in the current global information (dis)order, the blurring of boundaries between “national” and “transnational”, “state” and “non-state”, “authentic” and “inauthentic” becomes increasingly apparent (cf., e.g. Wardle & Derakhshan, 2017). This issue is twofold. Firstly, the abundant and ever-growing conceptual and terminological frameworks used to denote distinct phenomena in the digital sphere can create an impression of an epistemic chaos, making it difficult to accurately and clearly delineate specific practices (cf. Gilbert & Mohseni, 2011; Waller, 2024). Secondly, the apparent interconnectedness of a multitude of actors within and across different states, coupled with the opaque mechanisms facilitating these connections and resulting outcomes, calls for a more holistic approach. Such an approach must be capable of comprehending individual experience and complexities of collective identity while recognizing the broader contextual relationships that span legal, market, and geopolitical domains (cf. Rauch, 2021).

Information (dis)order, digital authoritarianism, and transnational authoritarian practices are extremely broad concepts, discussed in vast academic literature and practitioners’ output. To address this, one must acknowledge the dual nature of the terms used to describe and study diverse phenomena pertaining to “information (dis)order”, while avoiding their indiscriminate or over-restrictive application, which might lead to crude generalizations or obfuscations. The existence of grey areas between certain practices, especially in authoritarian contexts insists on caution about projecting the functioning of democratic institutions onto authoritarian regimes and vice versa (cf. Galeotti, 2020; Wardle, 2018). The increasing abuse of digital technologies to spread falsehoods, target individuals, groups, organizations, and institutions has been termed as the “information disorder” (Wardle, 2018; Wardle & Derakhshan, 2017). The main aberrations of the information order in this conceptual framework are misinformation, disinformation, and malinformation (Wardle, 2018). The term “fake news”, which has recently risen to prominence following the 2016 U.S. Presidential election, has been widely criticized for failing to capture the nuanced and complex nature of the modern information ecosystem (Benkler et al., 2018; Gelfert, 2018; Michaelson et al., 2019; Wardle, 2018).

While both *disinformation* and *misinformation* are false information, the crucial difference between them, based on the surveyed literature, lies in the presence or absence of the intent to harm or deceive the recipient (Fallis, 2015; Fetzer, 2004; Hameleers, 2023). Conversely, malinformation is true information shared to cause harm (Wardle, 2018), which might include misrepresentation of true information to create a misleading impression by omitting important details or context (Grimes & Gorski, 2022, p. 4). These contiguous types of “problematic content” represent only a single dimension of “information disorder” not fully comprehending the use of rhetorical and affective devices (e.g., satire, irony and sarcasm) as well as content created with total disregard for the truth solely to affect the recipient (i.e. “bullshit” according to Deck, 2023; Pennycook et al., 2015; Sarajlic, 2019); (cf. DeJong & Souza, 2022; Grimes & Gorski, 2022; Rossini, 2023; Shcherbakova & Nikiforchuk, 2023).

Of course, within the political dimension of “information disorder”, the superordinate phenomenon of propaganda cannot be overlooked. Building on the definitions of early 20th-century propaganda theorists like Edward Bernays (Bernays, 2005) and Harold Lasswell (Lasswell, 1971), propaganda can be viewed as “communication designed to manipulate a target population by affecting its beliefs, attitudes, or preferences in order to obtain behavior compliant with political [and other] goals of the propagandist” (Benkler et al., 2018, p. 29). As such, propaganda can be seen as an overarching strategy that may incorporate misinformation, disinformation, and malinformation to influence public opinion and behavior. This definition

effectively captures the main characteristics of political and state propaganda inclusive of non-state dynamics as well as the commercial and social dimensions of propaganda (e.g., in the case of using commercial or social “bots” for commercial or social benefit) (cf. Benkler et al., 2018; Freelon & Wells, 2020; Guess & Lyons, 2020; Lock & Ludolph, 2020).

Political, commercial, and social dimensions are often intertwined, with each supporting or reinforcing the others. Examples include a group of Macedonian teenagers producing “fake news” for profit during the 2016 U.S. Presidential election (Guess & Lyons, 2020) or the “Channel3Now” news resource sharing false information about the name of a 17-year-old charged for the Southport attack in the UK, which is suspected to be a commercial operation focused on disseminating viral news for profit (Quinn, 2024; Spring, 2024). Hence, “information (dis)order” actors may be politically, ideologically or commercially motivated depending on their aims and the type of operation carried out.

The rise in digital authoritarian practices globally challenges the traditional definition of authoritarianism based on the type of state political organization or lack of free and fair elections. Conversely, a practice-oriented approach to authoritarianism allows for a more nuanced understanding of how these practices operate not only in neo-authoritarian regimes, but also in modern liberal democracies. Instead of focusing on regime types and where “information disorder” actors originate, this approach emphasizes *authoritarian practices* that are viewed as “patterns of action that sabotage accountability to people over whom a political actor exerts control, or their representatives, by means of secrecy, disinformation and disabling voice.” (Glasius, 2018, p. 517). This perspective dispels the assumption that authoritarian practices are exclusively confined to authoritarian states, and helps to address the global challenges digital authoritarianism poses while extending beyond traditional authoritarian and democratic frameworks.

Finally, the distinction between state and non-state actors may be less useful in authoritarian contexts, where public state and private business operations are centralized, intersect, and overlap, reflecting complex underlying mechanisms of authoritarian governance and authoritarian capitalism. Russia’s Internet Research Agency (IRA) is a prime example of this intersection. The IRA, while seemingly a private entity, operated with clear connections to the Kremlin, performing tasks that aligned with state interests and receiving funding and directives from state actors (DiResta et al., 2019). In other authoritarian contexts, such as China’s, private technology firms like Huawei and Tencent became actively involved in the Chinese government’s broader surveillance agenda, integrating their technologies and capabilities to support state objectives (Huang & Tsai, 2022). Under such circumstances, the nominal designation of these actors as “non-state” becomes problematic and needs to be re-examined.

DOMAIN 1 – Identity, Dominance, and Diaspora

Practices of population management through surveillance, media manipulation, and influencing public opinion are undertaken to achieve specific political results – to different degrees, these are features of any modern state, be it a democracy or autocracy (cf. Bernays, 2005; Ellul, 1965; S. Hutchings et al., 2024a; Lasswell, 1971; Lippmann, 1922). Many of these techniques were pioneered as early as the 19th and early 20th centuries by democracies who were at the forefront of this as the most advanced modern states at the time. Autocracies also adopted these practices (often importing them from democracies) to their own use. These practices took a different form in autocracies, as autocratic rulers have been unaccountable or far less accountable to their citizens and far more relied on cohesion and violence, rather than “engineering consent” (Lippmann, 1922), in order to stay in power.

The fact that such practices are not exogenous, but rather endogenous to democratic countries as any other modern state tends to be overlooked by many current “Disinformation Studies” scholars is significantly

foregrounded in historical and political communication scholarship of the early-mid 20th century. Ellul (1965), for instance, points out that during World War I, it was the democratic states – specifically France, UK, and the U.S. – that pioneered large-scale propaganda efforts, combining mass media with advertising and psychological techniques. These efforts demonstrated the ability of democratic states, rather than authoritarian regimes, to employ propaganda tools not just for the war effort but also in the promotion of political agendas, laying the groundwork for modern propaganda practices. Over time, authoritarian states have adopted and intensified these methods, but the origin of modern propaganda lies within democratic systems. This revelation challenges the commonly held notion that propaganda is primarily a tool of authoritarian regimes, instead demonstrating that it is a feature of any modern state, which seeks to mobilize and control public opinion for political ends.

Russia, for example, as one of the most prominent authoritarian actors propagating “information disorder” in many ways acted as a learner, rather than innovator, by historically adopting population surveillance from the European states, including emerging democracies (cf. Holquist, 2001). Russian media, especially state-affiliated entities like RT and Sputnik, have not just innovated but have also borrowed and adapted strategies already in use within Western media landscapes, mimicking the strategies of right-wing media ecosystems in the United States, such as those employed by outlets like Fox News and Breitbart. These techniques include crafting hyperpartisan narratives and leveraging digital platforms to amplify their messaging (cf. Hutchings et al., 2024a). The application of these techniques in authoritarian regimes and liberal democracies, however, differs. In Russia, for example, these techniques are centrally coordinated and embedded in a broader strategy of state propaganda, where the primary goal is to consolidate state power, control public opinion, and project influence internationally, especially by exploiting the weaknesses of liberal democracies. In contrast, when similar “information disorder” techniques are employed in democratic states, they tend to be less coordinated and more dispersed, reflecting the pluralistic nature of democratic media environments. To better understand these techniques, first we must examine the contemporary role individual identity and collective identity construction.

The Contradictions of Identarian Isolation and Dominance

There is a growing sense among scholars that disordered information is not merely a communication tool, but is deeply embedded in the socio-political fabric and psychological predispositions of individuals and groups. What are the narratives which underpin disinformation efforts? If we do not understand this, we risk focusing on the symptom of the issue. The very term “disinformation” must be problematized to better understand how it differs from state propaganda but also to highlight what it means to call something disinformation in the context of a neoliberal yet democratic culture where advertising, public relations, electoral campaigning, political lobbying and the numerous industry services of ‘crisis management’ and ‘spin’ are adjacent, yet legal forms misrepresentation, deception and persuasion. What is the effect on public trust, when so much emphasis rests on disinformation but not on these other forms of deception?

In this era of constant connection, communication overload, and the glut of often contradictory information, everyday citizens and news consumers alike rely on cognitive shortcuts – often in the form of habitualized media practices – to simply the world around them (Andrejevic, 2013; Burchell, 2024). Alarmist narratives about disinformation and indeed institutional trust and societal polarization are not wholly new – yet they are presented as unique and unprecedented contemporary situation often deterministically linked the latest cycle of innovation in the media. These narratives undermine everyday individuals’ sense of agency in navigating the informational landscape – undermining the practices of digital resilience that news consumers have already developed. As journalists and scholars, we need to consistently test these claims – challenging narratives that today’s social ills are unprecedented in their complexity and degree by asking compared to when historically, compared to where culturally and globally, and compared to which sort of constellation of political, economic

and technological factors. By asking these questions, we also locate our own debate more precisely – where both disinformation and the digital technologies at the center of these narratives then represent a symptom or characteristic of neoliberal, populist, and authoritarian political economies – what occurs when these political economies intersect is at the heart of this report.

When we talk about the normalization of disinformation, a number of additional moral and political dimensions demand our attention. Where disinformation and other practices of and strategic interpretation are status quo political establishment buttressed by economies of persuasion and misrepresentation, then it is important to understand this as establishing epistemic hegemony where our critique must first ask whose perspective, whose positionality, whose recourse to economic security or political power is that normalization benefiting? A critical theory lens highlights this as an ideological critique: numerous, historically marginalized groups and identities that have been subject to the hegemonic narratives of those in power – narratives that uphold the erasure of historic and on-going inequality, violence, repression, and colonialism. Yet this critique is today being employed by those groups that have traditionally been of a dominant class – as ethnonationalist majorities and men are taking on the mantle of being collectively aggrieved – “wronged” amid a more pluralistic society and empowered by populist rhetoric directed towards political movements that seek change towards equality and a more responsible tolerant collective public discourse (Chouliaraki, 2024; Reckwitz, 2020). Individually, as citizens and media users, our own reasoning in relationship fact or fiction, truth or lie, is embedded within this hegemonic and historical landscape. The “common sense” of the contemporary Anglo-American neoliberal society allows use as individuals to perceive the informational landscape as a digital marketplace and as consumers of media products rather than as a citizen in moral-political community or public sphere, such that our selection, interpretation, and use of media is simply an economic right – albeit one that mutually constitutes our perspective on the world around us.

Where disinformation strategically targets certain identity groups, whether as subjects of the disinformation or audiences of it, it is important to consider this as entangled with longer colonial histories. The focus on disinformation in the media can be understood as reinforcing pre-existing power structure “by leveraging anti-Black racism, misogyny, and xenophobic sentiment to protect conservative interests.” (Reddi et al., 2023, p. 2202) Moreover, some authors critique the “racial amnesia” of disinformation studies and its technological determinism: by treating disinformation as a new, digital phenomenon, we obscure the “longer histories of racial power and hierarchies that manifest in our contemporary media and information environment.” (Mejia et al., 2018; Reddi et al., 2023) In other words, while the term post-truth is treated as a novel phenomenon precipitated by digital disinformation, “for many minorities this is nothing new and the Internet has just made alternative facts more evident to other groups.” (Gittens, 2017) Indeed, although the concept of post-truth has only recently come to prominence in political science, the empirical experience of the post-truth has long been in existence. Consider the definition of post-truth in the *Oxford Dictionaries*, “relating to or denoting circumstances in which objective facts are less influential in shaping public opinion than appeals to emotion and personal belief.” This definition can encompass realities that far preceded the advent of technologically facilitated information. And indeed for Mejia et al. (2018), the point is that “American racial politics has never been concerned with ‘the truth’” (Mejia et al., 2018).

When we speak to the nature of news media itself, journalistic work that accounts for and engages interpretative gaps, pluralities of opinion, and locality of perspectives and identities suffers from both an elite- and event-orientation towards what qualifies as news– the prominence of short-termism only concerned with “who”, “what” and “when” over the longer exploration of “how” and “why” and “to what effect” – a media bias entangled with the actions of powerful institutions and actors, often central to event itself and therein strategically readied with prepared denials, interpretations, accusations that form an alternative, or preferential narrative to sway the public (Burchell, 2020; Burchell & Fielding 2024; Stein, 2021). Fact-checking suffers from similar narrow aperture for determining what qualifies as details of

event, identifying actors, and located the source of deceptions, all of which serves to once again focus our media landscape on the actions of powerful actors. However, rather than these actors being held to account, they and the news media are maintained as the determining center of hegemonic narratives (Couldry, 2012). Indeed, there is a hubris to fact-checking that must be unpacked – the act of calling something disinformation can skew or misrepresent the phenomena under consideration by flattening it to the factual basis an action or event – a simplification only possibly through a loss of interpretive breadth and dearth of experiential depth, aspects that are so central to bridging disparate individual and collective experiences.

Rather than focusing on the content of disinformation, the solution may not be a matter of regulating hate speech or algorithmic distribution, we made need to focus on what happens before the message– what’s been called pre-propaganda. As early as 1965, French philosopher and sociologist J. Ellul proposed thinking beyond the psychological predispositions which make individuals susceptible to propaganda – he argued that there were crucial sociological processes that occurred slowly, over time, which set the stage for propaganda and allowed these messages to work (Ellul, 1965). Writing in *Harper’s Magazine* in 2021, J. Bernstein argued that understanding this “pre-propaganda” continues to be crucial and that “the fix” has nothing to do with algorithms (Bernstein, 2021). Instead, we need to look at the history that shaped the specific type of person that responds to these types of problematic information. What is the historical, social, political, and cultural context in which the audiences for disinformation live? How has this shaped their psychological predispositions, or the social fabric in which they operate daily? Fixing algorithms may provide temporary relief, but if our issues and propensities are so deeply embedded, they are bound to continue causing issues down the line.

In the last few years, some scholars and practitioners have expressed concern about the focus on digital literacy as a catch-all solution to digital harms. The overarching issue is not related to the practical complexities of implementing digital literacy, but rather argues that we are not doing the social-community work needed to combat disinformation; as a result, digital literacy is a “band-aid” solution, and that we risk over-emphasizing its positive effects. The real issue – and the reason for which disordered information is argued to work in the first place – is that social and political trust are in sharp decline. So, what social-community work ought we be doing to improve the declining social and political trust?

Social isolation is argued to play a key role in worsening polarization and socio-political trust. Social isolation is considered a public health issue, and a socio-political challenge, which is ironic when digital technologies have made us feel more connected than ever. danah boyd argues that we have removed youth from public spheres and from inner-age dynamics (boyd, 2018). With the advent of social media and increasingly isolated youth, we have removed youth from an environment where they can be part of a broader ecosystem. In this way, youth do not interact with others from dissimilar environments, thus trapping them in echo chambers and not exposing them to different perspectives. In her perspective, digital literacy can backfire because you cannot resolve fundamental epistemological differences through compromise, and that media literacy and critical thinking may be deployed in the classroom as an assertion of authority over epistemology. Teaching students to criticize media can lead them down conspiracy rabbit-holes. Instead, boyd argues that we need to teach students how interpretation is socially constructed.

Sociologists have long engaged with the dangers of social isolation – in particular isolation amid and amongst others. In his landmark book *Bowling Alone* (2000), Putnam argued that Americans were experiencing unprecedented social isolation due to the television. As a result of increased screen-time, individuals were no longer engaging in activities of civic engagement and community participation, such as bowling leagues, churches, and civic groups (Putnam, 2000). Putnam recently published an updated study in which he argues that social isolation has continued to worsen. He argues that there is a “decline in the sense that we are all in this together, and that we have obligations to other people ... to care for other people” (Garcia-Navarro, 2024; Putnam, 2020). Putnam differentiates between bonding and bridging social capital; bonding social capital means bonding with others like yourself, while bridging social capital is bonding with others unlike

yourself. It is this latter form of bonding which we are lacking, and it is harder to build. In a society with low rates of bridging social capital, levels of trustworthiness are low. Joining clubs helps democracy because “it’s only by connecting with other people that we generalize from our experience. In the running club, you learn that you can trust other people, and learn in a way what you need to do to maintain that trust” (Garcia-Navarro, 2024). The U.S. Surgeon General published a report in 2023 characterizing the “loneliness epidemic” as an urgent public health issue – partially due to the adverse social impacts of isolation, but also because social isolation causes adverse health effects, increasing the risk for premature death as much as smoking up to 15 cigarettes a day (Murthy, 2023).

But why is social isolation such an issue? What are the ramifications of spending increasing time alone? And how does it connect to the risks of disinformation? There are tangible negative social effects to the fact that we are spending a lot more time alone, and that we simply want to be with others more; a study from Colorado State University found that more than 40% of respondents wished they had more time to spend with their friends (Pennington et al., 2024). The fundamental issue is that interaction with others helps citizens develop empathy, problem-solving, and cooperation (Department for Digital, Culture, Media and Sport, 2018; Murthy, 2023). Decreased interaction with those unlike us also impacts our ability to engage in democratic dialogue with political opponents, because we are out of practice with in-person interaction. Expert facilitators from the NGO Convergence argue that “living life primarily online minimizes our ability to engage directly and deeply with others. It makes in-person dialogue feel more foreign and uncomfortable” (Fersh et al., 2024). Indeed, scholars agree that the nature of online dialogue is vastly different than the one observed in-person. Behind screens, we are less likely to be empathetic and understanding, and we are observing a deterioration of online discourse (Habib et al., 2022).

The platforms are partly responsible for this decline in social cohesion, and for our increased inability to stomach the opposing perspectives of others, and to engage in civic dialogue. Platforms provide certain affordances – they reward certain behaviour. The built environment of social media platforms dissuades democratic dialogue and reasoned exchanges, instead incentivizing users to post extreme, provocative, binary, simplistic content (Forestal, 2022).

Violent communities have always existed. But particularly important today is how hate becomes technologically facilitated. Communities such as incel groups are generally discovered through the web, and when the narratives underpinning these ideologies go mainstream, these ideologies are much easier to find. Regehr et al. argue that incel ideology used to occupy an isolated corner of the internet, but the ideology underpinning these ideas are now dispersed in mainstream channels, particularly via TikTok and YouTube. The authors argue that this “Incel 2.0” – the dispersion of this ideology into the mainstream – is a symptom of a much wider cultural phenomenon of popularizing technologically facilitated misogyny through mainstream social media platforms (Regehr et al., 2024). Scholars and educators have grown more concerned with the impact of incel content on young men’s mental health, suggesting that they warp perceptions of healthy relationships, and that these ideologies can provide paths to radicalization. A report by the U.K. Government’s Commission for Countering Extremism found that there is “an important mental health dimension to incel networks including depression and suicidal thoughts” (Whittaker et al., 2024). Another study demonstrated that joining the Manosphere (by making a post or submitting a comment) resulted in the increase of many radicalisation “warning signs” (Habib et al., 2022).

Indeed, the platform affordances and users’ general inclinations to interact with provocative content causes violent and divisive ideologies to go mainstream, thus reaching a wider audience. In December 2024, the UK’s Senior National Coordinator for Counter-Terrorism pointed to the ways that radicalization is changing: “We’re seeing search histories which contain violence, misogyny, gore, extreme pornography, racism, fascination with mass violence, school massacres, incel and...terrorist material” concluding that “It is a pick and mix of horror, horrific content” (Dodd, 2024). Consider the rise of the Manosphere, the family of content also referred to as The Red Pill (TRP). TRP content was initially isolated to a corner of the internet,

and included various communities, including men's rights activists (MRAs), pick-up artists (PUAs), "men going their own way" (MGTOW), and involuntary celibates (incels) (Wilson et al., 2024). TRP has emerged as a neoconservative ideology which adopts essentialist notions of gender, such as gendered narratives of biological inferiority or hard-wiring, or #tradwife (i.e., traditional wife) content about women submitting to male partners.

What is striking is how these isolated individuals are nevertheless powerfully connected online. Some Manosphere subcommunities, such as incels, adopt and perform nihilistic perspectives and extremely violent views towards women with growing concern about how these ideologies are influencing men to commit acts of violence in the real world (Lewis, 2019). Incel communities were catapulted to front page news when two known members of incel communities committed mass murders. In 2014, Elliott Rodger uploaded a video to YouTube announcing his intention to punish women for their lack of interest in him, and proceeded to kill six people and injure fourteen others in a terror attack in Isla Vista, California ('Elliot Rodger', 2018). For years following the mass murder, Rodger was celebrated in incel forums, hailed as a martyr having died for the cause. In 2021, Alek Minassian posted on Facebook praising Rodger and stating that "The Incel Rebellion has already begun" ('Alek Minassian: Toronto van Attack Suspect Praised "incel" Killer', 2018). Minassian proceeded to kill ten people and injured 13 others by driving his van onto a busy Toronto sidewalk. Individuals like Rodger continued to be celebrated in online incel forums, with users calling him a "Supreme Gentleman", a "legend", and some users even dedicating poems to him (basedcrackaddict, 2024).

The concern is that these communities are discovered through online research and through algorithms suggesting content. A study of the reddit forum "r/exredpill" confirmed this concern, demonstrating that TRP ideology is generally discovered by (1) friends suggesting content, (2) encountering online communities by chance, and (3) social media platforms suggesting content (Botto & Gottzén, 2024). Beyond incel ideology specifically, TRP ideologies began to gain more mainstream traction as the narratives regarding gender began to shift quickly in the last decade and 'old-fashioned' misogyny, these essentialist notions of gender, made a comeback. Often called "cultural commentators," podcasters and vloggers in the Manosphere tend to publish short clips of longer-form interviews featuring abrasive hosts and defensive guests, aiming for "gotcha" moments which can be easily captioned for short clips with provocative titles. Podcasts such as *Whatever* (4.42M followers), *Fresh&Fit* (1.57M followers), and *the Pearly Show* (1.98M followers) follow this format and have amassed huge followings.

The audience for Manosphere content skews younger, and Manosphere talking points and narratives have made their way into schools. Teachers have noticed a shift in the behaviour of male students, a resurgence of male supremacy and misogyny in the classroom which often translates to harassment of female students and staff. In an Australian study interviewing 30 female teachers, these teachers expressed having to engage in increasingly combative interactions with male students that directly challenge and undermine their gender (Wescott et al., 2024). As one teacher recalls, "If we read something that's by a woman, [boys say], 'Why do we have to read this myth?' Or if we read a poem that deals with the woman's experience, 'Oh, it's not that bad. It's not that bad'" (Wescott et al., 2024, p. 177). Some Manosphere influencers, such as Andrew Tate, have had a disordinate impact on the narratives espoused by young boys – Tate is often directly quoted by students. A teacher in Melbourne recalls an interaction with a male student in which he told her: "Andrew Tate says women shouldn't be able to drive because they get into more accidents than men." (Wescott et al., 2024, p. 173) The issue is that there is perverse intent, a hope for a reaction, and that these narratives translate into actual sexual harassment in schools. And while male students have always challenged the authority of female teachers, participants in the Australian study observed that these behaviours have worsened, "performed with a growing sense of brazen, remorseless entitlement" (Wescott et al., 2024, p. 173).

Pedagogical responses have sought to address how to offer alternatives to the toxic representations of relationships and genders in social media, because the content is argued to be a gateway to radicalisation. The dominant view is that educators need to be imbued with knowledge of these online communities in order

to offer more equitable alternatives to the dominant messages and values in the social media content (Stahl et al., 2023). The question is also how platforms can respond, and how “delayed platform administration and moderation decisions can harm the quality of online discourse and our ability to prevent radicalization” (Habib et al., 2022).

Censorship and Self-Censorship among Diasporas

Across more democratic, illiberal and authoritarian contexts, for decades elites have manipulated the truth for political and economic gain, but in the last decade elites have more openly engaged in “post-truth” tactics, explicitly embracing “alternative facts” and twisting the rhetoric of “fake news” to undermine criticism and divergent points of view. It is in this informational milieu where ethnonationalism and chauvinism are on the rise, again with their intentions explicitly part of the messaging, serving to stigmatize women and minorities with tangible effects. Consider *The Trump Effect* – a study found that “in the absence of prejudiced elite speech, prejudiced citizens constrain the expression of their prejudice. However, in the presence of prejudiced elite speech – particularly when it is tacitly condoned by other elites – the study finds that the prejudiced are emboldened to both express and act upon their prejudices.” (Newman et al., 2021) In other words, elite rhetoric can lead individuals to publicly admit to prejudice and/or act on prejudice. Norms, which are standards of social behaviour which are context-dependent, can work to limit prejudice. For instance, a norm of racial equality will work to limit the expression of prejudice. These norms have also affected the types of racial appeals used and deemed acceptable by political elites. As Mendelberg documents, before the norm of racial equality was firmly rooted, candidates would use explicit racial appeals – often including ambiguous, deniable cues or so-called “dog whistles” – in campaign communications to appeal to prejudiced voters (Mendelberg, 2017). However, once the norms of racial tolerance and equality became entrenched, “such explicit appeals became ineffective, as individuals would recognize the message as violating these norms” (Stryker et al., 2016). However, equality norms did not lead to the disappearance of prejudice; “rather, it simply went ‘underground’ and could be activated under certain conditions using particular types of appeals” (Newman et al., 2021, p. 1121). And entrepreneurial elites harness these undercurrents, using versions of information recent scholarship would deem “alternative facts” or disinformation. Problematically, these “post-truth” narratives (which often employ implicit or explicit racial rhetoric) are perceived as honest, “real talk”, in contrast with the perception of the “dishonest, lying politician” in the public imaginary. Indeed, in a study of over 400 Americans, 91% who espouse an authoritarian ideology responded positively to the statement: “Donald Trump is not prejudiced, he simply speaks the truth” (Choma & Hanoch, 2017).

An initial, epistemological link between diasporas and disinformation emerges where theoretical concepts and the above trends are applied in good faith to make sense of the messy realities of lived experience. Yet these concepts reflect situated – and therein temporary visions and imaginings – of their own era. Almost inevitably these concepts misrepresent the actual dynamics of diverse communities and everyday practices on the ground. In a context when the world is imagined as naturally being divided into nations, the reductive concepts of ‘nation’ and ‘diaspora’ can have major policy-related outcomes, with devastating consequences.

This section of the report surveys a critical set of diaspora communities across a number of national contexts to better understand the role of disinformation in non-majoritarian communities that find themselves relationally linked to distinct media cultures worldwide and, often, divergent media narratives which, in turn, underpin distinct worldviews. Roger Brubaker (2005, p. 5) outlines three main criteria for defining diaspora: dispersion — any kind of dispersion (traumatic or otherwise) either across or within state borders; homeland orientation — orientation to “a real or imagined homeland as an authoritative source of value, identity, and loyalty”; boundary maintenance — the preservation of a distinctive identity vis-à-vis the host society. This may be a conscious resistance to assimilation or an unintended consequence of social exclusion. There is some consensus on the inclusion of boundary maintenance – cultural practices that define the boundaries and

characteristics of what a community is and what it is not – as a fundamental criterion that enables discussion of a diaspora as a distinctive entity while not simply referring to all immigrant communities as “diasporas” of one sort or another (Armstrong, 1976; Cohen, 1996; Safran, 1991; Tölölyan, 1991 cf. Brubaker, 2005). As will be demonstrated in more detail below, in the Chechen, Crimean Tatar, and Palestinian cases each of Brubaker’s three criteria apply equally — there is a notable point (or points) of dispersion, and homeland orientation and boundary maintenance remain salient. In the Syrian case, the three criteria are present but homeland orientation and boundary maintenance are less prominent. For the Indian and Chinese diasporas, Brubaker’s three criteria also apply but to differing degrees, specifically in the case of homeland orientation and boundary maintenance which vary depending on, *inter alia*, generation and regional origin.

Other scholars, however, such as Homi K. Bhabha (1994), James Clifford (1994), Paul Gilroy (2002) and Stuart Hall (1990) propound that diaspora cannot be reduced to an essence or purity, but rather the diaspora experience is heterogenous and should be thought of in terms of hybridity. Broadly speaking, hybridity forefronts the discursive limitations of binaries between colonizer and colonized by emphasizing that an individual comes to know themselves in relation to the “Other” (Bhabha, 1994). Examining the concept of diaspora through the lens of hybridity accentuates the transnational nature of the former. Hybridity is particularly pertinent within the Chinese (and Indian?) diasporas, exemplified in the oft-cited term “Chinese Australians”. Hybridizing group identity by merging ethnic or national labels did not feature in discussion of any other case study.

Demir (2022, p. 5) lauds the theorization of diaspora through hybridity for stressing the relationship between empire and diaspora. However, Demir states that in focusing on ‘becoming’, this approach, like the “ideal type”, has also “too narrowly confined diaspora theorizing to ontological concerns.” Instead, Demir conceives of diasporans as active agents and is thus engaged with what diasporas do, rather than what the diasporas are. For Demir, in the context of the Global North specifically, the insights of translation studies and research on migrancy, race, and culture illustrate how “diaspora as translation” and “diaspora as decolonization” can advance foreignization and decolonization in the host country. In discussing how diasporas can dislodge coloniality, Demir commends and expands the notion of “methodological nationalism.” Along a similar vein, Celia Haig-Brown (2012) proposes a decolonial reframing of diaspora studies discourse, noting that the central question of such studies should not only be about “where people of the diaspora come from, but where have they come to?” (p. 74, 2012). In other words, when looking at diaspora communities and their engagement with identity, host societies, media, and other key domains, it is pertinent to also consider whose traditional lands they have found themselves on (Haig-Brown, 2012). In effect, narratives and discourse around land ownership and indigeneity are central components of the diaspora identity and dictate how communities may position themselves within a host society, and vice-versa.

According to Andreas Wimmer and Nina Glick Schiller (Wimmer & Glick Schiller, 2002, p. 301), “methodological nationalism is understood as the assumption that the nation/state/society is the natural social and political form of the modern world.” This manifests in diaspora studies by imagining dispersed populations as “an organic, integrated whole” overlooking how “nation-state building processes that impinge upon diasporic populations” (Wimmer & Glick Schiller, 2002, p. 324). Wimmer and Schiller extend their criticism to transnational studies, for, *inter alia*, overstating the internal homogeneity of transnational communities — particularly relevant in the Chinese diaspora as multiple generations from diverse regions who share limited commonality are nonetheless framed in homogenous terms simply as “Chinese”. Indeed, only with the triumph of the nation-state in the nineteenth century did collective identity become largely synonymous with the concept of nation, where prior collective identity was more likely to be considered in terms of other markets of difference, such as religious affiliation or patois (Tölölyan, 1991). The rhetorical force of “nation” thus becomes redundant when examining populations dispersed before the inception of the modern nation-state and state-building (Vortevic, 1997).

The censoring and at times silencing of diaspora voices across information ecosystems is closely linked to the issue of disinformation. State censorship – particularly of newcomer and diaspora communities – is used by host societies as a means of countering disinformation campaigns from abroad by censoring content that is linked to authoritarian regimes and their proxies (Braga et al., 2024; Stray, 2019). Yet censorship remains analytically distinct from disinformation, despite being a tactic within broader disinformation campaigns and activities. Pinpointing what determines the views presented in various diaspora media outlets is difficult: Self-censorship among newcomers including media producers seems, at least in part, to be determined by the likelihood of the host country supporting or negating particular narratives. In the case of the Crimean diaspora of the 1970s, we find the Crimean Tatar newspaper *Lenin Bayragi* was published in Uzbekistan and thus, “affiliated with the Uzbek state and censorship so did not openly support the [local oppositional] National Movement” while also being anti-capitalist and anti-West (Kahraman, 2014, p. 150). Whereas the rhetoric and references in other Crimean Tatar news outlets *Emel* and *Dergi*, operating in Turkey and the West, positioned themselves as anti-Soviet and anti-Russian and anti-communist.

Presently, censorship plays a determining role in the information landscape for Russian-speaking communities in Estonia and Latvia, particularly due to EU-wide bans on Russian state media. These bans, implemented in response to concerns over disinformation and propaganda, have left a vacuum in the media consumption of these communities, who traditionally relied on Russian sources for news but also as a matter of access to their known and intimate cultural milieu. The absence of these outlets has not been adequately filled by localized media that can effectively address the linguistic and cultural needs of Russian speakers in their host countries. As a result, many in these communities feel disconnected from mainstream narratives – a disenfranchisement and estrangement at the heart of cultural and informational silos. The lack of comprehensive Russian-language media that reflects local realities further alienates these groups and could exacerbate existing social divides in a context where wider state efforts to promote integration through media have fallen short. This situation highlights the challenge of balancing censorship with the need for inclusive, diverse media that caters to all linguistic groups within the EU.

Compared to Syrian diasporic media outlets in Turkey, two forms of self-censorship have been observed in parallel to the 13 yearlong Syrian Civil War coming to a conclusion at the time of writing: (1) limiting the focus of their content and its target audiences to Syrians within Syria and avoiding any commentary on Turkish affairs while (2) censoring content overtly critical of Turkish policies relating to the Syrian crisis and their direct involvement in the conflict (Badran, 2020, p. 79). Syrian oppositional media have refrained from commenting on the tensions in Turkey’s socio-political climate in the preceding years. Badran nonetheless concludes that “media actors felt they had broad autonomy over the content they were producing in Syria” (2020, p. 80). Drawing on interviews with Syrian advocates for transitional justice, however, Tenove (2019) determined that there is an increase in authoritarian regimes using digital communication technologies to counter the narratives set forth by critics of the regime abroad and to impede safe expression of anti-regime views. How different state and non-state actors restrict the production of diaspora political discourse without overtly breaching their civil liberties would be valuable for understanding covert forms of media control as a form of censorship.

Turning to Australia, one examination of how the PRC sought to influence the political participation of Chinese Australians through media content asserts that most diaspora media coverage in Australia shows subtle political alignment with the interest of Beijing and sometimes contributes to PRC talking points (Christensen, 2021). The PCR is known to exert soft power in the diaspora through narratives around the sovereignty of the South China Sea, Taiwan, Tibet, and Xinjiang as seen by analyzing samples from Twitter, other media archive data, and the United Nations migrants data (Padua & Liu, 2019). Regarding social media censorship, Sun (2019, p. 26) portends that while “WeChat is subject to censorship in China, it operates more or less outside Australia's regulatory framework”. In a similar investigation, Yu & Li (2022, p. 104) report that although WeChat has expressed a willingness to engage with Australian authorities, they are

nonetheless guilty of transgressions regarding “platform oversight of misinformation or content censorship”.

For many diaspora communities, in particular those who faced an on-going or generational traumatic dispersal, transitional justice is central pillar of their media engagement and collective identity, a process of seeking accountability and responsibility for past systematic violations of human rights. Mechanisms for achieving justice can include fact-finding commissions, trials, repatriations, and institutional reform (Atallah & Masud, 2021). The commencement of these processes usually coincide with transitions from authoritarian to liberal society, though may not occur at all. Despite some consensus, debates persist in the existing literature on a unifying definition (Mendes, 2023; Skaar et al., 2016). More broadly, and with a diminished priority of achieving accountability, transitional justice can be defined as involving:

Anything that a society devises to deal with a legacy of conflict and/or widespread human rights violations, from changes in criminal codes to those in high school textbooks, from the creation of memorials, museums, and days of mourning to police and court reform, to tackling the distributional inequality that underlie conflict (Roht-Arriaza, 2006, p. 2).

Diaspora mobilization is increasingly significant for transitional justice movements given that diasporans are, “non-state actors with increased agency in homelands, host-lands, and other global locations” (Koinova & Karabegović, 2019, p. 1809). The myth of return can become an idealized manifestation of transitional justice, though a desire to return does not constitute part of all transitional justice narratives. Previously dispersed populations which have returned to their territorial homelands may also seek transitional justice and encounter different obstacles to those still resident in host countries. Understanding how subnational, transnational, and diasporic engagement interacts with transitional justice and the myth of return is pivotal for moving beyond/countering disinformation and creating collaborative transnational solutions to myriad geopolitical crises.

Disinformation targeting diasporas

Since the 2022 Russian escalated invasion of Ukraine, disinformation scholars have increasingly focused on the role that Kremlin-linked media actors and disinformers work to target Russian-speaking diaspora and mobilize them to work against their respective host governments, particularly in the Baltics. In Estonia and Latvia, Russian disinformation targeting diasporas often emphasizes the strategic use of media to maintain influence in these post-Soviet states. Kremlin-backed media outlets exploit cultural and linguistic ties to spread narratives that undermine trust in local governments and Western institutions (Piret Ehin 2016; Epp Lauk 2019). Russian-language media in these countries fosters a sense of alienation among Russian-speaking minorities, fueling separatist sentiments (Andis Kudors 2018). Disinformation campaigns are tailored to resonate with historical grievances and socio-economic disparities (Janis Bērmziš 2022). These efforts are part of a broader Russian strategy to assert soft power and destabilize NATO’s eastern flank (Kristina Kallas 2016). Such realities underscore the challenges these nations face in countering disinformation while protecting minority rights and maintaining social cohesion. At the same time, there is scholarly disagreement around the impact of disinformation on these audiences: Mangirdas Morkūnas (2023) and Coolican (2022) note that Russian disinformation targeting Russian-speaking audiences is not particularly effective in impacting public opinion in the Baltics, and there is little evidence to suggest that there is a strong security risk. Other literature on this topic focuses on building resilience to Russian disinformation and how strategic communications and media literacy can help serve as an antidote to disinformation (Robbins, 2020; Teperik, 2022).

In relation to Chechnya within the Russian Federation, with a militarized succession movement, terrorism, and a current political proximity to the Kremlin – two areas of disinformation are of particular importance — the representation of North Caucasian migrants in mainstream Russian media as criminals

element, and the “memory war” between pro-independence and pro-Russia groups in Chechnya, neither of which directly pertain to the diaspora communities created by the 1944 Soviet deportations. Following protests around Putin’s re-election in 2012, official discourses around Russian nationhood shifted, and new regime imperatives emerged. Television reporting began to reflect this change which manifested as “the social contract between the political leadership and society” becoming “based primarily on the issue of security - the government’s ability to successfully defend Russia from its multiple (perceived) enemies” both internally and externally (Tolz, 2017, p. 743). Narratives about security threats require identification with the national group to justify interventions in public life (Tolz, 2017). Before 2011, Channel 1 and Rossiia, the most popular and trusted television stations in Russia, framed migration as necessary for Russia’s economic well-being which limited discussion of any social issues arising from migration (Tolz, 2017). From 2012 onwards, this changed drastically as a growing sentiment of xenophobia found in opinion polls was mobilized to frame the protests as anti-migrant. Subsequently giving the impression that protests had been anti-migrant and that anti-migrant media campaigns were part of the government’s diligence to citizens’ security concerns (Tolz, 2017). “The Muslim migrant” — referring primarily to migrants from the North Caucasus and Central Asia became the target of the campaigns. The manipulation of public sentiment and stereotyping of national groups are typical characteristics of disinformation campaigns which seek to “dismiss/deny, distort, distract, and dismay” (Ring, 2015).

Similarly, since the Second Chechen War (1999-2009), the pro-Russia Chechen government has been engaged in a “memory war” with pro-independence actors which has occurred mainly within the media sphere. For Iliyasov (2024), the memory war being fought through conventional and social media constitutes a continuation of the armed conflict of the First and Second Chechen Wars (Iliyasov, 2024). Moreover, the memory war in Chechnya potentially strengthens narratives that pro-independence/separatist actors pose a security threat to Russia – additionally framing Russia as Western ally in the so-called global war on terror. Crimean Tatars are framed less dialectically than Chechens in media coverage, potentially a result of less conspicuous independence sentiments. Nevertheless, Ukrainian media content between 2010 and 2012 indicates that Crimean Tatars were framed as “the source of various problems” and how “discursive strategies aimed at portraying minorities as a problem is a way to rationalize and justify the discrimination against them, to categorize the experience of social interaction with these groups in the simplified and stereotyped way” (Bezverkha, 2015, p. 109). Thus, even decades after mass return to the homeland, both Chechens and Crimean Tatars continue to encounter ethno-national-based marginalization by federal state-media.

Comparing this to the Palestinian context, disinformation narratives centre around the colonial framing of either settlement or occupation as opposed to representations of the diasporas (Lakhani & Khan, 2023; Stein, 2021). The proliferation of social media and the active engagement of users have played a central role in shaping opinions about the contemporary conflicts as narratives are constructed once again through the lens of historical memory and identity (Maharani, 2024). Studies on disinformation in Israel/Palestine include analysis of the perceived origins of fake news (Masharqa, 2020), a Zionist Disinformation Campaign in Syria and Lebanon during the Palestinian Revolt, 1936–1939 (Muhareb, 2013) and content analysis of more recent fake news stories (Stănescu, 2023).

Turning to the Syrian diaspora, two themes emerge. First, the systemic disinformation campaigns launched by the Assad regime in relation to the now simmering Civil War (Eddin, 2013; Levinger, 2018; Tumber & Waisbord, 2021) see Russian-backed propagandists circulating stories on how the White Helmets volunteer rescue organization is associated with terrorism (Levinger, 2018) and, in relation to the Syrian diaspora, how Syrian pro-democracy activists and diasporic political entrepreneurs utilize webinars to counter mis/disinformation on the war in Syria (Wessels, 2023). Second, coverage of the Syrian diaspora in across Turkish media and social media has changed over the 13 years since the onset of the civil war and remains in flux. For example, a study of 1,000 articles from state-controlled media between June to September 2015 revealed that Syrians were predominantly portrayed as victims in need of assistance to survive, though the

study also noted that occasional references to Syrians as criminals were present (Sunata & Yıldız, 2018). In contrast, a more recent study conducted between March and August 2020 demonstrates a drastic shift towards ignoring the plight of Syrians (Yücel, 2021). During the Covid-19 pandemic, Syrians were “symbolically annihilated” which may have resulted in healthcare disparities among communities systematically underserved by the Assad government (Yücel, 2021, p.8). Thus, minority and diaspora communities are more vulnerable to media representations which may directly influence, inter alia, their access to government services. In contrast, anti-Chinese sentiment dominated framing of Chinese diaspora during the Covid-19 pandemic in Australia and elsewhere furthering pre-existing racial discrimination (Lim & MacDonald, 2022; Tan & Tao, 2024; Xia et al., 2024).

As an additional point of comparative contrast, we end this section by noting the dearth of disinformation analysis in relation to the Indian diaspora – currently facing a wave of targeted transnational repression that comparable in nature to transnational security mission among Chinese diaspora. In Australia, some recent literature has argued that policies enacted by the Indian government, alongside the development and proliferation of social media and other forms of communication, have changed how Indian diasporic communities identified with their host nations and their homeland, including in the case of Australia’s Indian community (Voigt-Graf, 2005). Building on this, Mamalipurath (2023) conducted a mapping of the key issues and needs related to information among these communities, finding that there are mis- and disinformation campaigns leading to communal polarization and that Australian politicians are becoming enmeshed and amplifying certain narratives about Indian communities. The report also found that current Australian government efforts to counter mis- and disinformation among the Indian diaspora fall short because they do not cater to the culturally and linguistically diverse diaspora. Hindutva related disinformation – which is tied to a Hindu-centric, right-wing ethno-nationalist political ideology – is of particular concern as it is on the rise in Australia, but local Australian media is said to be giving excessive attention to Hindutva narratives that “oversimplify and ignore” the diverse political perspectives of wider Indian communities (Mamalipurath, 2023; Thapliyal et. al, 2023).

Emerging digital authoritarian practice heavily relies on the use of digital technologies by modern states and complex webs of associated actors to surveil, control, and manipulate target audiences, both domestically and internationally (Feldstein, 2019; Roberts, 2018). Techniques such as internet shutdowns, content filtering, and the use of state-controlled media help authoritarian regimes to control the flow of information and suppress dissenting voices (Deibert et al., 2010; King et al., 2013). Modern states – with authoritarian regimes, perhaps, being the most illustrative examples – collect vast amounts of data on their citizens to monitor and pre-empt any dissent (cf. Greitens, 2016) but this extends beyond their borders due to the transnational nature of the technological infrastructure and global communications. Sophisticated technologies like facial recognition, internet monitoring, and social media surveillance are involved (cf. Cohen, 2020; Lyon, 2018; Xu, 2021) but also a sophisticated legal infrastructure to curtail and manage dissent with a sheen responsible political consistency. Diasporic audiences, however, often reside beyond the systemic edges of national jurisdictions, where numerous media, state, and non-state actors are still vying for their attention, especially in times of heightened geopolitical tensions involving their home countries. While bottom-up diasporic digital storytelling combines circulating news media narratives and social media platforms, forms of censorship and self-censorship from within diaspora groups allow state-led narratives to be produced about, rather than by, the geopolitically sensitive diaspora communities.

DOMAIN 2 – Lawfare

While we have found self-censorship as a characteristic of diasporas relationship to disinformation, these practices are arguably extension of some home-country censorship regimes – both in legislation and in practice. As a representative “ideal” case (for lack of a better term) of democratic backsliding and authoritarian regime capture, we have conducted audit of legislation enacted within the Russian Federation over the past 15 years spanning Internet control, restrictive registration of press and civil society, suppression of freedom of expression and freedom of assembly.⁵

These repressive frameworks reveal the founding traumas that have come to define new diasporas including an emerging Russian LGBTQIA+ diaspora finding ways to emigrate and connect abroad as well as the waves of young adults abruptly resettling outside of the Russian Federation at the onset of the 2022 full invasion of Ukraine and subsequent widening of mobilization efforts. At that time, censorship laws were radically expanded including the proliferation of defamation laws, the inclusion of prison time as punishment, and new laws focused on “discrediting and spreading false information” about the Russian military. Earlier blasphemy laws and the so-called “Anti-LGBT Propaganda” laws already limited discussion, expression or representation of LGBTQIA+ experiences in the media and online. Amendments were made to articles of the criminal code relating to “National Security” introducing and expanding definitions of separatism, high treason, extremism, and terrorism – labels currently being used to describe opposition political movements and LGBTQIA+ communities, in addition to discussions of decolonization relating to sovereignty of ethnic communities or separatist movements within the Russian Federation. Laws against NGOs, news outlets as well as individual and public associations have expanded to include the “Foreign Agents” and “Undesirable Organizations” laws, thereby tightening legal and economic control of independent media, advocacy groups, and researchers alike. Laws against the right to peaceful assembly have been accompanied by those policing historical memory and “propaganda” in public education. Control over the internet has incrementally been consolidated through laws permitting the blacklisting of sites, extrajudicial blockings, mandatory “localization” of storage for user data on Russian Federation soil, intermediary liability in the network of platform dependencies that make up the digital economy, the “sovereignization” of the Internet as law, mandatory identification of users and bans on VPN services to skirt these restrictions, and laws focused on criminalizing the spreading of “fake news” – an arbitrary and weaponized vehicle for denouncing any criticism.

In these ways, the current Russian regime offers not only a template for illiberal democracies within the EU but actively supports the export of the associated security and surveillance techniques upon which the application and prosecution of these laws depends. This is lawfare – the redefinition of the political landscape and the body politic itself through repressive legislation.

Domestic Legislation and the Dispossession of Rights

Once again, the disinformation landscape reveals itself in terms of censorship: rather than the self-censorship of diasporic media, we see the development of legal techniques to contour the political landscape in such a way as to preclude freedom of expression and political participation – all but ensuring the dominance of strategic state narratives. International organizations that monitor oppressive legislation in different countries have been sounding the alarm since early years of modern Russia (*Список репрессивных законов*, 2021). However, in the absence of any meaningful tools to turn the tides from the outside and due

⁵ Texts of all Federal laws (FZ) and Federal Constitutional Laws (FKZ) can be found in the online database ConsultantPlus : <https://www.consultant.ru/> by typing the year and the number of the law and adding “ФЗ” (for FZ) or “ФКЗ” (for FKZ) in the search line.

to the lack of accountability mechanisms of authorities inside the Russian Federation, the state has succeeded in solidifying the legal framework freezing all springs of free speech in the country. NGOs, international organizations and independent media outlets then fill that vacuum where the citizenry would normally voice their dissent, delivering increasingly condemning reports with increasingly depressive titles on the updates in the Russian legislation and its (mis)application (Alina Danilina, 2023; FIDH, 2018, 2023; *From War to Prison*, 2024; *Russia: Freedom*, 2024; *New Heights of Repression*, 2024; *Repressive Laws*, 2024).

A prominent feature of censorship legislation in Russia is its all-encompassing character – targeting actors, discursive themes, public and online spaces as well as legal frameworks all at once – just one of the reasons that the Russian State Duma is known as “the rabid printer” of laws. This assault on freedom of expression extends across various sectors, affecting legal entities and private individuals alike, including NGOs, media organizations, social media platforms, and journalists. The legislation also imposes restrictions on speech regardless of its source, inclusive of current events such as the Russian war in Ukraine, historical narratives in education, and the personal lives of citizenry such as in the case of the LGBTQI+ community and women’s and girl’s rights against domestic abuse. Authorities are systematically eliminating all potential avenues for expression, targeting street rallies, educational institutions, online spaces, etc. They employ both existing and newly created laws, swiftly adapting them to serve their specific control objectives. In August 2024 alone, the Duma made 151 amendments were made to these laws, further restricting freedom of expression and public assembly in parallel to the Kremlin’s high “historic” profile prisoner swap with the United States and Germany.

The broad and evolving scope of censorship in Russia ensures total control over public discourse, effectively closing off any potential loopholes for freedom of speech. Five pillars of this lawfare are 1) harsh penalties 2) the ambiguity and quasi-legal nature of legislative acts 3) triggers of legislative adjustments 4) pretexts for additional laws and 5) the cross-fertilization of politicized legal techniques across both democratic, illiberal, and authoritarian legal regimes.

Journalists often face specific targeting under these laws. The oldest example, the U.S. Foreign Agents Registration Act (FARA), was enacted in 1938 to counter Nazi propaganda. It regained relevance during the Trump administration, particularly with the Mueller investigation and actions against Russian state broadcaster RT. Unlike the Russian law, FARA imposes bureaucratic requirements without curbing speech and is subject to judicial scrutiny. Other countries have enacted similar laws since Russia’s law passed in 2012. For instance, China, Uganda, Australia, and Hungary have introduced laws targeting foreign-funded groups. In 2017, Hungary’s law faced criticism for violating EU laws. This year, Georgia attempted to pass a similar law but withdrew it following protests. Foreign-agent laws are also emerging in Kyrgyzstan and Republika Srpska, with proponents citing FARA as a model (Allsop, 2023). The EU considered introducing its own foreign-agent-type law, sparking concerns among civil-society groups about potential negative consequences and undermining democratic values. Kazakhstan recently established a list akin to Russia’s foreign agent registry, including many media-related entities. Human Rights Watch expressed concerns that this could lead to further restrictions and the arrest of journalists, as seen in Russia. The increasing use of foreign agent laws highlights a broader trend of suppressing dissent and tightening control over civil society in various countries (Krupsky, 2023).

Notably, the legislation of Russia, Belarus, and Central Asian states is distinctive from other sub-regional groups in that these countries classify ‘extremism’ as a criminal offense, while the Criminal Codes of Ukraine, Georgia, Estonia, and Armenia only contain provisions regarding ‘terrorism’ (Soladov, 2020, p. 136). Freedom House noted similar patterns in the excessive use of anti-extremism legislation in Russia, Belarus, Kazakhstan, Kyrgyzstan, and Uzbekistan. A significant shift occurred in 2013-2014, following Ukraine’s Revolution of Dignity. Various studies highlighted the simultaneous replication of restrictive public gathering

laws in Russia and Central Asian republics after the Ukrainian protests. Another research showed that authoritarian leaders responded to these opposition events by enacting stricter anti-extremism laws to prevent separatism in ethnic minority regions and maintain their grip on power (Soladov, 2020, p. 125).

The severe punishment for many of the “offenses” listed above is intended to serve as a deterrent to everyday citizens, activists, journalists, and advocates with what was once Russian civil society – including those in exile who reside in, travel in, or remain in communication with others throughout the Russian Federation and, ostensibly, within six members states Collective Security Treaty Organization (CSTO) which also includes Armenia, Belarus, Kazakhstan, Kyrgyzstan and Tajikistan. As a result, the penalties for certain crimes, such as organizing assembly that can be deemed “mass riots”, are now harsher than they were during the USSR period, with the maximum prison sentence increased from 10 to 15 years. Many of these non-violent “crimes,” such as discrediting the Russian military, carry consequences that are on par with those for committing murder, rape, terrorist attacks, human trafficking, slavery, and even genocide. In cases where the judgement does not (solely) result in imprisonment, offenders may face prohibitive multi-million-ruble fines and severe restrictions on their professional activities. These measures effectively cripple the individual or organization, often forcing them to shut down operations or end their careers altogether. The combination of draconian penalties and the broad categorization of offenses as serious crimes reflects a strategy aimed at stifling dissent and maintaining strict control over society.

Comparatively, the Foreign Agents Law in Russia or, as some of have argued, the implementation of the International Holocaust Remembrance Alliance's Working Definition of Antisemitism (IHRA WDA) in Germany and other countries, exhibit only a quasi-legal character (Krupsky, 2023). They often lack the necessary clarity and specificity required by legal standards, resulting in ambiguous and broad interpretations. The lack of clear definitions allows authorities to target individuals or organizations based on political or social objectives, rather than objective legal standards. This ambiguity creates a potential for abuse, enabling the suppression of dissent and stifling of public discourse. Consequently, the uncertainty and risk of arbitrary application can deter free speech and civic engagement and encourage self-censorship.

By analyzing significant events and the subsequent adoption of restrictive policies, one can identify three types of incidents that typically trigger or precede such legislation: mass protests or revolutions (as seen in Russia, Hong Kong, Belarus and the Middle East), interference by foreign states in domestic affairs (notably in the EU and the UK), and crises such as the COVID-19 pandemic (which prompted the introduction of laws targeting fake news, for instance). These patterns suggest that restrictive policies are often implemented in response to perceived threats or disruptions, reflecting a tendency to use legal measures to control and mitigate challenges to authority or stability.

Censorship laws are frequently introduced under the pretexts of national security, upholding sovereignty, and protecting citizens from disinformation and hate speech. National security is often cited to justify restrictions on speech and information deemed threatening to the nation's stability or safety. Similarly, the argument about the importance of upholding sovereignty is used to limit external influences and criticisms that are perceived as challenges to a country's independence and self-determination. Protecting citizens from disinformation, particularly in the digital age, is another common rationale, with governments claiming that such laws are necessary to prevent the spread of false or misleading information that could incite unrest or erode public trust. While these justifications are framed as protective measures, they can also serve to control public discourse and suppress dissent. This leads to reduced transparency and a diminished space for open debate, ultimately constraining the flow of information and affecting the freedom of expression in society.

Most alarming and paralleling the export of digital disinformation techniques, data reveals trends in the international export of legal frameworks among countries that are political corollaries and/or geographically proximate. In this manner, we parallels can be drawn between the adoption of the IHRA

Working Definition of Antisemitism (WDA) in the US, Canada, the UK, and the EU to and the legislation tightening Internet control in Russia and other Former Soviet Republics (FSR), exemplifies this pattern of legislative design as templates for adoption and export. Simultaneously, there are common developments across various regions, such as fake news legislation and third-party liability bills: the NetzDG law, which originated in Germany, has been adopted in multiple countries worldwide, particularly in those with authoritarian regimes.

The German Networks Enforcement Act (NetzDG, 2017) imposed intermediary liability on social media networks with more than two million registered users. These platforms must remove illegal content, including "hate speech" and "defamation of religions," flagged by users. Any content deemed "manifestly unlawful" must be taken down within 24 hours. Failure to remove illegal content is punishable by fines of up to 50 million euros. The categories of illegal content violate international human rights standards (Mchangana & Alkiviadou, 2020, p. 4). Amendments adopted in 2021 require social media platforms to report certain types of "criminal content," along with the IP addresses, last logins, user passwords, and port numbers of the user who shared such content, directly to the Federal Criminal Policy Office (BKA). This provision has been legally challenged by major platforms (Holznagel, 2023, p. 111). Though intended to ensure legitimate regulation, it has become a model for more restrictive measures in authoritarian regimes. Since the adoption of the act, at least 24 countries have passed similar bills, often referring to the NetzDG as a model, only 4 of them are designated as "free" by the Freedom house (Mchangana & Alkiviadou, 2020, p. 2). Ironically, the German government repealed the NetzDG in 2024 (Holznagel, 2023, p. 108).

A report published by UNESCO in 2022 shows that 80% of countries still criminalize defamation (UNESCO, 2023). The report highlights that since 2016, 57 laws and regulations in 44 countries have been adopted or amended with vague language and disproportionate punishments, jeopardizing online freedom of expression and media freedom. In Western Europe and North America, 20 out of 25 states still have criminal defamation laws. Between 2003 and 2018, five countries abolished criminal defamation and insult laws, while one partially repealed them. These laws result in disproportionate damages and have a chilling effect on freedom of expression and journalism. Of additional analytical importance is the endorsement and implementation of the International Holocaust Remembrance Alliance's "Working Definition of Antisemitism" (IHRA WDA) which conflates antizionism and antisemitism in the EU, its Member States, the UK, Canada and the US, has led to significant restrictions on freedom of expression and assembly (ELSC, 2023, p. 5). Despite being declared "non-legally binding" in the EU, the IHRA WDA is treated as law, and is often used by pro-Israel advocates to silence dissent, disproportionately targeting Palestinians and Jewish advocates for Palestinian rights leading to job loss and reputational damage. In Germany, the IHRA WDA has been used to pass resolutions and laws against the BDS movement and far-right extremism, risking the misinterpretation of legitimate criticism of Israel as antisemitism. Recent legislative proposals to criminalize denial of Israel's right to exist and amend immigration laws further risk chilling free speech and arbitrary interpretation of antisemitism (ECF, 2024, pp. 14-16). In contrast and for the sake of comparison, blasphemy laws were found in 71 countries from all regions of the world. Regionally, 22.5% of the laws found are from Europe. 62% of these laws deviate from many of the international and human rights law principles examined. The data indicate that the majority of laws do not fully respect international standards of freedom of opinion and expression (Fiss & Kestenbaum, 2017, p. 3).

It becomes evident that authoritarian countries and democracies alike use similar legal frameworks to address issues like hate speech and misinformation, but the outcomes can diverge significantly. Instead of trying to avoid ambiguity and vagueness in the legal texts, some governments exploit these flaws to bolster their control over public discourse. Consequently, laws intended to safeguard freedom of expression among

liberal democracies can act as a double-edged sword, simultaneously enhancing free speech domestically while stifling free speech globally.

The Market and Infrastructure of Digital Lawfare

In conjunction with these legislative feats of lawfare, the control of digital informational landscapes sees surveillance and data collection as critical instruments for modern nation-states (Huang & Tsai, 2022), even more so for authoritarian regimes, whose reliance on information control makes these regimes particularly vulnerable, especially during crises (Mansted, 2020). Ensuring political compliance and identifying dissent within the population becomes vital in order to pre-empt potential threats to their rule before they manifest into larger challenges (cf. Huang & Tsai, 2022; Weber, 2019; Xu, 2021). This approach is most evident in the practices of countries like China and Russia, where sophisticated technologies such as facial recognition, internet monitoring, and social media surveillance are deployed to suppress opposition and maintain autocratic governance.

China relies extensively on censorship and strategic information dissemination, underpinned by comprehensive surveillance systems such as the Great Firewall, which blocks access to major Western platforms like Google and Facebook (Weber 2019). In contrast, Russia employs pervasive surveillance, self-censorship, and strategic information dissemination to maintain domestic stability, but its censorship mechanisms are less sophisticated and more prone to over-blocking than China's.

In Turkey, the government under Recep Tayyip Erdoğan, has developed a sophisticated system of internet control. Drawing on the University of Toronto Citizen Lab's categorization of internet controls (Deibert 2015), Topak et al. (2022) argue that Turkey's digital surveillance system includes first-generation measures like website blocking, second-generation practices involving surveillance of citizens' online activities without judicial oversight, and third-generation tactics such as the use of state-sponsored trolls ("AkTrolls") and advanced spyware. Legal frameworks, including post-2016 attempted coup decree laws, have further enhanced the state's ability to monitor and censor digital content, with social media platforms being compelled to store user data locally and comply with content removal requests. This is exemplified by the August 2024 nine-day ban of Instagram by the Turkish state, following allegations that the platform censored posts related to the Palestinian militant group Hamas. The ban was lifted after Instagram agreed to comply with Turkish authorities ('Turkey Blocks Instagram amid "Censorship" Row', 2024; 'Turkey Restores Access to Instagram after 9-Day Block', 2024). The Turkish state's use of Deep Packet Inspection (DPI) technology and spyware like FinFisher, coupled with coordinated disinformation campaigns, mirrors the techniques employed by authoritarian regimes such as Russia and China (Topak et al., 2022). The alignment with these global powers underscores Turkey's integration into a broader network of digital authoritarianism, where propaganda and control are exercised through both technological means and legal mandates.

Venezuela has similarly intensified its digital authoritarian practices, particularly in response to political instability (Puyosa 2021). The Venezuelan government has engaged in "information warfare", leveraging bots and trolls to manipulate social media narratives, spread propaganda, and target dissidents, a practice that escalated significantly after 2017. These efforts are not isolated, as they involve coordination with foreign actors from Turkey, Russia, and Spain, reflecting a transnational dimension to Venezuela's digital repression. Russian state-sponsored trolls and Turkey's "AK Trolls", the author argues, coordinated with Venezuelan "Chavismo" trolls to polarize Venezuelan society in the wake of 2017 protests (Russian trolls) and amplified pro-Maduro content internationally (AK Trolls). Puyosa (2021) further points to the evidence of the Venezuelan Embassy in Madrid and the Catalan independence movement coordinated 2019 pro-Maduro Twitter campaigns such as the one using the hashtag "#NoEnMiNombre". The Venezuelan state's control extends to the direct censorship of digital media through mechanisms like DNS spoofing and the blocking of opposition websites by regulatory bodies such as the National Commission of Telecommunications

(CONATEL). These actions illustrate a comprehensive approach to digital authoritarian practices, where the Venezuelan state seeks to dominate the online space and stifle grassroots movements.

According to recent studies on authoritarian practices in the Middle East and North Africa (MENA) region, various regimes have adopted both traditional and modern methods to maintain control in increasingly complex political environments. Maghraoui (2022) discusses Morocco's layered approach to digital control and repression, combining legal persecution, financial manipulation, and digital surveillance to silence dissent, particularly among journalists. In a similar vein, Davidson (2022) describes the UAE's evolving authoritarian toolkit, which includes extensive digital surveillance and the use of spyware to control both domestic and international opposition. These findings reflect a broader trend identified by Topak et al., (2022a) where authoritarian regimes across the region are increasingly integrating modern technologies with established repressive practices to sustain their power amidst both internal and external challenges.

Recent surveillance controversies in democracies highlight growing concerns over the use of authoritarian techniques in democratic states. For example, Greece has been embroiled in a controversy involving the use of spyware, specifically the "Predator" software, to surveil journalists, politicians, and other public figures. The scandal, which emerged in 2021, led to resignations within the government and ongoing judicial investigations. Despite governmental denials, the situation has raised serious concerns about transparency and the misuse of surveillance powers in the country. The bill proposed in response to the controversy aimed to legalize the Greece state's use of spyware, while criminalizing its possession or use by non-state actors. However, it has been condemned for undermining the oversight powers of independent bodies like the Hellenic Authority for Communication Security and Privacy (ADAE), potentially legitimizing surveillance abuses rather than preventing them (Greece, 2022).

Further, transatlantic data flows between the EU and the U.S. have sparked controversy, especially after the establishment of a secretive court known as the Data Protection Review Court to address privacy concerns related to transatlantic data transfers between the U.S. and the EU, by the Biden administration. This court has been criticized for potentially offering more privacy protection to Europeans than to Americans, raising questions about fairness and the extent of surveillance powers (Ng & Sakellariadis, 2024).

Export of Authoritarian Tools & Narratives

Countries like China and Russia not only apply the above legal techniques domestically but also export authoritarian technologies and practices to other authoritarian regimes, thereby expanding their influence and creating a network of digital authoritarian states – their own "technosphere" (Weber, 2019; Feldstein, 2021; Polyakova & Meserole, 2019). At the same time, they also adopt and adapt these techniques from democracies as leading "cyber powers", especially in the digital and media spheres (Hutchings et al., 2024; Nakashima & Warrick, 2012).

The export of authoritarian tools, including surveillance technologies, censorship methods, and repressive strategies, has become a hallmark of modern authoritarianism. Simultaneously, the view that these practices originate in autocracies, rather than being a feature of a modern state with any political system (even if these practices take different form and are seen differently by actors in autocracies and democracies), is problematic and should be critically interrogated, as it does not properly reflect the full range and nature of these complex dynamics. In certain cases discussed earlier in this report, democracies such as the U.S., Israel, and South Korea have at times been "exporters", while Russia, for example, has been a learner. Acknowledging this, it needs to be recognized that China and Russia, in particular, have recently played leading roles in the diffusion of authoritarian practices, using formal channels like the Belt and Road Initiative (BRI) and the Commonwealth of Independent States (CIS) to disseminate these practices in the Global South and the Post-Soviet space, among other regions (Weber, 2019).

The exportation is not only about commerce but is strategically aimed at reinforcing authoritarian governance structures globally (Weber, 2019). Through the BRI, China has provided surveillance

technologies to countries across Africa, Latin America, and Southeast Asia, thereby creating a network of states that rely on Chinese infrastructure to maintain control over their populations (cf. Gravett, 2022). These technologies include facial recognition systems, internet monitoring tools, and advanced data analytics platforms, which are integrated into the security apparatuses of recipient countries (cf. Gravett, 2022; Huang & Tsai, 2022; Weber, 2019).

In Venezuela, for instance, the adoption of Chinese surveillance technologies has significantly bolstered the government's ability to suppress opposition and control public dissent (Berwick, 2018; Moreno, 2022). Greitens (2016) notes that these technologies were instrumental in monitoring and quelling protests, thereby ensuring the stability of the regime. Similarly, in Turkey, surveillance technologies imported from China have been used to enhance the state's ability to monitor and control its citizens, reinforcing Erdoğan's authoritarian rule (cf. Topak et al., 2022).

Russia's role in exporting authoritarian tools is equally significant. Through the CIS and other less formal networks, Russia has provided surveillance technology and cyber expertise to several former Soviet states, including Kazakhstan, Belarus, and Kyrgyzstan, enabling these regimes to resist democratization and maintain tight control over their populations (Polyakova & Meserole, 2019). China and Russia have developed distinct models of digital authoritarianism that they are now exporting globally. China's model, characterized by advanced surveillance and extensive internet censorship systems like the Great Firewall, has been exported to at least 18 countries (Polyakova & Meserole, 2019). Russia, on the other hand, has focused on lower-cost tools such political repression of opponents and civil society as well as extensive legal framework enabling further monitoring and censorship by the telecom watchdog Roskomnadzor (Polyakova & Meserole, 2019). Russia's systems like the SORM (System of Operative-Search Measures) have been adopted by several post-Soviet states and are designed to monitor communications and internet activity comprehensively (Polyakova & Meserole, 2019).

China and Russia have begun to collaborate more closely on digital surveillance, monitoring, and censorship tactics as early as 2017, as evidenced by the leaked files (Belovodyev et al., 2023; Scott, 2023). Chinese officials reportedly sought Russia's expertise in media regulation and handling public dissent, while their Russian counterparts explored strategies for disrupting tools like virtual private network (VPN) and Tor (The Onion Router – a software that enables anonymous online communication), cracking encrypted internet traffic, and controlling messaging platforms (Belovodyev et al., 2023; Scott, 2023). This collaboration between China and Russia represents a broader trend of authoritarian regimes supporting each other, not only in terms of technology transfer but also in strategic alignment against democratic governance. This has created a robust global alliance that actively undermines liberal democratic institutions and promotes authoritarian governance across various regions, including Post-Soviet space, Southeast Asia, Africa, and Latin America.

Cottiero and Emmons (2024) expand on this by arguing that modern authoritarian collaboration goes beyond the mere export of technologies. It involves the active sharing of resources, the legitimization of repressive practices, and the mutual support of regimes in times of crisis. This collaboration is designed not just to maintain power within individual states but to undermine democratic norms and challenge the liberal international order. To counter these trends, Cottiero and Emmons (2024) suggest that the international community must develop strategies to disrupt these networks, counter disinformation, and cut off authoritarian actors from critical resources.

DOMAIN 3 – Digital Authoritarianism & Non-State Actors

Mis- and disinformation campaigns have been used as a powerful authoritarian tool for state actors seeking to manipulate public opinion, maintain control, and discredit opposition both domestically and internationally. These campaigns often involve the production and dissemination of falsehoods and misleading information through state-controlled media and social media platforms through state-affiliated or state-sponsored actors. Studies have shown that in 2020 at least 81 countries, including democracies, had organized social media manipulation programs or engaged in computational propaganda online (Bradshaw et al., 2021). In most of these countries either governments, government affiliated entities, political parties or private firms used social media as a part of a political strategy aimed at misleading users, suppressing political activism, and targeting opponents (Bradshaw et al., 2021).

Systemic Industrialized Persuasion

It is necessary to recognize that, historically and today, disinformation has taken many forms in Western countries including public relations, promotional culture, lobbying, and other forms of political consulting. For critical disinformation scholars, deception has been part of the Western socio-political fabric for decades, and these forms of deception have been kept separate from contemporary disinformation studies because they are treated as normal parts of Western society. And yet, these forms of deception ultimately share many of the characteristics and dangers associated to contemporary disinformation framed by the particularities of Western, neoliberal political economies. In other words, the deception we as academics so often critique does not receive public scrutiny when it is industrialized and systematic.

The critical subfield of disinformation studies argues that Western persuasion takes many forms. Beyond the typical political propaganda of which it accuses foreign states such as Russia and China, the West engages in many more subtle forms of propaganda, including public relations and marketing. Public relations for instance is simply “deception-for-hire” – money buys you access to professional communication expertise, which seeks to manipulate opinions and present information deceptively for a particular end (Edwards, 2021). More generally, Edwards (2021) points out that public relations firms and actors have been successful in painting the work as good and professional communication, unlike the shadowy “other” bad actors which engage in disinformation. In this way, public relations is a form of “organized lying” that sidesteps responsibility for the current disinformation crisis (Edwards, 2021, pp. 167–169). This is part of a broader phenomenon of public relations company agreeing to take on increasingly politically charged and partisan contracts outside of the realm of formal political institutions. In *The New York Times*, journalist M. Fisher writes: “Private firms, straddling traditional marketing and the shadow world of geopolitical influence operations, are selling services once conducted principally by intelligence agencies. They sow discord, meddle in elections, seed false narratives and push viral conspiracies, mostly on social media. And they offer clients something precious: deniability.” (Fisher, 2021) Simply put, the PR industry is complicit in the disinformation problem, not only because it “casually” produces “organized lying” on a wide scale, but also because it continues to do so while protecting the legitimacy of the profession at large, allowing these realities to endure (Grohmann & Corpus Ong, 2024a).

Another type of systemic industrialized deception that has been normalized by the West is advertising and marketing. As Hearn (2011) recalls from Wernick’s work (1991), there are cultures where promotional discourse is ubiquitous – in these cultures, truth and reason are not valued, but winning is valued, and the goal is to win “attention, emotional allegiance, and market share.” (Hearn, 2011; Wernick, 1991) Recalling the neoliberal debate above, neoliberal systems do not have incentives to protect citizens against the excesses of capitalism, which partially explain why big tech platforms have wreaked havoc on democratic discourse.

But beyond this socio-political and economic realities, democratic governments in neoliberal systems have also mimicked the types of persuasion inherent in promotional culture. As Glaser (2013) argues, these subliminal forms of policy and persuasion erode “vital distinctions between government, psychology, and marketing. ... We are no longer appealed to as thinking citizens. We are simply flawed units to be prompted into spending more and costing the state less. The propaganda lies not only in the political-corporate manipulation of the public but also – most insidiously – in the way this is cloaked in the language of ideology-free empiricism and the semblance of autonomy: the idea that people are being nudged “to make better decisions for themselves.” (Glaser, 2013) Glaser also argues that social media provided a veneer of openness and people-power, while in reality, the online advertising industry has created an objective now to “make your customers a partner in the selling process. ... [Another example of] western propaganda's habit of masquerading as its opposite ”(Glaser, 2013) At the time of writing, Glaser had pointed to joint report by the U.K.'s Cabinet Office and the Institute for Government describing how using behavioural sciences to inform policy can help nudge citizens to make better decisions for themselves (Dolan et al., 2010). And while some nudges are innocuous (e.g., encouraging citizens to eat healthy), the critical point for Glaser is that these types of nudge units erode “vital distinctions between government, psychology and marketing” (Glaser, 2013).

Key to the authors' concerns and to the critical approach to disinformation is that when deception is industrialized and systemic, it is hidden in the socio-political fabric, interwoven so deeply in Western values that it is difficult to unearth, to critique, and to compare to the forms of disinformation that are so often highlighted by the same authorities engaging in their own forms of deception. Some authors argue that these are issues of “definitional vortexes”; disinformation scholars cannot continue to study disinformation with these overly broad definitions without acknowledging that they encompass these forms of systemic industrialized deception perpetrated by the West (Harsin, 2024). Moving beyond the definitional issues, disinformation scholarship has also been criticized for neglecting to acknowledge that the industry underpinning disinformation operations^{3/4}or “Big Disinformation”^{3/4}mirrors colonialist dynamics, and that these narratives are technologically deterministic.

First, operations and the digital labour which ensues are often outsourced by resource-rich actors to actors Global Majority countries (Ong & Cabañes, 2018). Individuals, often operating in precarious labour conditions due to the “gig economy” style of work, are recruited into disinformation labour by elite politicians collaborating with upper-middle class marketing consultants (Grohmann & Corpus Ong, 2024a). For these digital labourers, disinformation work can often be the less precarious option depending on an individual's socio-political and economic circumstances. Moreover, acknowledging this reality means demystifying the “human infrastructures behind the fake news” (Grohmann & Corpus Ong, 2024b, pp. 3–4). In this way, disinformation scholarship cannot legitimately make its arguments without acknowledging and incorporating the dynamics of digital labour studies, because there are inherent inequalities and coloniality in the production of disinformation (Grohmann & Corpus Ong, 2024b).

Several distinct actors and techniques are usually identified in relation to organizing, carrying out, facilitating and abetting dis/misinformation campaigns. While the exact configuration of actors will depend on the state, the type of campaign and its goals, a general pattern emerges: (a) solely state actors (e.g., trolling / astroturfing dis/misinformation efforts by Russia's GRU (Twitter Moderation Research Consortium - X Transparency Center, n.d.), China's “50 Cent Army” (Han, 2015), or U.S. Military (Bing & Schectman, 2024)), (b) state actors-private contractors arrangements (e.g., dis/misinformation campaigns by Russia's state-sponsored Internet Research Agency (IRA) (Bradshaw & Howard, 2017) and Social Design Agency (SDA) (COUNCIL DECISION (CFSP) 2023/1566 of 28 July 2023 Amending Decision 2014/145/CFSP Concerning Restrictive Measures in Respect of Actions Undermining or Threatening the Territorial Integrity, Sovereignty and Independence of Ukraine, 2023; Miller, 2024), the Iranian state-backed organization International Union of Virtual Media (IUVM) (Stubbs & Bing, 2018; *Treasury Sanctions Iranian Entities for*

Attempted Election Interference, 2024), “keyboard warriors”/ cyber troops hired to post pro-Duterte content and target opposition in the Philippines) (Bradshaw & Howard, 2017), (c) solely private actors (e.g., consultancy firms, marketing agencies, information technology (IT) and “big data” companies) motivated financially or politically / ideologically and funded by donors or clients politically aligned with certain causes or self-funded (cf. Bradshaw et al., 2021).

“Information disorder” actors employ a variety of techniques, which can overlap and intersect. These include (1) trolling – usually coordinated online attacks aimed at discrediting, harassing, or silencing opponents, often using aggressive language and ad hominem attacks (Bradshaw & Howard, 2017; Galeotti, 2017; Zannettou et al., 2019). Trolling typically involves disruptive and provocative online behaviour and can employ various rhetorical and affective devices (e.g., irony, sarcasm, appeal to emotion, etc.) (cf. Hardaker, 2010, 2013). Recent examples include Russian and Venezuelan state-sponsored “trolls farms” used to intimidate opposition figures domestically, harass and attack regime critics overseas (Puyosa, 2021; Zannettou et al., 2019). The first known example of setting up a “troll farm” to influence the outcome of elections can be traced back to South Korea (Bradshaw & Howard, 2017; Keller et al., 2020). In 2012, the South Korean National Intelligence Service (NIS) was implicated in a scandal where it orchestrated a coordinated online campaign to sway public opinion in favor of the conservative candidate, Park Geun-hye, during the presidential election. This operation involved creating fake social media accounts and posting pro-government comments in an attempt to influence voters.

(2) Astroturfing – imitating authentic user activity and grassroots movements by using online/social media accounts with fictitious or stolen online identities to simulate public support or opposition (Keller et al., 2020; King et al., 2013). Paid commentators from Russia’s IRA (“troll farm”) or China’s “50 Cent Army” posting tailored messages on social media to give the impression of widespread popular support for a cause or political candidate illustrate this (Bradshaw & Howard, 2017; Han, 2015). First online astroturfing efforts in the context of elections seemed to have occurred in the U.S. around 2010 U.S. midterm elections and the 2009 Massachusetts special election (Ratkiewicz et al., 2011). Some U.S. Tea Party organizations such as the Tea Party Express with close ties to the U.S. Republican party, have also been accused of astroturfing (Dyke, 2016, p. 41).

(3) Amplification – the use of “bots” (i.e. automated accounts) or coordinated human activity to artificially inflate the popularity of specific content or narratives (Howard et al., 2018). For example, Russian IRA “bots” amplified their own and other users’ divisive content on Twitter during the 2016 U.S. presidential election (*Publications | Intelligence Committee*, 2020).

(4) Manipulated Media – the creation and dissemination of false or misleading information, including deepfakes, fictitious news articles, doctored images, and videos (Citron & Chesney, 2019). Examples include the use of deepfakes like an AI-generated audio recording in Slovakia used to falsely accuse a politician of planning to rig an election or a video falsely depicting a U.S. State Department official stating that a Russian city is a legitimate target for Ukrainian strikes using U.S. weapons (Bond, 2024; Kottasová, 2024).

(5) Mass Reporting – coordinated reporting of content or accounts to social media platforms, triggering their automated systems to take down or demote content (Gleicher, 2021; ‘Opinion | The Bad Guys on Social Media Are Learning New Tricks’, 2021). For instance, the network in Vietnam, which orchestrated false reports against activists and critics of the Vietnamese government to have them removed from Facebook, imitating real users and using duplicate accounts to submit hundreds or thousands of complaints through abuse reporting tools (Gleicher, 2021).

(6) Brigading – coordinated attacks on social media posts by groups aiming to overwhelm a particular discussion or viewpoint (Marwick & Lewis, 2017). Example: a network of accounts from Italy and France that targeted medical professionals, journalists, and elected officials with mass harassment. Meta (Facebook) investigation connected this activity to the anti-vaccination conspiracy movement “V_V”. The operation used

a mix of authentic, duplicate, and fake accounts to flood comments on posts of news outlets and individuals, aiming to intimidate and suppress opposing views (Gleicher, 2021).

(7) Fake Fact-Checking – the creation of false fact-checking sites or posts that appear to debunk legitimate information, thereby confusing the public (Kovalenko, 2024; Thomas, 2024). Kremlin-linked website “War on Fakes” (voina s feikami) is promoted as a fact-checking resource but actually pushes false narratives that support Russian state propaganda (Kovalenko, 2024).

(8) Micro-Targeting – the use of data analytics to target specific demographic groups with tailored dis/misinformation campaigns (Cadwalladr & Graham-Harrison, 2018; Confessore, 2018). For example, Russia’s IRA micro-targeted users on multiple social media platforms with tailored political advertisements and targeted messages on divisive issues, such as race, religion, and gun rights (*Publications | Intelligence Committee*, 2020). Cambridge Analytica’s data was also reportedly used to micro-target U.S. voters during the 2016 Presidential Election and UK voters during the Brexit campaign (Cadwalladr & Graham-Harrison, 2018; Confessore, 2018).

(9) Information Laundering – the spreading of dis/misinformation through seemingly credible intermediaries to give it an air of legitimacy (Pomerantsev, 2019). For example Russian dis/misinformation often spreads through proxy websites, obscure blogs or apparently legitimate social media accounts before being picked up by media in target countries (Pomerantsev, 2019; ‘The Kremlin’s Efforts to Covertly Spread Disinformation in Latin America’, 2023).

Disinformation is also a regime of private labour and state-sector employment. Unlike “cyber troops”, whose organization or coordination is, at least in part, political, some actors engage in dis/misinformation exclusively for commercial gain as mentioned earlier in this report. Automated accounts (“bots”) or human-operated accounts (“trolls”) can also be used for political purposes or, for example, to simulate public support for brands and products (Lock & Ludolph, 2020). The Israeli-based Archimedes Group’s dis/misinformation campaigns to disrupt elections across Africa, Latin America, and Southeast Asia using trolling and astroturfing (Bradshaw et al., 2021, p. 9) provide a clear example of how private contractors are used to further authoritarian political objectives while seemingly being primarily motivated by financial gain (‘Facebook Busts Israel-Based Campaign to Disrupt Elections in Various Countries’, 2019; Timberg & Romm, 2019). Similarly, the cases of Russia’s IRA interfering in U.S. elections (*Publications | Intelligence Committee*, 2020) and the Israeli company STOIC targeting U.S. audiences and politicians to further pro-Israeli sentiments online (Pro-Israeli Influence Network. New Findings, 2024) highlight the convergence of private financial interests and state political agendas. Research highlights how these contractors created fake social media accounts to influence political outcomes, employing tactics such as the use of bots and sock puppet / troll accounts to promote and amplify messages beneficial to state actors (Bradshaw et al., 2021; Pro-Israeli Influence Network. New Findings, 2024; *Publications | Intelligence Committee*, 2020).

The Chinese state also employs state-sponsored internet commentators, often referred to as the “fifty-cent army”, who anonymously engage in online discussions to promote pro-state narratives mainly domestically (Han 2015). This tactic is part of a broader adaptation of China’s state propaganda system to the digital age, aiming to maintain regime stability and legitimacy. However, the strategy often backfires due to the commentators’ lack of motivation, exposure by other users, and the persistence of outdated propaganda practices, ultimately undermining the operation’s credibility and fueling public distrust. Similar operations targeting China critics globally have recently been linked to Chinese law enforcement (Nimmo et al., 2023).

OpenAI (AI and Covert Influence Operations: Latest Trends, 2024), the creator of ChatGPT, highlights the misuse of its AI models by various threat actors to carry out covert influence operations aimed at manipulating public opinion and influencing political outcomes. The OpenAI report details influence operations by several state-linked actors: “Bad Grammar”, a Russian campaign, used AI-generated, poorly written comments on Telegram to target audiences in Ukraine, Moldova, and the Baltic States, promoting pro-Russian narratives. “Doppelganger”, also from Russia, targeted Europe and North America with anti-

Ukraine content in multiple languages on platforms like 9GAG and X. “Spamouflage”, linked to Chinese law enforcement, aimed at global audiences, including Chinese dissidents, using AI to generate pro-China content and discredit critics across platforms like X, Medium, and Blogspot. The Iranian International “Union of Virtual Media (IUVM)” focused on anti-U.S. and anti-Israel content, disseminating AI-generated articles on its websites and social media. Lastly, “Zero Zeno”, an Israeli operation run by a commercial firm STOIC, targeted audiences in Israel, Canada, and the U.S. with AI-generated content supporting Israel and criticizing Hamas, spread across Facebook, Instagram, and X. These operations struggled to engage audiences because their AI-generated content was often generic, poorly targeted, lacked authenticity, relied on fake interactions, and was undermined by human errors, failing to resonate with real users.

State Use of Non-State Actors

In democracies, the manipulation of information and public opinion is often driven by various actors, including political parties, media outlets, and private entities, each with their own agendas. This decentralized approach in democracies contrasts with the state-directed strategy observed in Russia, where the media and other platforms are systematically used to advance state interests under a unified narrative. This difference highlights the qualitative divergence in how such techniques function across these political systems, with authoritarian regimes’ approaches often being more aligned with coordinated disruptive aims to destabilize liberal orders globally (Hutchings et al., 2024).

The examples of Russia and China illustrate that the scope of actors, propagating authoritarian practices can be only loosely defined and would greatly depend on the specific country. At the same time, the following types of “information disorder” actors are often distinguished in literature: government agencies, politicians and political parties, private contractors, civil society organizations, citizens and influencers (Bradshaw et al., 2021). These actors can operate both in authoritarian regimes and liberal democracies as well as transnationally (Bradshaw et al., 2021).

Acknowledging the complexity of “state” via-a-vis “non-state” distinction, it is useful to outline the specific actors typically described as “non-state” by researchers in authoritarian contexts. These actors are frequently defined as individuals or organizations that operate apparently independently from the systematic and direct state control but can significantly influence or support the authoritarian regime’s policies (cf. Chase & Chan, 2016). These actors might receive state funding directly or indirectly through various channels including government contracts, loans, grants, etc. (Galeotti, 2016b, 2017; Huang & Tsai, 2022). Although they might be acting in the state’s interests or work on specific state-funded projects, their administrative links to the state are often obscure (Galeotti, 2017; Huang & Tsai, 2022; Sallai & Schnyder, 2021). The types of non-state actors in authoritarian contexts include private contractors, corporations, non-governmental organizations (NGOs), civil society organizations, political parties and lobbying groups, militant groups (private and quasi-private military organizations), private and quasi-private security organizations, criminal networks, and influential individuals such as business magnates or media personalities (Galeotti, 2020; Ostrovsky, 2015). Their roles can vary from providing technological support, consultancy and facilities to engaging in propaganda/mis/disinformation and cyber activities (e.g., hacking, disseminating stolen data, disrupting digital facilities (Clark, 2020; Galeotti, 2017; *Publications | Intelligence Committee*, 2020).

The United States has enshrined laws aimed at protecting citizens from surveillance and information campaigns run by the U.S. government. In the U.S., the proposed Government Surveillance Reform Act aims to address the apparent abuse of Section 702 of the Foreign Intelligence Surveillance Act (FISA), which is intended for foreign intelligence, but has been used to conduct warrantless searches of Americans’ communications. A new bill, introduced in 2023, seeks to reform these surveillance practices by adding stronger privacy protections, but concerns about government overreach remain (Wyden et al., n.d.). However, an intricate network of military, federal, state, and local governing bodies, legal institutions, corporations, private security and military companies, and law enforcement bodies make use of gaps in these

protections in such a way as to recycle digital authoritarian techniques and information operations against domestic populations to further state policy and maintain the socioeconomic and political status quo.

What follows is an overview of multiple investigative reports from the news media concerning American disinformation and surveillance initiative both domestically in relation to the Dakota Access Pipeline protests #NoDAPL and the role of the private security contractor TigerSwan who policed surveilled the protest and also abroad including Operation Earnest Voice and the Trans-Regional Web Initiative – both coordinated by sectors of the U.S. military, serving to further U.S. military objectives. For brevity's sake we will only examine one case here:

As detailed by an investigation from the Guardian Newspaper in the UK, Operation Earnest Voice (2011- Present OEV) is an influence campaign operated by the United States Central Command (CENTCOM) to control online conversations and narratives surrounding U.S. military actions. It was designed to “secretly manipulate social media sites by using fake online personas” that posted and spread “pro-American propaganda” (Fielding & Cobain, 2011). The operation launched in 2010 with a US\$2.76 million contract for software that would allow up to 50 military personnel to each control up to 10 online personas from MacDill Air Base in Florida. These personas would be complete with “background, history, supporting details, and [plausible] cyber presences” and could “originate in nearly any part of the world” without “fear of being discovered by sophisticated adversaries” (“Persona,” 2010). The contract was awarded to Ntrepid, a California startup that owned the VPN tool Anonymizer, which was previously used to combat internet censorship. The operation was designed to combat al-Qaeda supporters and anti-coalition sentiment in Iraq, but it gradually expanded and received an additional US\$200 million in funding to operate campaigns in Pakistan, Afghanistan, and other parts of the Middle East. The software allowed the U.S. military to manufacture a “fake consensus” on social media platforms and in other online conversations by “crowd[ing] out unwelcome opinions” and offering “smoother commentaries” on reports of U.S. actions (Fielding & Cobain, 2011).

As it is unlawful for propaganda to target U.S. audiences, the operation primarily posted content in Arabic, Farsi, Urdu, and Pashto, and a CENTCOM official specifically stated that it would not operate on Facebook, Twitter, nor any other English speaking or U.S.-based platform (Fielding & Cobain, 2011). However, an investigation by the Stanford Internet Observatory and Graphika found thousands of accounts on Twitter and Facebook linked to U.S. government-backed operations. These accounts often featured AI-generated deep fake profiles, used “memes and short-form videos,” attempted to launch petitions and hashtag campaigns, and even “posed as independent media outlets” (Stanford Internet Observatory, 2022, p. 3). Stanford found that in 2022 some of CENTCOM’s Twitter accounts “posed as Iraqi activists” and accused Iran of “threatening Iraq’s water security” and “flooding the country with crystal meth” (p. 44). Other accounts in Afghanistan claimed that Iran was harvesting the organs of Afghan refugees, and that refugees would be deported unless they joined militias fighting in Syria or Yemen (p. 40). The report found that, at the time, a “vast majority” of CENTCOM’s posts “received no more than a handful of likes or retweets,” with the average tweet receiving 0.49 likes and 0.02 retweets (p. 3).

As uncovered by the international news agency Reuters, During the COVID-19 pandemic, the U.S. military also launched a campaign in the Philippines to spread disinformation about the Chinese vaccine using the hashtag #Chinaangvirus, which translates to “China is the virus” (Bing & Schectman, 2024). One of the tweets from 2020 read: “COVID came from China and the VACCINE also came from China, don’t trust China!” The campaign spread to countries in Central Asia and the Middle East, where it targeted Muslim audiences with disinformation claiming that the vaccines contain pork (Bing & Schectman, 2024). The COVID disinformation campaign eventually terminated in 2021.

After Twitter granted public access to its internal documents in 2022, journalists found that Twitter provided “direct approval and internal protection to the U.S. military’s network of social media accounts and online personas” (Fang, 2022). Both Facebook and Twitter had removed fake accounts that were likely

attached to OEV in 2020, however, officials from both platforms participated in classified briefings with the Pentagon to warn them of the potential for foreign adversaries to uncover U.S. associations with the accounts (Nakashima, 2022). Military officials later submitted, and Twitter subsequently approved, batch whitelisting requests for accounts that were flagged as spam for engaging with extremist groups. The military also requested “priority service” for some of its accounts, including @yemencurrent, which announced U.S. drone strikes in Yemen and posted about how strikes against Houthi rebels were “accurate” and “killed civilians, not terrorists” (Fang, 2022). On May 16, 2022, Twitter purged many of CENTCOM’s accounts, though some remained active and Stanford’s report suggests the U.S. has rebuilt its capabilities.

When these tactics are brought home, the mis/dis-information campaigns and militarized suppression of Water Protector encampments, for example, can be seen to also empowered lobbyists and conservative legislatures to enact anti-protest legislation across the country. The effort reveals continued cooperation between corporations, governments, law enforcement bodies, Private Security and Military Contractors and lobbyists to prevent protests before they start. As of April 2023, “corporate lobbyists [have] spurred the passage of so-called critical infrastructure laws widely understood to stifle fossil fuel protests in 19 states across the U.S.” (Brown and Sadasivam, 2023a). At the same time, the involvement of private contractors in corporate security and anti-protest action has proliferated. Class action lawsuits and other investigations revealed that, since 2016-2017, the private contractor TigerSwan has pitched their “counterinsurgency approach” toward protest suppression to petrochemical corporations, U.S. states, and intergovernmental bodies including ConocoPhillips, Dominion, the state of Nebraska, and the United Nations (Brown and Sadasivam, 2023a; Brown, 2020; Downie, 2016). They have secured further security and mis/dis-information work with Energy Transfer Partners to secure the Mariner 2 Pipeline in Pennsylvania and the Rover Pipeline in Ohio and West Virginia (Brown and Sadasivam 2023a).

The above case studies demonstrate a concerted effort by the U.S. government and corporate, private military/security, institutional, and individual partners to shape the information landscape, and consequentially, the geopolitical, social, and economic landscapes both domestically and abroad. These mis/disinformation campaigns the authoritarian practices deployed in their operations, are producing global impact regardless of whether the original campaign began in an authoritarian or liberal democratic regime.

DOMAIN 4 – Marketcraft & Platform Power

In the digital era, facing an uncertain global environment and an increasingly disordered information landscape interfered with by both state and non-state actors, sustainably maintaining strategic autonomy across the technological and communication economies for a sovereign state is crucial. The supranational European Union, for example, has reintroduced the concept of “Strategic Autonomy” in 2017 across hundreds of official documents to consolidate actionable plans for its member states. However, the terms “sovereignty” and “strategic autonomy” have both evolved over time and space. Strategic autonomy, as defined by the Ministry of Economic Affairs of the European Union, is “the capability as a global player, in cooperation with international partners, based on own insights and choices – to secure public interests in the digital domain and to be digitally resilient in an interconnected world” (Okano-Heijmans, 2023). Sovereignty is a complex politico-legal concept currently undergoing transformation due to shifting power dynamics between states and between state and non-state actors (Broeders et al., 2023). For example, emerging powers like China and Russia demand “state sovereignty” over their “national info-sphere,” contrasting with the U.S. ostensible support for unlimited internet freedom globally (Gu, 2023). Non-state commercial actors, in particular so-called Big Tech, represent another emerging set of political actors that enjoy a degree of sovereignty due to their economic clout but they are also the target of regulatory action to secure state sovereignty. These

commercial entities, the most dominant of which have captured the market lead are based in the US, claim self-sovereignty or freedom from sovereignty through a number of transnational legal strategies but heavily interfere with cross-border national authority and state-to-state relations, prompting strong regulatory demands from the EU and countries in the Global South. Additionally, the interchangeable use of terms like data sovereignty, digital sovereignty, and technological sovereignty complicates the issue further.

Sovereignty in the digital context encompasses three groups of “layers” through which sovereignty is enacted (as detailed in Table 1 in Appendix 2). The first is the “Physical Layer”, which involves sovereignty over physical infrastructure such as computers, servers, mobile devices, optical fibers, and other network equipment. The second is the “Logical Layer”, which involves sovereignty over computer codes, especially the communication protocol software responsible for network interconnection and transmission, governed by organizations like ICANN and ISOC (Gu, 2023). The third and most controversial is the Social Layer, which involves sovereignty over the control, processing, and circulation of massive amounts of data on platforms and AI models (Gu, 2023). This layer is contentious due to the lack of a widely accepted governance model globally between states and between state and non-state actors (Gu, 2023). With continuously growing power in data mining, computing, and modeling (algorithms and AI), reinforced by financial capital, Big Tech as the new oligarchs co-govern states alongside legitimate political powers without formal institutional authority, threatening the sovereignty of national states (Khanal et al., 2024). Obviously, Big Tech is not the only player with such power; any technological companies or capital, private or state-held, that have resources or power that crosses the boundaries of state territorial and jurisdictional sovereignty will pose risks, as case studies will below indicate.

The EU uses an analytical framework called the “National Digital Technology Stack (NDTS),” derived from the Open Systems Interconnection (OSI) model, to analyze weaknesses and dependencies. This framework features a layered structure of technological and non-technological components, including natural resources, critical infrastructures, data availability and usage, standardization and interoperability, digital skills, and cybersecurity. The NDTS is divided into three categories: (1) digital society and culture; (2) digital technologies and the economy (covering layers four to ten); and (3) the planet (represented by the bottom layer). Due to limited space, this report will not cover all the shortcomings faced by states in the Global South. Instead, it will focus on four of the “layers” consisting of the digital technologies categories – Application, Data, Intelligence, and Resources – applied and analyzed through multiple case studies.

For a state in the Global South, projecting its sovereignty involves governing with strategic autonomy over authority, territorial assets (including natural resources and digital resources like data), and institutionalized systems of the economy, politics, and socio-cultural life internally, as well as defending sovereignty and managing international relationships externally. However, due to historical institutional inequalities, their sovereignty will be impaired and will face greater challenges in the geopolitical digital era. Global South nations heavily rely on importing technologies while exporting raw planetary resources such as rare minerals to high-income countries. Consequently, they also lose control over essential materials (such natural resources) and immaterial assets like data about population, health, and nature, exacerbating and compounding the geopolitical digital divide (UN, 2023). Moreover, these dependencies are exploited in the interests of technology owners, whether private or state entities. More seriously, heads of state or parties may use these while backsliding towards authoritarianism to maintain power, dramatically harming and violating citizen and democratic sovereignty.

Data Colonialism and Digital Sovereignty

Global competitiveness between liberal democratic orders of all shades and authoritarian regimes understate the colonial nature of the current digital economy as represented by, for example, Meta’s Free Basics Initiative in the Global South and overstate the risky nature of current digital infrastructures represented by, for example, the “Made in China 2025” initiative and the “Belt and Road Initiative” (BRI) .

Mark Zuckerberg, the CEO of Meta the parent company of Facebook, Instagram and WhatsApp, stated that he views internet connectivity as a basic human right. This belief ostensibly motivated him to provide free internet access to millions of people in Africa through the Free Basics initiative. Instead of spending money on telecommunication towers, Facebook used a solar-powered drone and satellite network to provide internet service and partnered with local telecom companies using a freemium model as a marketing approach. Initially, the initiative was very successful, with over half of African countries joining the program, as well as Asian countries like India and the Philippines. However, access was limited to Facebook and a few other websites sponsored by business partners. Across Africa, Facebook is the internet. Criticism arose, accusing Facebook of neo-colonialism by concentrating its monopoly power and subjecting users to censorship and surveillance. Critics argue that Facebook exploited the dependency of poorer countries, making their populations consume primarily Western corporate content. In India, around 2016, the initiative was suspended because it violated net neutrality rules, a principle that all content and applications should be equally accessible by internet service providers.

We can also look the supply chains of what are called “soft infrastructures” that create new market for software dependency. South Africa’s dependency on U.S. Big Tech for software and digital services highlights significant supply chain vulnerabilities. This dependency affects data sovereignty, economic stability, and technological development in the country. In August 2023, the current “Big Five”—Apple, Google, Meta, Amazon, and Nvidia—were the most valued transnational tech companies, with a combined market value surpassing the GDP of any single nation except the U.S. and China (Wallach, 2021). This hegemonic power enables digital neo-colonization, as Kwet criticized, through control of software, hardware, and network connectivity for profit and plunder in the form of extracting rents and data globally (Kwet, 2019, 2022). The Global South, especially Africa, is hit hardest, as they must comply with WTO membership rules enforcing the TRIPS agreement, limiting their ability to negotiate protections for local industries (Kwet, 2019, 2022). Dominant tech companies undermine local businesses: Google and Facebook capture 82% of advertising revenue; Uber’s financial power has reduced driver pay by 25%; and Netflix and Apple Music have eroded the market share of MultiChoice, resulting in a loss of 115,000 subscribers in South Africa (Kwet, 2019, 2022). Governments have tried to adopt Free and Open-Source Software (FOSS) in the public sector to bypass superior proprietary software. However, this approach has failed as software has shifted towards cloud-based services. Although the Open-Source Community created the Affero GNU General Public License (AGPL) to encourage source code disclosure, it has not gained widespread acceptance. Meanwhile, Microsoft has partnered with local governments to provide free training on its platforms, further marginalizing domestic software developers (Kwet, 2019, 2022).

In contrast, China’s Digital Silk Road (DSR) is widely criticized, primarily from Western elite and governmental perspectives, as economic and political colonialism. Despite its stance as an alternative path, respecting the autonomy of the Global South, it faces scrutiny for exporting authoritarianism through surveillance systems and governance models. These efforts are seen as entrenching authoritarian regimes and threatening human rights and democracy. Exporting the idea of Chinese digital governance has been another way of introducing authoritarianism, which is embedded in and bound up with informal norms like views on human rights, formal norms like the choice of currency and trade procedures, and formal institutions in the form of laws, policies, regulations, and standards (Heeks et al., 2024). More concretely, governance is conducted through (1) the control of the physical foundation of digital infrastructure—internet/cyber governance, (2) the control of data flows—data governance, and (3) the control of services and applications—surveillance governance. Unlike the earlier dominant Western position, the Chinese digital governance model prioritizes state sovereignty over *laissez-faire*, solely international regulation, or a regime of multi-stakeholder institutions. It advocates for sovereign national control rather than giving voice to civil society, which represents a form of individual sovereignty (Heeks et al., 2024). China uses itself as an appealing role model of digital sovereignty with digitally enabled growth to promote its version of digital

governance in the Global South and encourages and advises these nations to develop their own local laws and policies. Meanwhile, using its increasing influence, China strives to be a standard-setter rather than a follower by contributing to the development of standards and promoting them in global bodies such as the International Telecommunication Union (ITU) regarding 5G, AI, IoT, and blockchain. When pushed back by the U.S., China, allying with the Global South, has been creating its regional standards rather than global versions through the BRI Connectivity and Standards Action Plan in 2019.

We must also look to ways in which these imitative involve Knowledge Supply and Technology transfer to the global south. Algeria and Egypt serve as strategic hubs for the Digital Silk Road (DSR). They are middle-income countries with a growing young population, high internet penetration rates, and proximity to the EU market (Hinane El-Kadi, 2024). This case study examines the implications of technology transfer and knowledge supply on local supply chain development. Researcher El-Kadi used a conceptual framework combining Technology Transfer and Techno-politics perspectives to scrutinize Huawei's Technology Transfer outcomes in these markets through interviews with 71 participants, including employees, subcontractors, customers, policymakers, university researchers, and government officials. The technology transfer occurs both horizontally and vertically. Horizontally, technology and know-how are transferred through labor mobilization, such as local hiring and skill training. Huawei and ZTE hired 70% local workers, but most are not in managerial positions, creating a glass ceiling for local employees. The horizontal linkage is limited as turnover mostly happens between foreign OEMs rather than between transnational firms and local firms. The limited effectiveness of technology transfer impacts the local supply chain by perpetuating dependency on imported components and technology. Local suppliers struggle to move up the value chain due to insufficient training and lack of integration into the broader technological ecosystem. This situation hinders the development of a robust and self-sustaining local supply chain.

In the Indonesian case, China has been largest trade partner for over ten years, with trade increasing from US\$50 billion in 2014 to US\$124.34 billion in 2021, driven by the Digital Roadmap Strategy (DRS) (Wu, 2024). This case study examines the implications of this trade relationship on Indonesia's supply chain vulnerabilities. Direct investment projects under the DRS include high-speed railways, data centers, 5G telecom infrastructure, e-commerce, and social media. Approximately 1,000 Chinese enterprises have invested in Indonesia, making China the top Foreign Direct Investment (FDI) source for Indonesia. However, increased bilateral trade makes Indonesia vulnerable to potential supply chain disruptions (Wester, 2023). Imports from China more than doubled to \$16 billion by 2022, driven by construction and manufacturing needs. This dependence gives China significant leverage over supply and pricing of key inputs. But what is the impact: In addition to conventional trade, China's top e-commerce players have entered local markets: Lazada, supported by Alibaba; Shopee, backed by Tencent; and JD.id, a joint venture between JD China and Provident Capital Singapore (IDEAS, 2022). These efforts have facilitated the adoption of Chinese cashless payment systems, such as WeChat Pay and Alipay, in Indonesia. While the DSR has positively impacted Indonesia's economy, critics argue that the quality of democracy has declined, associated with Huawei programs and the ASEAN Academy Engineering Institute in Jakarta (IDEAS, 2022). The reliance on China's economy raises concerns about the fairness between Chinese sellers and local businesses, with 90% of products sold in the Indonesian marketplace being "Made in China" (IDEAS, 2022).

For historical context and a contrastive example of Western intervention, we look to the ZunZuneo (2009–2012) project for clear geopolitical balance acting between access to digital services and data sovereignty. While Operation Earnest Voice and the Trans-Regional Web Initiative, discussed in the previous section, were both coordinated by sectors of the U.S. military and served to further U.S. military objectives abroad, ZunZuneo evidences the broader application of disinformation campaigns in U.S. foreign policy and international relations as well.

ZunZuneo was a SMS-based social network developed by the U.S. and implemented in Cuba between 2009 and 2012. The goal of the network was to spark enough dissent in Cuba to reach a tipping point where

dissidents would organize mobs, hold political demonstrations, or otherwise “renegotiate the balance of power between the state and society” (Butler et al., 2014). ZunZuneo differs from Operation Earnest Voice in that it was developed by the U.S. Agency for International Development (USAID) and was considered part of U.S. foreign policy—under the “Internet freedom agenda”—rather than a tool for strategic military objectives (Butler et al., 2014). It was funded and coordinated by USAID’s Office of Transition Initiatives (OTI), a division created after the fall of the Soviet Union to promote U.S. interests “without the usual red tape” (Meyer, 2014). USAID contracted two companies, Creative Associates International and Mobile Accord, to build the network. The company offered an SMS service to Cubans, whose typical texts were unencrypted and tracked by the government. The service would route texts from the sender through one of the company’s servers in Spain (run by Lleida.net) or Ireland before reaching the recipient, effectively operating as a VPN for text messages (*The Guardian*, 2014). While the contents and metadata associated with the texts were hidden from the Cuban government, the U.S. collected data on users “in the hope that the information might be used someday for political purposes” (Butler et al., 2014). However, the U.S. stored and analyzed the text messages to create demographic profiles of Cubans that includes their gender, age, “receptiveness,” and “political tendencies” (Butler et al., 2014).

ZunZuneo grew its user base by offering free or discounted message rates and spreading “non-controversial content” such as news, sports, music, and weather updates (*The Guardian*, 2014). The influence and data collection operation soft-launched on September 20, 2009 during Colombian artist Juanes’ concert, “Peace Without Borders,” in Havana where the U.S. reached over 100k Cubans (*The Guardian*, 2014). The U.S. hired Alen Lauzan Falcon to post content ranging from “mildly political and comical” to “more pointed” so they could further refine their user demographics and determine who to target with further political content (*The Guardian*, 2014). USAID divided the surveilled Cubans into different segments: at one end was the “democratic movement,” in the middle was “still (largely) irrelevant,” and at the opposite end were “hard-core system supporters,” which the USAID nicknamed “Talibanes” in a “derogatory comparison to Afghan and Pakistani extremists” (*The Guardian*, 2014). The U.S. went through great lengths to distance itself from ZunZuneo.

At its peak, ZunZuneo had over 40,000 users and was referred to as “the fairy godmother of cellphones” by Cubans, though nobody knew of the U.S. government’s affiliation with the company (*The Guardian*, 2014). ZunZuneo began facing financial problems in 2011 because it was not profitable for companies to run ads on the network, which meant it still required U.S. funding. USAID abandoned its hopes of reaching 200,000 users and capped the number at 40,000, and decreased traffic to just 1% of Cuba’s total text messages (*The Guardian*, 2014; Meyer, 2014). Mobile Accord then began interviewing candidates for ZunZuneo’s CEO to make the company financially independent and sustainable, though they did not inform candidates that it was a U.S. government operation (Meyer, 2014). Suzanne Hall, a U.S. State Department official, even asked Twitter CEO Jack Dorsey to run the company (*The Guardian*, 2014). Ultimately, ZunZuneo’s financial troubles led to service outages and the company shut down in 2012. USAID never reached the critical mass they had hoped. Instead, their bulk text messaging deal with state-run company Cubacel funded the Cuban government (Meyer, 2014).

Domestic Platform Regulation

Another way to approach digital sovereignty is to look at the internal strategies for regulation of domestic tech actors. To do so we look to the cases of two search giants: Yandex in Russia and Google owned by parent company Alphabet in the U.S. In the regulation of Russia’s Yandex, ownership played a large role in a way that was not true of the regulation of Google. It was fears over foreign ownership of a critical asset like Yandex that prompted the government into action: to procure a golden share in 2009, attempting to pass legislation limiting foreign ownership to 20% in 2016 and 2018, and the creation of the public interest foundation in 2019. Foreign ownership of platforms is not as big of a concern in the United States, at least in

part due to the fact that most large platforms in the US are American and foreign capital. An obvious exception would be TikTok: the US passed a law in 2024 forcing TikTok to sell its US operation despite the on-going political debate, adjudication and likely appeals, specifically citing the threat of foreign ownership of the app. The concentrated capital and global corporate wealth invested in the United States, including domestic funds investment in TikTok's parent company ByteDance, may be a reason why the government has been less concerned about foreign ownership of tech platforms; while Russia exposure to global sanctions as a form of foreign interference leads to the government toward greater domestic ownership citing the threat of foreign ownership.

The United States' regulation of Google did not touch on content moderation in the same way as Russia's regulation of Yandex because this issue has been relatively static in the US via Section 230 — an amendment to the short-lived anti-online pornography Communications Decency Act of 1996 (Gillespie, 2018). Whereas most of the act did not survive a Supreme Court challenge, Section 230 did, thus continuing to provide 'safe harbor' to internet intermediaries, such as internet service providers and platforms. In short, Section 230 treats intermediaries like telephone companies, protecting them from liability for the content their users' speech — with the exception of "cases involving federal criminal law, intellectual property law, and electronic-communications privacy law" (Gillespie, 2018, p. 222). Though there has been a growing recognition that Section 230 may not be the perfect solution for today's social media platforms, disagreement between Democratic and Republican lawmakers "[has] led to policy stasis", at least in the legislative branch at the federal level (Gorwa, 2024, p. 126). State governments have thus began to 'contest' platform governance regarding content moderation — with Republican-ran states, such as Texas and Florida, passing laws combatting alleged 'censorship' of conservative voices, while New York state has passed an anti 'hateful-conduct' bill.⁶ All three bills are tied up in lawsuits, demonstrating: a) the tech industry's ability to influence regulatory policy; b) the interplay between state governments and the federal government; and c) the interplay between the legislative branch and the judicial branch.

In Russia, on the other hand, the regulation of content moderation was an important goal. This goal can be seen in multiple instances: a) the creation of the 'white list' of news sources for the Yandex.News homepage, which was implemented in 2015; b) the 2016 law "On News Aggregators", which prompted Yandex to drop non-Roskomnadzor-registered outlets from news segments at Yandex.News; and c) post-invasion laws in 2022 that called for jail sentences for 'fake information' about the Russian army.

A point of commonality between the two governments is that both began to 'contest' private platform governance after years of trying to 'convince' or 'collaborate'. In the United States, the government began to contest because of a change in 'political will', as opinion of technology companies has worsened at both the elite and public level. The change of opinion at the elite level has led to the appointment of tech-critical bureaucrats that hold decision-making power, such as Lina Khan in the FTC. In Russia, the move from 'convince' to 'contest' may be attributed to two factors: a) a change in 'political will' linked to the recognition of Yandex and other platforms as strategically important, similar to traditional media; and b) a change in 'power to intervene' via pro-kremlin ownership ties and new laws, both of which accompanied Putin's consolidation of power following his return to the presidency in 2012.

Google and Yandex's ability to shape or hinder policy has been curtailed as the US and Russia have taken firmer, legally-binding stances. In the US, Google's influence was at its apex during the Obama administration. Official lobbying, unofficial influence campaigns, and the revolving door between Google and the federal government contributed to the FTC deciding not to pursue Google over antitrust violations. This has changed, and Google has lost one DOJ antitrust lawsuit and faces a number of other lawsuits from both state governments and the federal government. Yandex was able to resist attempts to 'convince' the company to provide a more 'pro-Russia' media environment under the Medvedev administration. Even in the 2010s

⁶ For an overview of the regulatory environment in the US vis-à-vis platforms, see Gorwa, 2024, chapter 7.

Yandex and other tech companies were able to influence some aspects of bills before they became laws. Yandex lost all ability to resist or influence Russian law after Russia’s invasion, culminating in its break up amid relative state capture with the most valuable Ai and FinTech departments relocated through sale to the Netherlands.

Conclusion – Best Practices for Responsible Digital Resilience

Best practices for media literacy, inclusive communicative engagement, and responsible public discourse represent the most immediate field through which policy makers must respond to the strategic spoiling of the global information order. Media literacy interventions do work – they create a digital resilience that reduces belief in falsehoods and decreases chances of the sharing of misinformation (Huang, Jia and Yu 2024). When the disinformation scholarship ponders on solutions to the “disinformation problem”, scholars tend to propose two primary solutions. From the top-down, scholars often suggest refining and applying antitrust regulation to break up big tech monopolies and media market regulation. From the bottom-up, the primary solution is digital literacy yet these are often defined in the neoliberal terms of employment and labour – rather than literacy in terms of assessing information integrity, sourcing, and validity. The argument is that due to the pervasiveness of digital technologies, traditional literacy skills (e.g., reading and mathematics) are insufficient today to exercise full citizenship because the web has become the primary means by which citizens can access information, communicate, and participate in the system, as well as perform in their work, and manage their social lives. As such, states need to empower citizens by facilitating the provision of the suite of skills necessary to navigate this new information environment. Digital literacy skills include hard skills, such as programming, but also soft skills, such as an understanding of information verification, privacy, ethics, and safety. States have adopted digital literacy with varying degrees of success. On average, European countries tend to perform better in the digital literacy space. The Finnish and Estonian governments particularly have systematically integrated digital literacy in educational curricula and provide funding to organizations which provide digital literacy training to traditionally marginalized groups such as the elderly and newcomers. There remain some practical challenges to the implementation of digital literacy initiatives.

Government initiatives	Civil society initiatives	Journalist/news media initiatives	Academic initiatives
<ol style="list-style-type: none"> 1. Overseeing the implementation of regulations and laws promoting transparency, accountability, and ethical standards in media. 2. Supporting/funding independent journalism and fact-checking initiatives. 3. Promotion of media literacy through the integration education/school curriculum and public awareness campaigns. 	<ol style="list-style-type: none"> 1. Fact-checking organizations aimed at promoting government transparency. 2. Promote community engagement, i.e. Workshops, seminars, grass-roots initiatives. 3. Create and promote digital literacy programs. 4. Collaborate with technology companies to help identify and address disinformation. 	<ol style="list-style-type: none"> 1. Utilization of OSINT, explainer journalism, citizen journalism, etc. to report on breaking news. 2. Collaboration with NGOs and fact-checking operations. 3. Promote dialogue surrounding controversial issues to reduce the influence of disinformation 	<ol style="list-style-type: none"> 1. Conduct research and analysis on emerging disinformation trends. 2. Consult policymakers and advise government agencies on a range of related topics including AI, social media regulations, cybersecurity, ethical standards, etc. 3. Assist in media literacy curriculum building and develop educational programs that promote the critical thinking needed to evaluate the credibility of information.

Figure 1: Comprehensive interventions by domain.

The first challenge is that neoliberal economies do not have incentives to invest resources into developing and implementing digital literacy, but they do have incentives to continue investing in digital technologies. Moreover, the digital literacy skills in neoliberal systems tend to prioritize digital media production skills (i.e., the creation of “marketable skills”) (Notley & Dezuanni, 2019) over critical digital literacy skills, i.e., the type of digital literacy needed to become informed as a democratic citizen. The second challenge is the actual implementation of digital literacy; in multi-level systems of government like Canada and the U.S., with educational mandates at the sub-national level, multiple school boards and states/provinces/territories have jurisdiction over curricula, so a top-down, centralized strategy (such as the one implemented in Estonia) is difficult. The third challenge is that in some democracies, such as in Denmark and Switzerland (‘Thèmes’, 2021), the push for digital literacy integration in schools has been met with push-back from parents, teachers, and citizen groups which call for the outright banning of technology in the classroom. Driven by concerns surrounding screen time and digital addictions, these groups are arguing that screens should be banned in schools. The fourth challenge is that the constantly changing technologies make it difficult to implement digital literacy initiatives due to the need to update the curricula. However, some organisation such as the Future Classrooms Lab in Denmark (*Vejledning Til Tek Tjek*, 2023), argue that the framework for digital literacy remains the same and that through play, curiosity, and use, we can learn to question any technology critically by asking questions about its development, intended use, and how it makes us feel.

Finland has been proactive in addressing disinformation and serves as an appropriate case-study for the ways in which governments initiatives, education, and media strategies can work cohesively to build societal resilience. The Finnish approach to disinformation is largely based on cross-departmental engagement and a bottom-up approach that begins with the country’s education system (Miloš & Mlejnková, 2021). Much of Finland’s success in countering disinformation is attributed to a combination of high press freedom and innovative media literacy policies that include educational and e-participation activities (Horowitz et al., 2022). Finland is commonly referred to as a “media welfare state,” which is characterized by the notion of universal access to content and services ensured by strong public service media as well as institutionalized editorial freedom (Horowitz et al., 2022). The Finnish Broadcasting Company (Yle) has devoted coverage foreign interference, primarily around Russian disinformation campaigns in Finland, and have several documentaries and current affairs series covering information disorder (Horowitz et al., 2022). Finland has maintained a relatively ‘neutral media space’ that is free from heavily partisan political reporting which has resulted in a positive and generally more trusting relationship between the Finnish population and traditional news sources (Bjalo & Papadakis, 2021). Finland’s Council for Mass Media also surveys journalistic practices and examines emerging “fake news” trends in recent years (Bjalo & Papadakis, 2021).

The Finnish government considers its public education system as one of the most critical tools in building resistance to information warfare (Charlton, 2019). Finland’s public education system focuses heavily on digital and media literacy, providing educational content for its young population as part of its revised 2016 curriculum which seeks to prioritize the skills students need to navigate an increasingly complex digital landscape (Mackintosh, 2019). Educational initiatives include discussions of false news, internet security, journalism ethics and regulations, and accessible online classes for detecting false or biased information online (Horowitz et al., 2022). The Finnish Ministry of Education and Culture collaborates with the National Audiovisual Institute (KAVI) to strengthen children’s media skills and Finnish fact-checking organizations such as Faktabaari (FactBar) “adapts professional fact-checking methods for use in Finnish schools” (Charlton, 2019). Meanwhile, government agencies like KAVI work with hundreds of NGOs and news media organizations to extend media literacy beyond grade school (Lau, 2023). NGOs such as Helsinki-based SeniorSurf target specific demographics such as senior citizens and new immigrants by providing one-on-one digital literacy training (Lau, 2023). Though Finland still faces challenges surrounding societal polarization, radicalization fueled by far-right online communities, and persistent Russian disinformation

narratives, as a whole, Finnish society is far less vulnerable to these threats. The strong cohesion between the Finnish government, civil society initiatives, news media, and the education sector promote the kind of media literacy and public awareness necessary to minimize the impacts of disinformation.

The decentralized nature of the Internet offers users an equal opportunity to generate and disseminate content, allowing anyone to ‘push’ information into the virtual sphere as well as ‘pull’ information from a diverse and ever-expanding bank of sources (Heinrich, 2011). The push and pull of information online creates a unique dynamic where Internet users provide the supply of information while simultaneously serving as the demand for information. The supply-and-demand dynamic for information inherently applies to disinformation as well. Various actors serve as the supply for disinformation in the virtual sphere including actors intentionally disseminating false narratives as well as actors who unknowingly amplify disinformation simply by reposting or sharing information online. Meanwhile, due to the ubiquitous nature of disinformation, anyone seeking to consume information online implicitly serves as the demand for disinformation.

Freedom of press and independent journalism is necessary for the creation of strong civil societies that are resilient to disinformation and the challenges posed by an increasingly saturated information sphere. However, journalists cannot counter disinformation alone. Many government responses over the past decade have been aimed at tackling the ‘supply-side’ of disinformation, such as efforts to strengthen detection analysis, coordinated response to threats, and collaboration with online platforms to tackle, and regulate the sources of disinformation (Runcheva Tasev & Apostolovska-Stepanoska, 2019). Although these efforts may be effective temporarily, addressing disinformation from the supply side presents long-term challenges. This approach assumes a ‘cat-and-mouse’ dynamic that is ultimately ill-suited to the pervasive nature of disinformation. In order to build long-term societal resilience to disinformation, there must be a cohesive effort to confront the social structure of everyday information seeking – the demand-side of disinformation – which understanding the where and how to engage identarian and experiential experiences of media consumers, news-avoiders and information seekers – necessitating a whole society engagement through cooperation amongst government bodies, civil society organizations, journalists, and academics alike.

References

- Access Now*. (n.d.). *Access Now*. Retrieved 3 September 2024, from <https://www.accessnow.org/>
- «Яблоко» дополнило список репрессивных законов, нарушающих права и свободы граждан. (2021, September 16). *Партия Яблоко*. [https://www.yabloko.ru/cat-news/2021/09/«Яблоко» дополнило список репрессивных законов, нарушающих права и свободы граждан](https://www.yabloko.ru/cat-news/2021/09/«Яблоко»_дополнило_список_репрессивных_законов,_нарушающих_права_и_свободы_граждан)
- Aboubakr, F. (2017). Peasantry in Palestinian Folktales: Sites of Memory, Homeland, and Collectivity. *Marvels & Tales*, 31(2), 217–238. <https://doi.org/10.13110/marvelstaes.31.2.0217>
- Abu-Irmies, A., & Al-Khanji, R. R. (2019). The Role of Social Media in Maintaining Minority Languages: A Case Study of Chechen Language in Jordan. *International Journal of Linguistics*, 11(1), 62–75.
- Access Now*. (n.d.). *Access Now*. Retrieved 3 September 2024, from <https://www.accessnow.org/>
- Adala. (2011). "Nakba Law" - Amendment No. 40 to the Budgets Foundations Law. Retrieved from Adala: <https://www.adalah.org/en/law/view/496>

- AI and Covert Influence Operations: Latest Trends*. (2024). OpenAI.
https://downloads.ctfassets.net/kftzwdyauwt9/5IMxzTmUclSOAcWUXbkVrK/3cfab518e6b10789ab8843bcc18b633/Threat_Intel_Report.pdf
- Aitamurto, T. (2015). Motivation Factors in Crowdsourced Journalism: Social Impact, Social Change, and Peer Learning. *International Journal of Communication*, 9, 3523–3543.
- Alek Minassian: Toronto van attack suspect praised ‘incel’ killer. (2018, April 24). *BBC News*.
<https://www.bbc.com/news/world-us-canada-43883052>
- Alek Minassian: Toronto van attack suspect praised ‘incel’ killer. (2018, April 24). *BBC News*.
<https://www.bbc.com/news/world-us-canada-43883052>
- Alina Danilina. (2023, June 4). Come to your senses! The 15 most repressive laws adopted in Russia this year. And it seems that in 2023, the Duma is not planning to stop—Novaya Gazeta Europe. Novaya Gazeta. Europe. <https://novayagazeta.eu/articles/2023/01/04/come-to-your-senses>
- Allsop, J. (2023, October 21). *The insidious spread of ‘foreign agent’ laws*. Retrieved from Columbia Journalism Review:
https://www.cjr.org/the_media_today/alsu_kurmasheva_arrest_foreign_agent_laws.php
- Amazeen, M. A. (2020). Journalistic interventions: The structural factors affecting the global emergence of fact-checking. *Journalism*, 21(1), 95–111. <https://doi.org/10.1177/1464884917730217>
- Anderson, M. (2024, Aril). Americans’ Views of Technology Companies. *Pew Research Center*.
<https://www.pewresearch.org/internet/2024/04/29/americans-views-of-technology-companies-2/>
- Andrejevic, M. (2013). *Infoglut: how too much information is changing the way we think and know*. New York: Routledge.
- Arafat, R. (2024). Reporting on the Syrian conflict from exile: Examining advocacy strategies in diaspora journalists’ online news. In *Middle Eastern Diasporas and Political Communication* (1st ed., pp. 161–181). Routledge. <https://www-taylorfrancis-com.manchester.idm.oclc.org/books/edit/10.4324/9781003365419/middle-eastern-diasporas-political-communication-ehab-galal-mostafa-shehata-claus-valling-pedersen>
- Armstrong, J. A. (1976). Mobilized and Proletarian Diasporas. *American Political Science Review*, 70(2), 393–408. <https://doi.org/10.2307/1959646>
- Arthur, C. (2012, October 8). China’s Huawei and ZTE pose national security threat, says US committee. *The Guardian*. <https://www.theguardian.com/technology/2012/oct/08/china-huawei-zte-security-threat>
- AS News Bureau—Repost*. (n.d.). Retrieved 13 August 2024, from <https://wearerepost.com/foundation>
- Ashley Ford, C., & Henderson Auditorium, L. (2019). *Huawei and Its Siblings, the Chinese Tech Giants: National Security and Foreign Policy Implications*. <https://2017-2021.state.gov/huawei-and-its-siblings-the-chinese-tech-giants-national-security-and-foreign-policy-implications/>
- Aydingün, A., & Yıldırım. (2010). Perception of homeland among Crimean Tatars: Cases from Kazakhstan, Uzbekistan and Crimea. *Bilig*, 54, 21–46.
- Aydingün, I., & Aydingün, A. (2007). Crimean Tatars return home: Identity and cultural revival. *Journal of Ethnic and Migration Studies*, 33(1), 113–128.
- Baas, M. (2017). Indians in Australia. In R. S. Hegde & A. K. Sahoo (Eds.), *Routledge Handbook of the Indian Diaspora* (1st ed., pp. 317–329). Routledge. <https://doi.org/10.4324/9781315672571-25>
- Badran, Y. (2020). Strategies and (survival) tactics: The case of Syrian oppositional media in Turkey. *Journal of Alternative & Community Media*, 5(1), 69–85. https://doi.org/10.1386/joacm_00075_1

- Banat, B. Y. I., Entrena-Durán, F., & Dayyeh, J. (2018). Palestinian refugee youth: Reproduction of collective memory of the Nakba. *Asian Social Science*, 14(12), 147–155. <https://doi.org/10.5539/ass.v14n12p147>
- Barabantseva, E. (2010). Transnationalising Chineseness ‘Overseas Chinese work’ in the reform period. In *Overseas Chinese, ethnic minorities and nationalism: De-centering China* (pp. 108-). Routledge. <https://www.taylorfrancis.com/books/mono/10.4324/9780203845462/overseas-chinese-ethnic-minorities-nationalism-elena-barabantseva>
- Barker, J. (2021). *Red Scare: The State’s Indigenous Terrorist*. University of California Press.
- Barrett, P. M. (2020). *Who Moderates the Social Media Giants? A Call to End Outsourcing*. NYU Stern Center for Business and Human Rights. https://issuu.com/nyusterncenterforbusinessandhumanri/docs/nyu_content_moderation_report_final_version?fr=sZWZmZjI1NjI1Ng
- basedcrackaddict. (2024, July 24). Elliot Rodger would have been 33 today. *Involuntary Celibate Forum*. <https://incels.is/threads/elliott-rodger-would-have-been-33-today.633949/>
- Batta, A. (2021). *The Russian Minorities in the Former Soviet Republics: Secession, Integration, and Homeland* (1st ed.). Routledge. <https://doi.org/10.4324/9781003205340>
- BBC. (2014, April 22). Russian social network founder says he has been fired. *BBC*. <https://www.bbc.com/news/technology-27113292>
- Belovodyev, D., Soshnikov, A., Standish, R., & Systema. (2023, April 5). Leaked Files Show China And Russia Sharing Tactics On Internet Control, Censorship. *Radio Free Europe / Radio Liberty*. <https://www.rferl.org/a/russia-china-internet-censorship-collaboration/32350263.html>
- Ben-David, A. (2012). The Palestinian diaspora on the Web: Between de-territorialization and re-territorialization. , 51(4), 459-474. <https://doi.org/10.1177/0539018412456769>. *Social Science Information*, 51(4), 459. <https://doi.org/10.1177/0539018412456769>
- Benjamin, R. (2019). *Race After Technology: Abolitionist Tools for the New Jim Code*. Polity Press.
- Benkler, Y., Faris, R., & Roberts, H. (2018). *Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics*. Oxford University Press.
- Benton, G., & Gomez, E. T. (2014). Belonging to the nation: Generational change, identity and the Chinese diaspora. *Ethnic and Racial Studies*, 37(7), 1157–1171. <https://doi.org/10.1080/01419870.2014.890236>
- Bernays, E. L. (2005). *Propaganda*. Ig Publishing.
- Bernstein, J. (2021, September). Bad News: Selling the story of disinformation. *Harper’s Magazine*, September 2021. <https://harpers.org/archive/2021/09/bad-news-selling-the-story-of-disinformation/>
- Bernstein, J. (2021, September). Bad News: Selling the story of disinformation. *Harper’s Magazine*, September 2021. <https://harpers.org/archive/2021/09/bad-news-selling-the-story-of-disinformation/>
- Berwick, A. (2018, November 14). Special Report: How ZTE helps Venezuela create China-style social control. *Reuters*. <https://www.reuters.com/article/technology/special-report-how-zte-helps-venezuela-create-china-style-social-control-idUSKCN1NJ1ZV/>
- Bezverkha, A. (2015). *Representations of the Crimean Tatars in the Ukrainian Media Discourse [Doctoral Dissertation]*. National University of Kyiv-Mohyla Academy.
- Bhabha, H. K. (1994). *The location of culture*. Routledge.

- Bing, C., & Schectman, J. (2024, June 14). Pentagon ran secret anti-vax campaign to incite fear of China vaccines. *Reuters*. <https://www.reuters.com/investigates/special-report/usa-covid-propaganda/>
- Bjalo, C., & Papadakis, K. (2021). Digital Propaganda, Counterpublics, and the Disruption of the Public Sphere: The Finnish approach to building digital resilience. In *The World Information War* (1st ed., pp. 186–213). [https://www.taylorfrancis.com/myaccess.library.utoronto.ca/chapters/edit/10.4324/9781003046905-15/digital-propaganda-counterpublics-disruption-public-sphere-corneliu-bjola-krysianna-papadakis](https://www.taylorfrancis.com/myaccess/library.utoronto.ca/chapters/edit/10.4324/9781003046905-15/digital-propaganda-counterpublics-disruption-public-sphere-corneliu-bjola-krysianna-papadakis)
- Blachnicka-Ciacek, D. (2016). Remembering Palestine: A multi-media ethnography of generational memories among diaspora Palestinians [Doctoral, Goldsmiths, University of London]. https://research.gold.ac.uk/id/eprint/18751/1/SOC_redactedthesis_Blachnicka-CiacekD_2016.pdf
- Blank, S. (2008). Web War I: Is Europe's First Information War a New Kind of War? *Comparative Strategy*, 27(3), 227–247. <https://doi.org/10.1080/01495930802185312>
- Bloomberg News. (2024, July 15). Yandex Founder Volozh to Return as CEO After Sanctions Dropped. *Bloomberg News*. <https://finance.yahoo.com/news/yandex-founder-volozh-return-ceo-090846947.html>
- Bond, S. (2024, June 6). This is what Russian propaganda looks like in 2024. *NPR*. <https://www.npr.org/2024/06/06/g-s1-2965/russia-propaganda-deepfakes-sham-websites-social-media-ukraine>
- Bonnell, A.-L. (Director). (2016). *Donbass—2016* [YouTube Video]. https://www.youtube.com/watch?v=b8j0tJsKltg&ab_channel=77MegaMix
- Bott, M., Gigler, B.-S., & Young, G. (2014). The Role of Crowdsourcing for Better Governance in Fragile State Contexts. In *Closing the Feedback Loop: Can Technology Bridge the Accountability Gap* (pp. 107–148). World Bank Publications.
- Botto, M., & Gottzén, L. (2024). Swallowing and spitting out the red pill: Young men, vulnerability, and radicalization pathways in the manosphere. *Journal of Gender Studies*, 33(5), 596–608. <https://doi.org/10.1080/09589236.2023.2260318>
- boyd, dannah. (2018, March 7). *SXSW EDU Keynote | What Hath We Wrought?* <https://www.youtube.com/watch?v=0I7FVyQCjNg>
- Bradshaw, S., & Howard, P. N. (2017). *Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation*.
- Bradshaw, S., & Howard, P. N. (2018). The Global Organization of Social Media Disinformation Campaigns. *Journal of International Affairs*, 71(1.5), 23–32.
- Bradshaw, S., Bailey, H., & Howard, P. N. (2021). *Industrialized Disinformation: 2020 Global Inventory of Organized Social Media Manipulation*. Oxford University: Programme on Democracy & Technology. <https://demtech.oii.ox.ac.uk/research/posts/industrialized-disinformation/>
- Braga, A. E. P., Pinto, A. L., Muriel-Torrado, E., & Dutra, M. L. (2024). Censorship: A Reaction to Disinformation on the World Wide Web. *Investigación Bibliotecológica: Archivonomía, Bibliotecología e Información*, 38(98), 187–206. <https://doi.org/10.22201/iibi.24488321xe.2024.98.58855>
- Brown, A. (2020, November 15). In the Mercenaries' Own Words: Documents Detail TigerSwan Infiltration of Standing Rock. *The Intercept*. <https://theintercept.com/2020/11/15/standing-rock-tigerswan-infiltrator-documents/>
- Brown, A., & Sadasivam, N. (2023a, April 13). After Spying on Standing Rock, TigerSwan Shopped Anti-Protest “Counterinsurgency” to Other Oil Companies. *The Intercept*. <https://theintercept.com/2023/04/13/standing-rock-tigerswan-protests/>

- Brown, A., & Sadasivam, N. (2023b, May 22). Pipeline Company Spent Big on Police Gear to Use Against Standing Rock Protesters. *The Intercept*. <https://theintercept.com/2023/05/22/standing-rock-energy-transfer-tigerswan/>
- Brown, A., Parrish, W., & Speri, A. (2017a, May 27). Leaked Documents Reveal Counterterrorism Tactics Used at Standing Rock to “Defeat Pipeline Insurgencies.” *The Intercept*. <https://theintercept.com/2017/05/27/leaked-documents-reveal-security-firms-counterterrorism-tactics-at-standing-rock-to-defeat-pipeline-insurgencies/>
- Brown, A., Parrish, W., & Speri, A. (2017b, June 3). Standing Rock Documents Expose Inner Workings of “Surveillance-Industrial Complex.” *The Intercept*. <https://theintercept.com/2017/06/03/standing-rock-documents-expose-inner-workings-of-surveillance-industrial-complex/>
- Brubaker, R. (2005). The ‘diaspora’ diaspora. *Ethnic and Racial Studies*, 28(1), 1–19. <https://doi.org/10.1080/0141987042000289997>
- Budak, C., Nyhan, B., Rothschild, D. M., Thorson, E., & Watts, D. J. (2024). Misunderstanding the harms of online misinformation. *Nature*, 630(8015), 45–53. <https://doi.org/10.1038/s41586-024-07417-w>
- Burchell, K. (2020). Reporting, uncertainty, and the orchestrated fog of war: A practice-based lens for understanding global media events. *International Journal of Communication*, 14(2020), 2905-2927.
- Burchell, K. (2024). *Constant Disconnection: The Weight of Everyday Digital Life*. Redwood, CA: Stanford University Press.
- Burchell, K. and Fielding, S. (2024) “What hits me the hardest...the Photojournalist Blog: Genres and Practices of Journalistic Witnessing.” In M. Lithgow and M. Martin eds. *Eyewitness Textures: User Generated Content and News Coverage in the 21st Century*. McGill-Queens University Press.
- Butler, D., Gillum, J., & Arce, A. (2014, April 3). US secretly built ‘Cuban Twitter’ to stir unrest. *The Associated Press*. <https://apnews.com/article/technology-cuba-united-states-government-904a9a6a1bcd46cebfc14bea2ee30fdf>
- Cadwalladr, C., & Graham-Harrison, E. (2018, March 17). Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. *The Guardian*. <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>
- Calma, J. (2023, May 31). Twitter just closed the book on academic research. *The Verge*. <https://www.theverge.com/2023/5/31/23739084/twitter-elon-musk-api-policy-chilling-academic-research>
- Carlson, E. D., & Williams, N. E. (2020). Comparative demography of the Syrian diaspora: European and Middle Eastern destinations. Springer.
- Carlson, M. (2018). The Information Politics of Journalism in a Post-Truth Age. *Journalism Studies*, 19(13), 1879–1888.
- Chakars, J., & Ekmanis, I. (Eds.). (2022). *Information Wars in the Baltic States: Russia’s Long Shadow*. Springer International Publishing. <https://doi.org/10.1007/978-3-030-99987-2>
- Charlton, E. (2019). *How Finland is fighting fake news—In the classroom*. World Economic Forum. <https://www.weforum.org/agenda/2019/05/how-finland-is-fighting-fake-news-in-the-classroom/>
- Chase, M. S., & Chan, A. (2016). *China’s Evolving Approach to “Integrated Strategic Deterrence”*. Rand Corporation.

- Choma, B. L., & Hanoch, Y. (2017). Cognitive ability and authoritarianism: Understanding support for Trump and Clinton. *Personality and Individual Differences*, 106(Complete), 287–291.
<https://doi.org/10.1016/j.paid.2016.10.054>
- Chouliaraki, L. (2024). *Wronged: The Weaponization of Victimhood*. New York: Columbia University Press.
- Christensen, C. P. (2021). The Long Umbilical Cord: The role of race in China’s diaspora engagement in Australia [Masters, University of Oslo].
<https://www.duo.uio.no/bitstream/handle/10852/88279/MASTER-THESIS----The-Long-Umbilical-Cord---The-role-of-race-in-China-s-diaspora-engagement-in-Australia----FINAL.pdf?sequence=1&isAllowed=y>
- Cicilline, D. (2022). *INVESTIGATION OF COMPETITION IN DIGITAL MARKETS*. SUBCOMMITTEE ON ANTITRUST, COMMERCIAL, AND ADMINISTRATIVE LAW OF THE COMMITTEE ON THE JUDICIARY OF THE HOUSE OF REPRESENTATIVES.
<https://www.govinfo.gov/content/pkg/CPRT-117HPRT47832/pdf/CPRT-117HPRT47832.pdf>
- Citron, D., & Chesney, R. (2019). Deepfakes and the New Disinformation War. *Foreign Affairs*.
https://scholarship.law.bu.edu/shorter_works/76
- Clark, M. (2020). *RUSSIAN HYBRID WARFARE*.
- Clifford, J. (1994). Diasporas. *Cultural Anthropology*, 9(3), 302–338.
<https://doi.org/10.1525/can.1994.9.3.02a00040>
- Cohen, J. E. (2020). *Between Truth and Power*. Oxford University Press.
<https://global.oup.com/academic/product/between-truth-and-power-9780190246693>
- Cohen, R. (1996). Diasporas and the nation-state: From victims to challengers. *International Affairs*, 72(3), 507–520. <https://doi.org/10.2307/2625554>
- Cohen, R. (2022). *Global diasporas: An introduction (25th anniversary edition)*. Routledge Taylor & Francis Group.
- Confessore, N. (2018, April 4). Cambridge Analytica and Facebook: The Scandal and the Fallout So Far. *The New York Times*. <https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html>
- Cottiero, C., & Emmons, C. (2024). *Understanding and Interrupting Authoritarian Collaboration | IFES - The International Foundation for Electoral Systems*. <https://www.ifes.org/publications/authoritarian-collaboration>
- Couldry, N. (2012). *Media, society, world: Social theory and digital media practice*. Cambridge; Malden, MA: Polity.
- COUNCIL DECISION (CFSP) 2023/1566 of 28 July 2023 Amending Decision 2014/145/CFSP Concerning Restrictive Measures in Respect of Actions Undermining or Threatening the Territorial Integrity, Sovereignty and Independence of Ukraine, 2023/1566, THE COUNCIL OF THE EUROPEAN UNION (2023). <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A32023D1566>
- D’Alessandra, F., & Sutherland, K. (2024). The Promise and Challenges of New Actors and New Technologies in International Justice. *Journal of International Criminal Justice*, 19(1), 9–34.
<https://doi.org/10.1093/jicj/mqab034>
- Davenel, Y. M. (2009). ‘Are national minorities of the former USSR becoming new diasporas? The case of the Tatars of Kazakhstan. *Diasporas*. In *Diasporas: Critical and Interdisciplinary Perspectives*. Inter-Disciplinary Press.

- Davidson, C. (2022). The United Arab Emirates: Evolving Authoritarian Tools. In F. Cavatorta, M. Mekouar, & O. Topak (Eds.), *New Authoritarian Practices in the Middle East and North Africa* (pp. 320–339). Edinburgh University Press. <https://www.cambridge.org/core/books/new-authoritarian-practices-in-the-middle-east-and-north-africa/united-arab-emirates-evolving-authoritariantools/E6257E7B1DF4FAA1D64FE0DEECC73A7E>
- Dayen, D. (2016, April 22). The Android Administration: Google’s Remarkably Close Relationship With the Obama White House, in Two Charts. *The Intercept*. <https://theintercept.com/2016/04/22/googles-remarkably-close-relationship-with-the-obama-white-house-in-two-charts/>
- Debre, I., & Akram, F. (2021, October 25). Facebook’s language gaps weaken screening of hate, terrorism. *AP News*. <https://apnews.com/article/the-facebook-papers-language-moderation-problems-392cb2d065f81980713f37384d07e61f>
- Deck, O. (2023). Bullshit, Pragmatic Deception, and Natural Language Processing. *Dialogue & Discourse*, 14(1), Article 1. <https://doi.org/10.5210/dad.2023.103>
- Deibert, R. (2015). Authoritarianism Goes Global: Cyberspace Under Siege. *Journal of Democracy*, 26(3), 64–78.
- Deibert, R., Palfrey, J., Rohozinski, R., & Zittrain, J. A. (2010). *Access Controlled. The Shaping of Power, Rights, and Rule in Cyberspace*. The MIT Press. <https://mitpress.mit.edu/9780262514354/access-controlled/>
- DeJong, S., & Souza, A. B. de M. (2022). Playing Conspiracy: Framing Conspiracy Theory Analogies within Research-Creation Board Game Design. *M/C Journal*, 25(1), Article 1. <https://doi.org/10.5204/mcj.2869>
- Demir, I. (2022). *Diaspora as Translation and Decolonisation*. Manchester University Press.
- Department for Digital, Culture, Media and Sport. (2018). *A Connected Society, A Strategy for Tackling Loneliness – Laying the Foundations for Change*. Government of the U.K. https://assets.publishing.service.gov.uk/media/5fb66cf98fa8f54aafb3c333/6.4882_DCMS_Loneliness_Strategy_web_Update_V2.pdf
- Diacomet. (n.d.). Diacomet. Retrieved 20 May 2024, from <https://diacomet.eu/>
- Dickinson, P. (2023, August 22). Putin weaponizes history with new textbook justifying Ukraine invasion. *Atlantic Council*. <https://www.atlanticcouncil.org/blogs/ukrainealert/putin-weaponizes-history-with-new-textbook-justifying-ukraine-invasion/>
- DiResta, R., & Perrino, J. (2022). U.S. Influence Operations: The Military’s Resurrected Digital Campaign for Hearts and Minds. The Lawfare Institute. <https://www.lawfaremedia.org/article/us-influence-operations-militarys-resurrected-digital-campaign-hearts-and-minds>
- DiResta, R., Shaffer, K., Ruppel, B., Sullivan, D., Matney, R., Fox, R., Albright, J., & Johnson, B. (2019). The Tactics & Tropes of the Internet Research Agency. *United States Senate Documents*. <https://digitalcommons.unl.edu/senatedocs/2>
- Dodd, V. (2024). “Pick and mix of horror’ online pushes young people to violence, UK police chief says”. *The Guardian Online*. December 18. <https://www.theguardian.com/uk-news/2024/dec/18/pick-and-mix-horror-online-young-people-to-violence-uk>
- Dolan, P., Halpern, D., Hallsworth, M., King, D., & Viaev, I. (2010). *MINDSPACE: Influencing behaviour through public policy*. Cabinet Office and Institute for Government. <https://www.instituteforgovernment.org.uk/sites/default/files/publications/MINDSPACE.pdf>

- Douek, E. (2020). *The Rise of Content Cartels* (The Tech Giants, Monopoly Power, and Public Discourse). Knight First Amendment Institute at Columbia University. <https://knightcolumbia.org/content/the-rise-of-content-cartels>
- Downie, R. (2016). RE: UN Office for Drugs and Crime. Document Number 022702. North Dakota Private Investigative and Security Board v. TigerSwan LLC., No. 2021-0305 (N.D. 2022).
- Dyke, N. V. (2016). *Understanding the Tea Party Movement*. Routledge.
- ECF. (2024). *Horizontal Rule of Law Submission Repeated restrictions on Palestine solidarity*. Brussels: European Civic Forum.
- Eddin, C. (2013). Eddin, C. (2013). THE ASSAD REGIME'S PROPAGANDA (Doctoral dissertation, Georgetown University). [Doctoral Dissertation, Georgetown University]. https://repository.library.georgetown.edu/bitstream/handle/10822/709810/Eddin_georgetown_0076M_12398.pdf?sequence=1&isAllowed=y
- Edwards, L. (2021). Organised lying and professional legitimacy: Public relations' accountability in the disinformation debate. *European Journal of Communication*, 36(2), 168–182. <https://doi.org/10.1177/0267323120966851>
- Elliot Rodger: How misogynist killer became 'incel hero'. (2018, April 25). *BBC News*. <https://www.bbc.com/news/world-us-canada-43892189>
- Elliott, V., Christopher, N., Deck, A., & Schwartz, L. (2021, October 26). The Facebook Papers reveal staggering failures in the Global South. *Rest of World*. <https://restofworld.org/2021/facebook-papers-reveal-staggering-failures-in-global-south/>
- Ellul, J. (1965). *Propaganda. The Formation of Men's Attitudes*. Vintage Books.
- ELSC. (2023). *Suppressing Palestinian Rights Advocacy through the IHRA Working Definition of Antisemitism – Violating the Rights to Freedom of Expression and Assembly in the European Union and the UK*. Amsterdam: European Legal Support Center.
- Erdem, B. K., & Gündüz, U. (2017). A Comparative Analysis of the Representation of Syrian Refugees in Turkish and Diasporic Media: The Case of “etilaf.org.” In *Media, Diaspora and Conflict* (pp. 189–204). Palgrave Macmillan Cham. https://link.springer.com/chapter/10.1007/978-3-319-56642-9_12
- Estes, Nick. (2019). *Our History is the Future: Standing Rock versus the Dakota Access Pipeline, and the Long Tradition of Indigenous Resistance*. Verso.
- Facebook busts Israel-based campaign to disrupt elections in various countries. (2019, May 16). *NBC News*. <https://www.nbcnews.com/tech/tech-news/facebook-busts-israel-based-campaign-disrupt-elections-various-countries-n1006441>
- Fallis, D. (2015). What Is Disinformation? *Library Trends*, 63(3), 401–426.
- Fang, L. (2022, December 20). Twitter Aided the Pentagon in its Covert Online Propaganda Campaign. *The Intercept*. <https://theintercept.com/2022/12/20/twitter-dod-us-military-accounts>
- FedBizOpp. (2010, June 22). *Persona Management Software [Government]*. Federal Business Opportunities. https://web.archive.org/web/20110222010732/https://www.fbo.gov/index?s=opportunity&mode=form&id=d88e9d660336be91552fe8c1a51bacb2&tab=core&_cvview=1
- Feldstein, S. (2021). *The Rise of Digital Repression: How Technology is Reshaping Power, Politics, and Resistance*. Oxford University Press.
- Fernandez de Cordoba, S. (n.d.). *Trade and the MDGs: How Trade Can Help Developing Countries Eradicate Poverty* | United Nations. Retrieved August 7, 2024, from

- <https://www.un.org/en/chronicle/article/trade-and-mdgs-how-trade-can-help-developing-countries-eradicate-poverty>
- Fersh, R., Levison, M., & Ripley, A. (2024). *From Conflict to Convergence: Coming Together to Solve Tough Problems* (1st edition). Wiley.
- Fetzer, J. H. (2004). Disinformation: The Use of False Information. *Minds and Machines*, 14(2), 231–240. <https://doi.org/10.1023/B:MIND.0000021683.28604.5b>
- FIDH. (2018). Table Illustrating Legislative Crackdown on Rights and Freedoms of the Civil Society in Russia since 2012 (Addendum). International Federation for Human Rights. chrome-extension://efaidnbmninnibpcapjpcglclefindmkaj/https://www.fidh.org/IMG/pdf/loirussie_web_oct_18_v2.pdf
- FIDH. (2023, June). FIDH documents the destruction of civil society in Russia, law after law. International Federation for Human Rights. <https://www.fidh.org/en/region/europe-central-asia/russia/fidh-documents-the-destruction-of-civil-society-in-russia-law-after>
- Fielding, N., & Cobain, I. (2011, March 17). Revealed: US psy operation that manipulates social media. *The Guardian*. <https://www.theguardian.com/technology/2011/mar/17/us-spy-operation-social-networks>
- Fischer, N. (2020). Remembering/Imagining Palestine from Afar: The (Lost) Homeland in Contemporary Palestinian Diaspora Literature. In *Spiritual Homelands: The Cultural Experience of Exile, Place and Displacement among Jews and Others* (pp. 31–56). De Gruyter.
- Fischer, V., & O'Mara, S. M. (2022). Neural, psychological, and social foundations of collective memory: Implications for common mnemonic processes, agency, and identity. In *Progress in Brain Research* (Vol. 274, pp. 1–30). Elsevier. <https://doi.org/10.1016/bs.pbr.2022.07.004>
- Fisher, M. (2021, July 25). Disinformation for Hire, a Shadow Industry, Is Quietly Booming. *The New York Times*. <https://www.nytimes.com/2021/07/25/world/europe/disinformation-social-media.html>
- Fiss, J., & Kestenbaum, J. G. (2017). *Respecting Rights? Measuring the World's Blasphemy Laws*. U.S. Commission on International Religious Freedom (USCIRF) .
- Foreign Office Minister condemns Russia for NotPetya attacks*. (2018, January 15). GOV.UK. <https://www.gov.uk/government/news/foreign-office-minister-condemns-russia-for-notpetya-attacks>
- Forestal, J. (2022). *Designing for Democracy: How to Build Community in Digital Environments*. Oxford University Press.
- Forestal, J. (2022). *Designing for Democracy: How to Build Community in Digital Environments*. Oxford University Press.
- Fredheim, R. (2017). The loyal editor effect: Russian online journalism after independence. *Post-Soviet Affairs*, 33(1), 34–48. <https://doi.org/10.1080/1060586X.2016.1200797>
- Freelon, D., & Wells, C. (2020). Disinformation as Political Communication. *Political Communication*, 37(2), 145–156. <https://doi.org/10.1080/10584609.2020.1723755>
- From War to Prison: Repression in Russia is becoming more ‘planned’ and harsh, but not more widespread. (2024). <https://re-russia.net/en/analytics/0125/>
- FTC. (2013). *Statement of the Federal Trade Commission Regarding Google's Search Practices*. Federal Trade Commission. https://www.ftc.gov/sites/default/files/documents/public_statements/statement-commission-regarding-googles-search-practices/130103brillgooglesearchstmt.pdf

- FTC. (2013). *Statement of the Federal Trade Commission Regarding Google's Search Practices*. Federal Trade Commission. https://www.ftc.gov/sites/default/files/documents/public_statements/statement-commission-regarding-googles-search-practices/130103brillgooglesearchstmt.pdf
- Fujimura, N. (2016). Re-election isn't everything: Legislators' goal-seeking and committee activity in Japan. *The Journal of Legislative Studies*, 22(2), 153–174. <https://doi.org/10.1080/13572334.2016.1164437>
- Fung, B. (2024, February 5). DOJ antitrust case targeting Google's ad-tech business will go to trial in September, federal judge rules. *CNN*. <https://www.cnn.com/2024/02/05/tech/doj-antitrust-case-google-ad-trial-september/index.html>
- Fung, B. (2024, February 5). DOJ antitrust case targeting Google's ad-tech business will go to trial in September, federal judge rules. *CNN*. <https://www.cnn.com/2024/02/05/tech/doj-antitrust-case-google-ad-trial-september/index.html>
- Galeotti, M. (2016a). Hybrid, ambiguous, and non-linear? How new is Russia's 'new way of war'? *Small Wars & Insurgencies*, 27(2), 282–301. <https://doi.org/10.1080/09592318.2015.1129170>
- Galeotti, M. (2016b). *PUTIN'S HYDRA: INSIDE RUSSIA'S INTELLIGENCE SERVICES*.
- Galeotti, M. (2017). *Controlling Chaos: How Russia manages its political war in Europe*. https://ecfr.eu/publication/controlling_chaos_how_russia_manages_its_political_war_in_europe/
- Galeotti, M. (2019). *We Need to Talk About Putin: How the West gets him wrong*. Random House.
- Galeotti, M. (2020). *Russian Political War: Moving Beyond the Hybrid*. Routledge & CRC Press. <https://www.routledge.com/Russian-Political-War-Moving-Beyond-the-Hybrid/Galeotti/p/book/9780367731755>
- Garcia-Navarro, L. (2024, July 13). Robert Putnam Knows Why You're Lonely: The Interview. *New York Times (Online)*. <https://www.nytimes.com/2024/07/13/magazine/robert-putnam-interview.html>
- Gartzke, E. (2013). The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth. *International Security*, 38(2), 41–73. https://doi.org/10.1162/ISEC_a_00136
- Gelfert, A. (2018). Fake News: A Definition. *Informal Logic*, 38(1), Article 1. <https://doi.org/10.22329/il.v38i1.5068>
- Gilbert, L., & Mohseni, P. (2011). Beyond Authoritarianism: The Conceptualization of Hybrid Regimes. *Studies in Comparative International Development*, 46(3), 270–297. <https://doi.org/10.1007/s12116-011-9088-x>
- Gillespie, T. (2018). *Custodians of the Internet: Platforms, content moderation, and the hidden decisions that shape social media*. Yale University Press.
- Gilroy, P. (2002). *The black Atlantic: Modernity and double consciousness* (3. impr., reprint). Verso.
- Giovanni, C. (2024, July 3). Have China and the US really decoupled? Not so fast. <https://www.geopolitica.info/have-china-and-the-us-really-decoupled-not-so-fast/>
- Gittens, R. (2017, February 5). Dave Chappelle, Alternative Facts, and the Reinforcement of Racist Ideas | In Media Res. *In Media Res*. <https://mediacommons.org/imr/2017/02/05/dave-chappelle-alternative-facts-and-reinforcement-racist-ideas>
- Glaser, E. (2013, May 17). The west's hidden propaganda machine. *The Guardian*. <https://www.theguardian.com/commentisfree/2013/may/17/west-hidden-propaganda-machine-social-media>

- Glasius, M. (2018). What authoritarianism is ... and is not: * a practice perspective. *International Affairs*, 94(3), 515–533. <https://doi.org/10.1093/ia/iiy060>
- Gleicher, N. (2021). *Meta's Adversarial Threat Report*. <https://about.fb.com/news/2021/12/metad-adversarial-threat-report/>
- Google Antitrust Lawsuits Explained*. (n.d.). [Lanier Law Firm]. <https://www.lanierlawfirm.com/google-antitrust-lawsuits-explained/#:~:text=The%20first%20antitrust%20case%20came,market%20through%20anti%20competitive%20tactics.>
- Gorwa, R. (2024). *The politics of platform regulation: How governments shape online content moderation* (First edition). Oxford University Press.
- Goujard, C., & Cerulus, L. (2024, May 3). Elite Russian hackers breach Scholz's German socialist party. *POLITICO*. <https://www.politico.eu/article/olaf-scholz-social-democratic-party-russian-hackers-fancy-bear/>
- Government Accountability Office. (2013). Military Information Support Operations: Improved Coordination, Evaluations, and Training and Equipment Are Needed (Report No. GAO-13-426SU). Retrieved from: <https://cryptome.org/2013/07/gao-13-426su.pdf>
- Graves, L., & Amazeen, M. A. (2019). *Fact-Checking as Idea and Practice in Journalism*. <https://doi.org/10.1093/acrefore/9780190228613.013.808>
- Gravett, W. H. (2022). Digital Neocolonialism: The Chinese Surveillance State in Africa. *African Journal of International and Comparative Law*, 30(1), 39–58. <https://doi.org/10.3366/ajicl.2022.0393>
- Greece: Problematic Surveillance Bill | Human Rights Watch*. (2022). Human Rights Watch. <https://www.hrw.org/news/2022/12/08/greece-problematic-surveillance-bill>
- Greenberg, A. (2018, August 22). The Untold Story of NotPetya, the Most Devastating Cyberattack in History. *Wired*. <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/>
- Greitens, S. C. (2016). *Dictators and their Secret Police: Coercive Institutions and State Violence*. Cambridge University Press. <https://www.amazon.co.uk/Dictators-their-Secret-Police-Institutions/dp/1107139848>
- Grimes, D. R., & Gorski, D. H. (2022). *Malinformation—an emergent problem for medical journals and scientific communication*. <https://scholar.archive.org/work/njkytr5hzgfrph4jtp2lxcuha/access/wayback/https://files.osf.io/v1/resources/g4jwr/providers/osfstorage/6297df04068631086d729f19?action=download&direct&version=1>
- Grishin, N. (2012, December 3). Found Everything. *Kommersant*. <https://www.kommersant.ru/doc/2065978>
- Grohmann, R., & Corpus Ong, J. (2024). Disinformation-for-Hire as Everyday Digital Labor: Introduction to the Special Issue. *Social Media + Society*, 10(1), 20563051231224723. <https://doi.org/10.1177/20563051231224723>
- Grohmann, R., & Corpus Ong, J. (2024a). Disinformation-for-Hire as Everyday Digital Labor: Introduction to the Special Issue. *Social Media + Society*, 10(1), 20563051231224723. <https://doi.org/10.1177/20563051231224723>
- Gu, H. (2023). Data, Big Tech, and the New Concept of Sovereignty. *Journal of Chinese Political Science*. <https://doi.org/10.1007/s11366-023-09855-1>

- Guess, A. M., & Lyons, B. A. (2020). Misinformation, Disinformation, and Online Propaganda. In J. A. Tucker & N. Persily (Eds.), *Social Media and Democracy* (pp. 10–33). Cambridge University Press. <https://www.cambridge.org/core/books/social-media-and-democracy/misinformation-disinformation-and-online-propaganda/D14406A631AA181839ED896916598500>
- Habib, H., Srinivasan, P., & Nithyanand, R. (2022). Making a Radical Misogynist: How Online Social Engagement with the Manosphere Influences Traits of Radicalization. *Proc. ACM Hum.-Comput. Interact.*, 6(CSCW2), 450:1-450:28. <https://doi.org/10.1145/3555551>
- Haig-Brown, C. (2012). "Decolonizing Diaspora: Whose Traditional Land are We On?". In *Decolonizing Philosophies of Education*. Leiden, The Netherlands: Brill.
- Hall, S. (1990). Cultural Identity and Diaspora. In *Identity: Community, Culture, Difference* (pp. 222–237). Lawrence and Wishart.
- Halperin, A. (2018). *The use of new media by the Palestinian diaspora in the United Kingdom*. Cambridge Scholars Publishing.
- Hamburger, T., & Gold, M. (2014, April 12). Google, once disdainful of lobbying, now a master of Washington influence. *Washington Post*. https://www.washingtonpost.com/politics/how-google-is-transforming-power-and-politicsgoogle-once-disdainful-of-lobbying-now-a-master-of-washington-influence/2014/04/12/51648b92-b4d3-11e3-8cb6-284052554d74_story.html
- Hameleers, M. (2023). Disinformation as a context-bound phenomenon: Toward a conceptual clarification integrating actors, intentions and techniques of creation and dissemination. *Communication Theory*, 33(1), 1–10. <https://doi.org/10.1093/ct/qtac021>
- Han, R. (2015). Manufacturing Consent in Cyberspace: China’s “Fifty-Cent Army”. *Journal of Current Chinese Affairs*, 44(2), 105–134. <https://doi.org/10.1177/186810261504400205>
- Hao, K. (2021, October 5). The Facebook whistleblower says its algorithms are dangerous. Here’s why. *MIT Technology Review*. <https://www.technologyreview.com/2021/10/05/1036519/facebook-whistleblower-frances-haugen-algorithms/>
- Hardaker, C. (2010). *Trolling in asynchronous computer-mediated communication: From user discussions to academic definitions*. 6(2), 215–242. <https://doi.org/10.1515/jplr.2010.011>
- Hardaker, C. (2013). “Uh. . . not to be nitpicky,,,,,but...the past tense of drag is dragged, not drug.”: An overview of trolling strategies. *Journal of Language Aggression and Conflict*, 1(1), 58–86. <https://doi.org/10.1075/jlac.1.1.04har>
- Harsin, J. (2024). Three Critiques of Disinformation (For-Hire) Scholarship: Definitional Vortexes, Disciplinary Unneighborliness, and Cryptonormativity. *Social Media + Society*, 10(1), 20563051231224732. <https://doi.org/10.1177/20563051231224732>
- Hatmaker, T. (2022, March 1). Reddit quarantines r/Russia due to ‘high volume’ of misinformation. *TechCrunch*. <https://techcrunch.com/2022/03/01/reddit-russian-subreddit-quarantine/>
- Hearn, A. (2011). Promotional Culture. In D. Southerton (Ed.), *Encyclopedia of Consumer Culture* (Vol. 1, pp. 1158–1160).
- Heeks, R. (2022). Digital inequality beyond the digital divide: Conceptualizing adverse digital incorporation in the global South. *Information Technology for Development*, 28(4), 688–704. <https://doi.org/10.1080/02681102.2022.2068492>
- Heinrich, A. (2011). *Network Journalism, Journalistic Practice in Interactive Spheres* (1st ed.).

- Henriksen, F. M., Kristensen, J. B., & Mayerhöffer, E. (2024). Dissemination of RT and Sputnik Content in European Digital Alternative News Environments: Mapping the Influence of Russian State-Backed Media Across Platforms, Topics, and Ideology. *The International Journal of Press/Politics*, 29(3), 795–818. <https://doi.org/10.1177/19401612241230281>
- Hirsch, M. (2012). *The Generation of postmemory: Writing and visual culture after the Holocaust*. Columbia University Press.
- Hobsbawm, E. J. (2005). *On history* (reprint). Abacus.
- Holmgren, M. (2022). Autonomy through digital resilience: The importance of upholding the national tech stack.
- Holquist, P. (2001). To Count, to Extract, and to Exterminate Population Statistics and Population Politics in Lite Imperial and Soviet Russia. In R. Grigor & S. T. Martin (Eds.), *A State Of Nations: Empire and Nation-Making in the Age of Lenin and Stalin* (p. 0). Oxford University Press. <https://doi.org/10.1093/oso/9780195144222.003.0005>
- Holznapel, D. (2023). *The Free Speech Recession Hits Home: Mapping Laws and Regulations Affecting Free Speech in 22 Open Democracies*. The Future of Free Speech Project.
- Horowitz, M., Cushion, S., Dragomir, M., Gutiérrez Manjón, S., & Pantti, M. (2022). A Framework for Assessing the Role of Public Service Media Organizations in Countering Disinformation. *Digital Journalism*, 10(5), 843–865. <https://doi.org/10.1080/21670811.2021.1987948>
- House Judiciary GOP [@JudiciaryGOP]. (2024, August 26). *Mark Zuckerberg just admitted three things: 1. Biden-Harris Admin 'pressured' Facebook to censor Americans. 2. Facebook censored Americans. 3. Facebook throttled the Hunter Biden laptop story. Big win for free speech.* <https://t.co/ALlbZd9l6K> [Tweet]. Twitter. <https://x.com/JudiciaryGOP/status/1828201780544504064>
- Howard, P. N., Ganesh, B., Liotsiou, D., Kelly, J., & François, C. (2018). *The IRA, Social Media and Political Polarization in the United States, 2012-2018*.
- Huang, J., & Tsai, K. S. (2022). *Securing Authoritarian Capitalism in the Digital Age: The Political Economy of Surveillance in China*. 88, 2–28. <https://doi.org/10.1086/720144>
- Huang, G., Jia, W., & Yu, W. (2024). Media Literacy Interventions Improve Resilience to Misinformation: A Meta-Analytic Investigation of Overall Effect and Moderating Factors. *Communication Research*, 0(0). <https://doi.org/10.1177/00936502241288103>
- Hutchings, S. C. (2018). Projecting Russia on the global stage: International broadcasting and ‘recursive nationhood’. In *Russian Culture in the Age of Globalization* (pp. 124–145). Routledge. <https://doi.org/10.4324/9781315626628-6>
- Hutchings, S. C. (2024). Uncovering the uncoverers: Identity, performativity and representation in counter-disinformation discourse. *Cultural Studies*, 0(0), 1–28. <https://doi.org/10.1080/09502386.2024.2384942>
- Hutchings, S., Tolz, V., Chatterje-Doody, P., Crilley, R., & Gillespie, M. (2024). *Russia, Disinformation, and the Liberal Order: RT as Populist Pariah*. Cornell University Press. <https://www.degruyter.com/document/isbn/9781501777653/html>
- Ilyasov, M. (2017). Researching the Chechen diaspora in Europe. *Interdisciplinary Political Studies*, 3(1), 201–218.
- Ilyasov, M. (2021). To be or not to be a Chechen? The second generation of Chechens in Europe and their choices of identity. *Frontiers in Sociology*, 6, 1–11.
- Ilyasov, M. (2024). The Clash of Collective Memories in Postwar Chechnya. *Problems of Post-Communism*, 1–15. <https://doi.org/10.1080/10758216.2024.2340565>

- Ilyuk, Y. (2020). Journalistic Investigations in the Digital Age of Post-Truth Politics: The Analysis of Bellingcat's Research Approaches Used for the (Re) Construction of the MH17 Case. "A Critical Theory of the 'Public' for Digitally Mediated Urbanization," 1, 56–78.
<https://www.journals.ehu.lt/index.php/perekrestki/article/view/977>
- Ip, D. (2008). Memories and identity anxieties of Chinese transmigrants in Australia. In *At home in the Chinese diaspora: Memories, identities and belongings* (pp. 33–51). Palgrave Macmillan.
- Ip, M. (2012). Chinese immigration to Australia and New Zealand: Government policies and race relations. In *Routledge Handbook of the Chinese Diaspora* (pp. 156–175). Taylor and Francis Group.
<https://ebookcentral.proquest.com/lib/manchester/detail.action?docID=1125264>.
- ITU. (2023, March). Measuring digital development: Facts and Figures: Focus on Least Developed Countries. ITU. <https://www.itu.int/itu-d/reports/statistics/facts-figures-for-ldc/>
- Jauhainen, J., Özçürümez, S., & Tursun, Ö. (2022). Internet and social media uses, digital divides, and digitally mediated transnationalism in forced migration: Syrians in Turkey. *Global Networks*, 22(2), 181–343.
- Jégo, M. (2023, August 19). *Russia's new history textbook reinforces the Kremlin's narrative on the war in Ukraine*. https://www.lemonde.fr/en/international/article/2023/08/19/russia-s-new-history-textbook-reinforces-the-kremlin-s-narrative-on-the-war-in-ukraine_6098737_4.html
- Kahraman, A. (2014). The Crimean Tatar national movement in the publications of inner and outer diaspora: Lenin bayragi, emel and dergi? [Masters]. Middle East Technical University.
- Kaplan, P. (2007, August 9). US lawmakers plan Google-DoubleClick deal hearings. *Reuters*.
<https://www.reuters.com/article/idUSN1832669720070719/>
- Kaša, R., & Mieriņa, I. (Eds.). (2019). *The Emigrant Communities of Latvia: National Identity, Transnational Belonging, and Diaspora Politics*. Springer International Publishing.
<https://doi.org/10.1007/978-3-030-12092-4>
- Keats Citron, D. (2018). Extremist Speech, Compelled Conformity, and Censorship Creep. *Notre Dame Law Review*, 93(3), 1035.
- Keller, F. B., Schoch, D., Stier, S., & Yang, J. (2020). Political Astroturfing on Twitter: How to Coordinate a Disinformation Campaign. *Political Communication*, 37(2), 256–280.
<https://doi.org/10.1080/10584609.2019.1661888>
- Kerr, D. (2024, August 6). Google is defiant after losing antitrust lawsuit and being called a "monopolist." *NPR*. <https://www.npr.org/2024/08/06/nx-s1-5064669/google-loses-antitrust-monopoly-justice-department-lawsuit>
- Khanal, S., Zhang, H., & Taeihagh, A. (2024). Why and how is the power of Big Tech increasing in the policy process? The case of generative AI. *Policy and Society*, puae012.
<https://doi.org/10.1093/polsoc/puae012>
- King, G., Pan, J., & Roberts, M. E. (2013). How Censorship in China Allows Government Criticism but Silences Collective Expression. *American Political Science Review*, 107(2), 326–343.
<https://doi.org/10.1017/S0003055413000014>
- Koinova, M. (2009). Conditions and timing of moderate and radical diaspora mobilization: Evidence from conflict-generated diasporas. In *Global Migration and Transnational Politics*, Working Paper (p. 6).
- Koinova, M. (2021). *Diaspora entrepreneurs and contested states* (First edition). Oxford University Press.

- Kolstø, P. (2011). Beyond Russia, Becoming Local: Trajectories of Adaption to the Fall of the Soviet Union among Ethnic Russians in the Former Soviet Republics. *Journal of Eurasian Studies*, 2(2), 153–163. <https://doi.org/10.1016/j.euras.2011.03.006>
- Kottasová, I. (2024, June 4). How Russian trolls are meddling in the world’s second-biggest democratic vote. *CNN*. <https://www.cnn.com/2024/06/04/climate/russia-disinformation-eu-elections-intl/index.html>
- Kovalenko, O. (2024, May 21). How Kremlin uses false fact checks to spread disinformation. *Voice of America*. <https://www.voanews.com/a/how-kremlin-uses-false-fact-checks-to-spread-disinformation/7620992.html>
- Kravets, D., & Toepfl, F. (2022). Gauging reference and source bias over time: How Russia’s partially state-controlled search engine Yandex mediated an anti-regime protest event. *Information, Communication & Society*, 25(15), 2207–2223. <https://doi.org/10.1080/1369118X.2021.1933563>
- Kravets, D., Beseler, A., Toepfl, F., & Ryzhova, A. (2024). The Kremlin-Controlled Search Engine Yandex as a Tool of Foreign Propaganda. *Russian Analytic Digest*, 313. https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Russian_Analytical_Digest_313.pdf
- Kruger, A., First Draft Team, & Zhang, S. (2023). Understanding the Flow of Online Information and Misinformation in the Australian Chinese Diaspora. In *Mobile Communication and Online Falsehoods in Asia. Mobile Communication in Asia: Local Insights, Global Implications*. (pp. 69–96). Springer. https://link.springer.com/chapter/10.1007/978-94-024-2225-2_5#citeas
- Krupsky, M. (2023, March 27). *Why the growing number of foreign agent laws around the world is bad for democracy*. Retrieved from The Conversation: <https://theconversation.com/why-the-growing-number-of-foreign-agent-laws-around-the-world-is-bad-for-democracy-201846>
- Krupsky, M. (2023). The Impact of Russia’s “Foreign Agents” Legislation on Civil Society. *Fletcher Russia and Eurasia Program*, 47(2), 55–70.
- Kung, C. S., Jane Lytvynenko, William. (2020, January 7). Disinformation For Hire: How A New Breed Of PR Firms Is Selling Lies Online. *BuzzFeed News*. <https://www.buzzfeednews.com/article/craigsilverman/disinformation-for-hire-black-pr-firms>
- LaForge, G., & Gruver, P. (2023). *Governing the Digital Future [Government Report]*. New America. https://d1y8sb8igg2f8e.cloudfront.net/documents/Governing_the_Digital_Future_2023-10-02_131622_Nfua5xR.pdf
- Laitin, D. D. (1998). *Identity in formation: The Russian-speaking populations in the near abroad*. Cornell University Press.
- Lakhani, M., & Khan, H. M. A. (2023). Fighting Disinformation in the Palestine Conflict: The Role of Generative AI and Islamic Values. <https://doi.org/10.5281/ZENODO.11265514>
- Lamont, W. M. (Ed.). (1998). *Historical controversies and historians*. UCL Press.
- Largest Companies by Market Cap*. (n.d.). [Dataset]. <https://companiesmarketcap.com/>
- Largest Companies by Market Cap*. (n.d.). [Dataset]. <https://companiesmarketcap.com/>
- Lasswell, H. D. (1971). *Propaganda Technique In World War I*. MIT Press.
- Lau, Y. (2023, May 16). Finland’s ‘visionary’ fight against disinformation teaches citizens to question what they see online. *Canada’s National Observer*. <https://www.nationalobserver.com/2023/05/16/news/finland-visionary-fight-disinformation-teaches-citizens-question-online>

- Launching Horizon Europe project DIACOMET. (2023, June 9). *Vytautas Magnus University*.
<https://www.vdu.lt/en/launching-horizon-europe-project-diacomet/>
- Lee, R. (2006). “Flexible Citizenship”: Strategic Chinese Identities in Asian Australian Literature. *Journal of Intercultural Studies*, 27(1–2), 213–227. <https://doi.org/10.1080/07256860600608049>
- Leong, S. (2015). Provisional Business Migrants to Western Australia, Social Media, and Conditional Belonging. In *Media and Communication in the Chinese Diaspora* (pp. 184–202). Routledge.
<https://www.taylorfrancis.com/chapters/edit/10.4324/9781315717265-11/provisional-business-migrants-western-australia-social-media-conditional-belonging-susan-leong>
- Levinger, M. (2018). Master Narratives of Disinformation Campaigns. *Journal of International Affairs*, 71(1.5), 125–134.
- Lewis, H. (2019, August 7). To Learn About the Far Right, Start With the ‘Manosphere’. *Atlantic Online*.
- Lilkov, D. (2020). Made in China: Tackling Digital Authoritarianism. *European View*, 19(1), 110–110.
<https://doi.org/10.1177/1781685820920121>
- Lim, S. Y., & MacDonald, J. B. (2022). COVID-19-related racial discrimination on Asian Australians: An evaluation of symptoms of psychological distress, social support, and acculturation. *Traumatology*, 28(3), 366–375. <https://doi.org/10.1037/trm0000374>
- Lippmann, W. (1922). *Public Opinion*. Transaction Publishers.
- Lock, I., & Ludolph, R. (2020). Organizational propaganda on the Internet: A systematic review. *Public Relations Inquiry*, 9(1), 103–127. <https://doi.org/10.1177/2046147X19870844>
- Locker, R. (2014). Military propaganda websites on verge of extinction. *USA Today*.
<https://usatoday.com/story/nation/2014/01/02/trans-regional-web-initiative-defense-bill/4291467/>
- Lohr, S. (2020, September 21). This Deal Helped Turn Google Into an Ad Powerhouse. Is That a Problem? *The New York Times*. <https://www.nytimes.com/2020/09/21/technology/google-doubleclick-antitrust-ads.html>
- Lu, J. (2017). Understanding the Chinese diaspora: The identity construction of diasporic Chinese in the age of digital media [Doctoral, Queensland University of Technology].
https://eprints.qut.edu.au/112817/1/Jiajie_Lu_Thesis.pdf
- Lu, M. (2024, July 16). Charted: The G7’s Declining Share of Global GDP. *Visual Capitalist*.
<https://www.visualcapitalist.com/charted-the-g7s-declining-share-of-global-gdp/>
- Lyon, D. (2018). *The Culture of Surveillance: Watching as a Way of Life* | Wiley. Wiley.
<https://www.wiley.com/en-us/The+Culture+of+Surveillance%3A+Watching+as+a+Way+of+Life-p-9780745671734>
- Mac, R. (2021, May 12). Instagram Labeled One Of Islam’s Holiest Mosques A Terrorist Organization. *BuzzFeed News*. <https://www.buzzfeednews.com/article/ryanmac/instagram-facebook-censored-al-aqsa-mosque>
- MacAskill, E. (2011, January 16). Stuxnet cyberworm heads off US strike on Iran. *The Guardian*.
<https://www.theguardian.com/world/2011/jan/16/stuxnet-cyberworm-us-strike-iran>
- Mackintosh, E. (2019). Finland is winning the war on fake news. What it’s learned may be crucial to Western democracy. *CNN*. <https://edition.cnn.com/interactive/2019/05/europe/finland-fake-news-intl/>

- Maghraoui, D. (2022). 'The Freedom of No Speech': Journalists and the Multiple Layers of Authoritarian Practices in Morocco. In F. Cavatorta, M. Mekouar, & O. Topak (Eds.), *New Authoritarian Practices in the Middle East and North Africa* (pp. 189–207). Edinburgh University Press. <https://www.cambridge.org/core/books/new-authoritarian-practices-in-the-middle-east-and-north-africa/freedom-of-no-speech-journalists-and-the-multiple-layers-of-authoritarian-practices-in-morocco/74ACCE2221B92CFAA91DC7D63E829E4D>
- Maharani, N. A. M. (2024). Social media as a primary source of information: Exploring its role in disseminating the current situation in Palestine. *Gema Wiralodra*, 15(1), 275–281. <https://doi.org/10.31943/gw.v15i1.628>
- Mahubani, K. (2024, March 21). Measuring the power of the Global South. <https://www.chathamhouse.org/publications/the-world-today/2024-02/measuring-power-global-south>
- Mansted, K. (2020). *Strong Yet Brittle: The Risks of Digital Authoritarianism*.
- Martin, C. A. (2023). Influxes and invaders: The intersections between the metaphoric construction of immigrant otherness and ethnonationalism. *Ethnic and Racial Studies*, 46(7), 1478–1501. <https://doi.org/10.1080/01419870.2022.2142062>
- Marwick, A., & Lewis, R. (2017). Media manipulation and disinformation online. *New York: Data & Society Research Institute*, 7–19.
- Masharqa, S. (2020). Fake News in Palestine: Exploratory Research into Content, Channels and Responses (p. 47). 7amleh –The Arab Center for Social Media Advancement. <https://fada.birzeit.edu/handle/20.500.11889/7194>
- May, R. (2018, May 8). How Putin's oligarchs funneled millions into GOP campaigns. *The Dallas Morning News*. <https://www.dallasnews.com/opinion/commentary/2018/05/08/how-putin-s-oligarchs-funneled-millions-into-gop-campaigns/>
- Mayhew, D. R. (2004). *Congress: The electoral connection* (2nd ed). Yale University Press.
- Mchangana, J., & Alkiviadou, N. (2020). *The Digital Berlin Wall: How Germany (Accidentally) Created a Prototype for Global Online Censorship - Act two*. Copenhagen: Justitia.
- Meduza. (2016, June 10). Госдума окончательно приняла законопроект о новостных агрегаторах. *Meduza*. <https://meduza.io/news/2016/06/10/gosduma-okonchatelno-prinyala-zakonoproekt-o-novostnyh-agregatorah>
- Meduza. (2018, October 22). В Госдуме предложили ограничить долю иностранцев в новостных агрегаторах. *Meduza*. <https://meduza.io/news/2018/10/22/v-gosdume-predlozhili-ogranichit-dolyu-inostrantsev-v-novostnyh-agregatorah>
- Meduza. (2018, October 22). В Госдуме предложили ограничить долю иностранцев в новостных агрегаторах. *Meduza*. <https://meduza.io/news/2018/10/22/v-gosdume-predlozhili-ogranichit-dolyu-inostrantsev-v-novostnyh-agregatorah>
- Meduza. (2019, August 16). The right stuff How the Russian authorities forced the country's top news aggregator to purge unwanted stories. *Meduza*. <https://meduza.io/en/feature/2019/08/16/the-right-stuff>
- Meduza. (2019, August 16). The right stuff How the Russian authorities forced the country's top news aggregator to purge unwanted stories. *Meduza*. <https://meduza.io/en/feature/2019/08/16/the-right-stuff>
- Mehta, A. (2024, August 5). *Memorandum Opinion: United States of America et al. V. Google LLC*. US District Court, DC. <https://www.courtlistener.com/docket/18552824/1033/united-states-of-america-v-google-llc/>

- Mehta, A. (2024, August 5). *Memorandum Opinion: United States of America et al. V. Google LLC*. US District Court, DC. <https://www.courtlistener.com/docket/18552824/1033/united-states-of-america-v-google-llc/>
- Mejia, R., Beckermann, K., & Sullivan, C. (2018). White lies: A racial history of the (post)truth. *Communication and Critical/Cultural Studies*, 15(2), 109–126. <https://doi.org/10.1080/14791420.2018.1456668>
- Mendelberg, T. (2017). *The Race Card: Campaign Strategy, Implicit Messages, and the Norm of Equality*. Princeton University Press,. <https://doi.org/10.1515/9781400889181>
- Mendelberg, T. (2017). *The Race Card: Campaign Strategy, Implicit Messages, and the Norm of Equality*. Princeton University Press,. <https://doi.org/10.1515/9781400889181>
- Merlin, A. (2014). Remembering and forgetting in Chechnya today: Using the Great Patriotic War to create a new historical narrative. In *Chechnya at war and beyond* (pp. 37–57). Routledge.
- Meyer, R. (2014, April 4). The Fall of Internet Freedom: Meet the Company That Secretly Built 'Cuban Twitter'. *The Atlantic*. <https://www.theatlantic.com/technology/archive/2014/04/the-fall-of-internet-freedom-meet-the-company-that-secretly-built-cuban-twitter/360168>
- Michaelson, E., Sterken, R., & Pepp, J. (2019). What's New About Fake News? *Journal of Ethics and Social Philosophy*, 16(2). <https://doi.org/10.26556/jesp.v16i2.629>
- Miconi, A. (2020). News from the Levant: A Qualitative Research on the Role of Social Media in Syrian Diaspora. *Social Media + Society*, 6(1), 1–12. <https://doi.org/10.1177/205630511990033>
- Middle East Monitor (2023, May 31). *Palestine president issues decree criminalising denial of Nakba*. Retrieved from Middle East Monitor: <https://www.middleeastmonitor.com/20230531-palestine-president-issues-decree-criminalising-denial-of-nakba/>
- Miladi, N. (2023). Global media coverage of the Palestinian-Israeli conflict: Reporting the Sheikh Jarrah evictions (First). Bloomsbury Visual Arts. <https://www-bloomsburycollections-com.manchester.idm.oclc.org/monograph?docid=b-9780755649921>
- Miller, M. (2024, March 20). *Imposing Sanctions on Actors Supporting Kremlin-Directed Disinformation Efforts*. United States Department of State. <https://www.state.gov/imposing-sanctions-on-actors-supporting-kremlin-directed-disinformation-efforts/>
- Miloš, G., & Mlejnková, P. (2021). *Challenging Online Propaganda and Disinformation in the 21st Century*. Springer International Publishing. <https://books-scholarsportal-info.myaccess.library.utoronto.ca/uri/ebooks/ebooks6/springer6/2021-06-12/1/9783030586249>
- Miloš, G., & Mlejnková, P. (2021). *Challenging Online Propaganda and Disinformation in the 21st Century*. Springer International Publishing. <https://books-scholarsportal-info.myaccess.library.utoronto.ca/uri/ebooks/ebooks6/springer6/2021-06-12/1/9783030586249>
- Milshtein, M. (2009a). Memory “from Below”: Palestinian Society and the Nakba Memory. In *Palestinian Collective Memory and National Identity* (1st ed.). Palgrave Macmillan. https://link.springer.com/chapter/10.1057/9780230621633_4
- Milshtein, M. (2009b). The Memory that Never Dies: The Nakba Memory and the Palestinian National Movement. In *Palestinian Collective Memory and National Identity* (1st ed., pp. 47–69). Palgrave Macmillan US. <https://www.vlebooks.com/Product/Index/889848?page=0&startBookmarkId=-1>
- Monaghan, J. (2014, April 17). V Kontakte Founder Says Sold Shares Due to FSB Pressure. *The Moscow Times*. <https://www.themoscowtimes.com/2014/04/17/vkontakte-founder-says-sold-shares-due-to-fsb-pressure-a34132>

- Moreno, J. (2022, January 14). China Seen Backing ‘Digital Authoritarianism’ in Latin America. *Voice of America*. <https://www.voanews.com/a/china-seen-backing-digital-authoritarianism-in-latin-america-/6398072.html>
- Muhareb, M. (2013). The Zionist Disinformation Campaign in Syria and Lebanon during the Palestinian Revolt, 1936-1939. *Journal of Palestine Studies*, 42(2), 6–25.
<https://doi.org/10.1525/jps.2013.42.2.6>
- Mukhametshina, E. (2019, February 12). Госдума пока не будет принимать законопроект о новостных агрегаторах. *Vedomosti*.
<https://www.vedomosti.ru/politics/articles/2019/02/12/793973-novostnih-agregatorah>
- Mullins, B. (2024, June 6). The Hidden Life of Google’s Secret Weapon. *The Wall Street Journal*.
<https://www.wsj.com/us-news/law/google-lawyer-secret-weapon-joshua-wright-c98d5a31>
- Mullins, B. (2024, June 6). The Hidden Life of Google’s Secret Weapon. *The Wall Street Journal*.
<https://www.wsj.com/us-news/law/google-lawyer-secret-weapon-joshua-wright-c98d5a31>
- Murthy, Dr. V. H. (2023). *Our Epidemic of Loneliness and Isolation: The U.S. Surgeon General’s Advisory on the Healing Effects of Social Connection and Community*. United States Public Health Service.
<https://www.hhs.gov/sites/default/files/surgeon-general-social-connection-advisory.pdf>
- Murthy, Dr. V. H. (2023). *Our Epidemic of Loneliness and Isolation: The U.S. Surgeon General’s Advisory on the Healing Effects of Social Connection and Community*. United States Public Health Service.
<https://www.hhs.gov/sites/default/files/surgeon-general-social-connection-advisory.pdf>
- Nakashima, E. (2022, September 19). Pentagon opens sweeping review of clandestine psychological operations. *The Washington Post*. <https://www.washingtonpost.com/national-security/2022/09/19/pentagon-psychological-operations-facebook-twitter/>
- Nakashima, E., & Warrick, J. (2012, June 1). Stuxnet was work of U.S. and Israeli experts, officials say. *Washington Post*. https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html
- Napoli, P., & Caplan, R. (2016). *When Media Companies Insist They’re Not Media Companies and Why it Matters for Communications Policy*.
- National Intelligence Council’s Strategic Futures Group. (2021). US-Backed International Norms Increasingly Contested [Government Report].
- Nellyullathil, M. (2020). Teaching Open Source Intelligence (OSINT) Journalism: Strategies and Priorities. *Communication & Journalism Research*, 9(1), 61–73.
- Nets-Zehngut, R. (2014). The Israeli and Palestinian collective memories of their conflict: Determinants, characteristics, and implications. *Brown Journal of World Affairs*, 20(2), 103-124.
- Newman, B., Merolla, J. L., Shah, S., Lemi, D. C., Collingwood, L., & Ramakrishnan, S. K. (2021). The Trump Effect: An Experimental Investigation of the Emboldening Effect of Racially Inflammatory Elite Communication. *British Journal of Political Science*, 51(3), 1138–1159.
<https://doi.org/10.1017/S0007123419000590>
- Ng, A., & Sakellariadis, J. (2024, January 17). Inside Biden’s secret surveillance court. *POLITICO*.
<https://www.politico.com/news/2024/01/17/inside-bidens-secret-surveillance-court-00136175>

- Nimmo, B., Torrey, M., Franklin, M., Agranovich, D., Milam, M., Hundley, L., & Flaim, R. (2023). *Adversarial Threat Report*. Meta. https://scontent-lhr6-2.xx.fbcdn.net/v/t39.8562-6/10000000_878173163681285_2523028760863660247_n.pdf?_nc_cat=100&ccb=1-7&_nc_sid=b8d81d&_nc_ohc=ZY4VkrYYk5sQ7kNvgHUI8Cy&_nc_ht=scontent-lhr6-2.xx&oh=00_AYB_hd8TU9iv1I9AIEBzIQ6tSUQmRXAgfzK9Txaogm2gA&oe=66C296C8
- Nimr, S. (2008). Fast Forward to the Past: A Look into Palestinian Collective Memory. *Cahiers de Littérature Orale*, 63–64, 338–349. <https://doi.org/10.4000/clo.287>
- Nix, N. (2022, August 24). Facebook, Twitter dismantle a U.S. influence campaign about Ukraine. *Washington Post*. <https://www.washingtonpost.com/technology/2022/08/24/facebook-twitter-us-influence-campaign-ukraine/>
- Notley, T., & Dezuanni, M. (2019). Advancing children’s news media literacy: Learning from the practices and experiences of young Australians. *Media, Culture & Society*, 41(5), 689–707. <https://doi.org/10.1177/0163443718813470>
- Nur, M. (2008). Remembering the Palestinian Nakba: Commemoration, oral history and narratives of memory. *Holy Land Studies*, 7(2), 123–156. <https://doi.org/10.3366/E147494750800019X>
- Nylen, L. (2021, March 16). How Washington fumbled the future. *Politico*. v
- O’Neil, C. (2016). *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. The Crown Publishing Group.
- Oberoi, K. (2022, March 1). Reddit ‘Quarantines’ subreddit r/Russia for spreading disinformation. *MobileSyrup*. <https://mobilesyrup.com/2022/03/01/reddit-quarantines-subreddit-r-russia-for-spreading-disinformation/>
- Okano-Heijmans, M. (2023). Open strategic autonomy. https://www.clingendael.org/sites/default/files/2023-01/Open_strategic_autonomy_.pdf
- Ong, J. C., & Cabañes, J. V. A. (2018). *Architects of Networked Disinformation: Behind the Scenes of Troll Accounts and Fake News Production in the Philippines*. <https://hdl.handle.net/20.500.14394/8445>
- Open Secrets. (2024). *Top Spenders*. Open Secrets. <https://www.opensecrets.org/federal-lobbying/top-spenders?cycle=2024>
- Opinion | The bad guys on social media are learning new tricks. (2021, December 23). *Washington Post*. <https://www.washingtonpost.com/opinions/2021/12/23/facebook-meta-2021-threat-report/>
- Ostrovsky, A. (2015). *The Invention of Russia: The Journey from Gorbachev’s Freedom to Putin’s War*. Atlantic Books Ltd.
- Overly, S. (2020, October 8). Facebook bans firm behind Turning Point’s election troll farm. *POLITICO*. <https://www.politico.com/news/2020/10/08/facebook-turning-point-election-troll-427985>
- Owen, D. M. (2022). Trump’s Effect on the Media World and Coverage of Presidents. In *The Trump Effect: Disruption and its Consequences in US Politics and Government*. Rowman & Littlefield Publishing Group, inc.
- Ozdoeva, M. (2024, February 24). Dan’ uvazheniia pamiati: V Kazakhstane vspominali deportatsiiu ingushei i chechentsev 80 let nazad. *Gazeta Ingush*. <https://gazetaingush.ru/v-kazakhstane-vspominali-deportatsiyu-ingushey-i-chechencev-80-let-nazad>
- Padua, J. A., & Liu, A. Y. (2019). THE MANCHURIAN QUESTION: CHINA’S EXPANDING GLOBAL MEDIA DOMINANCE AND THE CHINESE DIASPORA [Masters, Naval Postgraduate School]. https://upload.wikimedia.org/wikipedia/commons/1/12/THE_MANCHURIAN_QUESTION-

_CHINA%E2%80%99S_EXPANDING_GLOBAL_MEDIA_DOMINANCE_AND_THE_CHINESE_DIASPORA_%28IA_themanchurianque1094564041%29.pdf

- Passerini, L. (2009). *Fascism in popular memory: The cultural experience of the Turin working class* (R. Lumley & J. Bloomfield, Trans.). Cambridge University Press.
- Paxton, K. (2020, December 16). *Complaint: The State of Texas et al. V. Google LLC*. US District Court, Eastern District of Texas.
[https://www.texasattorneygeneral.gov/sites/default/files/images/admin/2020/Press/20201216_1%20Complaint%20\(Redacted\).pdf](https://www.texasattorneygeneral.gov/sites/default/files/images/admin/2020/Press/20201216_1%20Complaint%20(Redacted).pdf)
- Pearson, J. S. (2024). Defining Digital Authoritarianism. *Philosophy & Technology*, 37(2), 73.
<https://doi.org/10.1007/s13347-024-00754-8>
- Pennington, N., Hall, J. A., & Holmstrom, A. J. (2024). The American Friendship Project: A report on the status and health of friendship in America. *PLOS ONE*, 19(7), e0305834.
<https://doi.org/10.1371/journal.pone.0305834>
- Pennycook, G., Cheyne, J. A., Barr, N., Koehler, D. J., & Fugelsang, J. A. (2015). On the reception and detection of pseudo-profound bullshit. *Judgment and Decision Making*, 10(6), 549–563.
<https://doi.org/10.1017/S1930297500006999>
- Peteet, J. (2007). PROBLEMATIZING A PALESTINIAN DIASPORA. *International Journal of Middle East Studies*, 39(4), 627–646. <https://doi.org/doi:10.1017/S0020743807071115>
- Polyakova, A., & Meserole, C. (2019). *Exporting digital authoritarianism: The Russian and Chinese models*. (Policy Brief, Democracy and Disorder Series, pp. 1–22). Brookings.
https://www.brookings.edu/wp-content/uploads/2019/08/FP_20190827_digital_authoritarianism_polyakova_meserole.pdf
- Pomerantsev, P. (2019). *This Is Not Propaganda*. <https://www.hachettebookgroup.com/titles/peter-pomerantsev/this-is-not-propaganda/9781541762138/?lens=publicaffairs>
- Pro-Israeli Influence Network. New Findings*. (2024). Fakereporter. https://fakereporter.net/pdf/pro-Israeli_influence_network-new_findings-0624.pdf
- Publications | Intelligence Committee*. (2020). <https://www.intelligence.senate.gov/publications/report-select-committee-intelligence-united-states-senate-russian-active-measures>
- Putin, V. (2024a, February 9). *Interview to Tucker Carlson: President of Russia* (T. Carlson, Interviewer) [Interview]. <http://www.en.kremlin.ru/events/president/transcripts/interviews/73411>
- Putnam, R. D. (2000). *Bowling Alone: The Collapse and Revival of American Community* (First Edition). Simon and Schuster.
- Putnam, R. D. (with Romney Garrett, S.). (2020). *The Upswing: How We Came Together a Century Ago and How We Can Do It Again*. Simon and Schuster.
- Puyosa, I. (2021). Asymmetrical information warfare in the Venezuelan contested media spaces. In *When Media Succumbs to Rising Authoritarianism* (pp. 32–45). Routledge.
<https://doi.org/10.4324/9781003105725-4>
- Qiang, X. (2019). The Road to Digital Unfreedom: President Xi's Surveillance State. *Journal of Democracy*. <https://www.journalofdemocracy.org/articles/the-road-to-digital-unfreedom-president-xis-surveillance-state/>

- Quinn, B. (2024, July 30). Misinformation about Southport attack suspect spreads on social media. *The Guardian*. <https://www.theguardian.com/uk-news/article/2024/jul/30/misinformation-southport-attack-suspect-social-media-conspiracy-theories>
- Ratkiewicz, J., Conover, M., Meiss, M., Goncalves, B., Flammini, A., & Menczer, F. (2011). Detecting and Tracking Political Abuse in Social Media. *Proceedings of the International AAAI Conference on Web and Social Media*, 5(1), Article 1. <https://doi.org/10.1609/icwsm.v5i1.14127>
- Rauch, J. (2021). *The Constitution of Knowledge*. Brookings Institution Press. <https://www.brookings.edu/books/the-constitution-of-knowledge/>
- Re: Russia. (2023, December 13). Unfriendly Status: Expanding the scope of the ‘foreign agent’ label and its related restrictions, the Russian authorities are looking for a reliable bridge to criminalise those with this status. Re: Russia. <https://re-russia.net/en/review/442/>
- Reckwitz, A. (2020). *Society of Singularities*. Cambridge: Polity.
- Reddi, M., Kuo, R., & Kreiss, D. (2023). Identity propaganda: Racial narratives and disinformation. *New Media & Society*, 25(8), 2201–2218. <https://doi.org/10.1177/14614448211029293>
- Reeves, K., & Mountford, B. (2011a). Sojourning and settling: Locating Chinese Australian history. *Australian Historical Studies*, 42(1), 111–125. <https://doi.org/10.1080/1031461X.2010.539620>
- Regehr, K., Shaughnessy, C., Zhao, M., & Shaughnessy, N. (2024). *Safer Scrolling: How Algorithms Popularise and Gamify Online Hate and Misogyny for Young People* (Understanding the Cel: Vulnerability, Violence and In(Ter)vention). University College London and University of Kent. <https://www.alignplatform.org/resources/safer-scrolling-how-algorithms-popularise-and-gamify-online-hate-and-misogyny-young>
- Reiter, S. (2022, May 6). “Toxic Assets” How Russia’s Invasion of Ukraine tore Yandex apart. *Meduza*. <https://meduza.io/en/feature/2022/05/06/toxic-assets>
- Reply-Guys Go Hunting: An Investigation into a U.S. Astroturfing Operation on Facebook, Twitter, and Instagram*. (2020). Stanford Internet Observatory. <https://cyber.fsi.stanford.edu/publication/reply-guys-go-hunting-investigation-us-astroturfing-operation-facebook-twitter-and>
- Revie, R. (2015). Contemporary Conflict and the Online Information Environment: An examination of American military engagement with Web 2.0 [Doctoral thesis, University of Bath]. The University of Bath Research Portal. <https://researchportal.bath.ac.uk/en/studentTheses/contemporary-conflict-and-the-online-information-environment>
- Rid, T. (2011). Cyber War Will Not Take Place. *Journal of Strategic Studies*, 35(1), 5–32. <https://doi.org/10.1080/01402390.2011.608939>
- Rid, T. (2020). *Active Measures: The Secret History of Disinformation and Political Warfare*. <https://dauntbooks.co.uk/shop/books/active-measures-the-secret-history-of-disinformation-and-political-warfare>
- Ring, T. A. (2015). Russian information operations and the rise of the global internet [Masters]. University of Washington.
- Roberts, M. E. (2018). *Censored: Distraction and Diversion Inside China’s Great Firewall*. Princeton University Press. <https://press.princeton.edu/books/hardcover/9780691178868/censored>
- Roberts, S. T. (2018). Digital detritus: “Error” and the logic of opacity in social media content moderation. *First Monday*. <https://doi.org/10.5210/fm.v23i3.8283>
- Rossini, P. (2023). Farewell to Big Data? Studying Misinformation in Mobile Messaging Applications. *Political Communication*, 40(3), 361–366. <https://doi.org/10.1080/10584609.2023.2193563>

- Runcheva Tasev, H., & Apostolovska-Stepanoska, M. (2019). *EU AGAINST FAKE NEWS – THE NEED FOR POLICY ACTION COUNTERING ONLINE DISINFORMATION*.
<http://hdl.handle.net/20.500.12188/14457>
- Russia bans ‘international LGBT movement’ for ‘extremism’. (2024, November 30). *Le Monde*.
https://www.lemonde.fr/en/russia/article/2023/11/30/russia-bans-international-lgbt-movement-for-extremism_6302538_140.html
- Russia: Freedom in the World 2024 Country Report. (n.d.). Freedom House. Retrieved 11 August 2024, from <https://freedomhouse.org/country/russia/freedom-world/2024>
- Russia: New Heights on Repression | Human Rights Watch. (2024, January 11).
<https://www.hrw.org/news/2024/01/11/russia-new-heights-repression>
- Russia: Repressive Laws Used to Crush Civic Freedoms | Human Rights Watch. (2024, August 7).
<https://www.hrw.org/news/2024/08/07/russia-repressive-laws-used-crush-civic-freedoms>
- Rutland, P. (2021). Introduction: Nation-building in the Baltic states: thirty years of independence. *Journal of Baltic Studies*, 52(3), 419–424. <https://doi.org/10.1080/01629778.2021.1944551>
- Safran, W. (1991). Diasporas in Modern Societies: Myths of Homeland and Return. *Diaspora: A Journal of Transnational Studies*, 1(1), 83–99. <https://doi.org/10.1353/dsp.1991.0004>
- Sahoo, A. K. (2006a). Issues of Identity in the Indian Diaspora: A Transnational Perspective. *Perspectives on Global Development and Technology*, 5(1–2), 81–98.
<https://doi.org/10.1163/156915006777354482>
- Sallai, D., & Schnyder, G. (2021). What Is “Authoritarian” About Authoritarian Capitalism? The Dual Erosion of the Private–Public Divide in State-Dominated Business Systems. *Business & Society*, 60(6), 1312–1348. <https://doi.org/10.1177/0007650319898475>
- SAM.gov. (2008, October 7). Presolicitation: Trans Regional Web Initiative.
<https://sam.gov/opp/9b6914aef85cfc889d8ed5604204356a/view>
- SAM.gov. (2009, September 18). Award Notice: TRWI (Trans Regional Web Initiative).
<https://sam.gov/opp/1cd60ef2b74519e462e1c4391c43c914/view>
- Sarajlic, E. (2019). Bullshit, Truth, and Reason. *Philosophia*, 47(3), 865–879.
<https://doi.org/10.1007/s11406-018-9990-9>
- Sayegh, E. (2023, February 28). APT28 Aka Fancy Bear: A Familiar Foe By Many Names. *Forbes*.
<https://www.forbes.com/sites/emilsayegh/2023/02/28/apt28-aka-fancy-bear-a-familiar-foe-by-many-names/>
- Scarcella, M. (2024, January 3). Google faces March 2025 trial in Texas’ antitrust lawsuit. *Reuters*.
<https://www.reuters.com/legal/transactional/google-faces-march-2025-trial-texas-antitrust-lawsuit-2024-01-03/>
- Schaal, D. (2024, August 23). Google Scores Court Victory in Case Alleging Anticompetitive Bias. *Skift*.
<https://skift.com/2023/08/04/google-scores-court-victory-in-case-alleging-anticompetitive-bias/>
- Schlumberger, O., Edel, M., Maati, A., & Saglam, K. (2023). How Authoritarianism Transforms: A Framework for the Study of Digital Dictatorship. *Government and Opposition*, 1–23.
<https://doi.org/10.1017/gov.2023.20>
- Schnauffer, T. A. (2017). Redefining Hybrid Warfare: Russia’s Non-linear War against the West. *Journal of Strategic Security*, 10(1), 17–31.
- Schneier, B. (2016). *Data and Goliath: The hidden battles to collect your data and control your world* (First published as a Norton paperback 2016). W.W. Norton & Company.

- Scott, L. (2023, April 19). Leaked Documents Show How Russia, China Collaborate on Censorship. *Voice of America*. <https://www.voanews.com/a/leaked-documents-show-how-russia-china-collaborate-on-censorship/7057913.html>
- Seddon, M. (2019, November 18). Yandex agrees restructuring with Kremlin. *Financial Times*. <https://www.ft.com/content/999e3ca6-09db-11ea-bb52-34c8d9dc6d84>
- Sharani, S. (2022). The Narratives of Syrian Refugees on Taking Turkey as a Land of a Long or Temporary Settlement. In *Refugees on the Move: Crisis and Response in Turkey and Europe* (pp. 281–311). UK Berghahn Books. <https://www.jstor.org/stable/j.ctv2vr8tsk>
- Shcherbakova, O., & Nikiforchuk, S. (2023). IDENTIFYING MISLEADING INFORMATION AND TYPES OF FAKES. *Scientific Journal of Polonia University*, 59(4), Article 4. <https://doi.org/10.23856/5915>
- Simonyan, R. H. (2022). The Russian-speaking Diaspora in the Baltic States: A socio-cultural aspect. *Baltic Region*, 14(2), 144–157. <https://doi.org/10.5922/2079-8555-2022-2-9>
- Smets, K. (2018). The way Syrian refugees in Turkey use media: Understanding “connected refugees” through a non-media-centric and local approach. *Communications: The European Journal of Communication Research*, 43(1), 113–123. <https://doi.org/doi.org/10.1515/commun-2017-0041>
- Soladov, O. (2020). The Interplay between National Security and Freedom of Expression Online in the Post-Soviet Countries. *Universita' Commerciale “Luigi Bocconi”*.
- Sombatpoonsiri, J., & Mahapatra, S. (2024). *Regulation or Repression? Government Influence on Political Content Moderation in India and Thailand* (Digital Democracy Network). Carnegie Endowment for International Peace. <https://carnegieendowment.org/research/2024/07/india-thailand-social-media-moderation>
- Splidsboel Hansen, F. (2017). *Russian hybrid warfare: A study of disinformation*.
- Spring, M. (2024, August 7). *The real story of the website accused of fuelling Southport riots*. BBC News. <https://www.bbc.com/news/articles/c5y38gjp4ygo>
- Staff, T. (2023, May 30). *Abbas signs decree criminalizing ‘Nakba’ denial*. Retrieved from The Times of Israel: <https://www.timesofisrael.com/abbas-signs-decree-criminalizing-nakba-denial/>
- Stahl, G., Keddie, A., & Adams, B. (2023). The manosphere goes to school: Problematizing incel surveillance through affective boyhood. *Educational Philosophy and Theory*, 55(3), 366–378. <https://doi.org/10.1080/00131857.2022.2097068>
- Stănescu, G. (2023). Informational war: Analyzing false news in the Israel conflict. *Social Sciences and Education Research Review*, 10(2), 301–310.
- Stanford Internet Observatory. (2022, August 24). Unheard Voice: Evaluating five years of pro-Western covert influence operations. <https://stacks.stanford.edu/file/druid:nj914nx9540/unheard-voice-tt.pdf>
- Stanley-Becker, I. (2020, September 15). Pro-Trump youth group enlists teens in secretive campaign likened to a ‘troll farm,’ prompting rebuke by Facebook and Twitter. *Washington Post*. https://www.washingtonpost.com/politics/turning-point-teens-disinformation-trump/2020/09/15/c84091ae-f20a-11ea-b796-2dd09962649c_story.html
- Stein, R. L. (2021). “Hoax!” Palestinian Cameras, Israeli State Violence, and the “Fake News” Fantasy. In D. Della Ratta, G. Lovink, T. Numerico, & P. Sarram (Eds.), *The Aesthetics and Politics of the Online Self* (pp. 115–128). Springer International Publishing. https://doi.org/10.1007/978-3-030-65497-9_9

- Stein, R. L. (2021). *Screen Shots: State Violence on Camera in Israel and Palestine*. Redwood, CA: Stanford University Press.
- Stray, J. (2019). Institutional Counter-disinformation Strategies in a Networked Democracy. Companion Proceedings of The 2019 World Wide Web Conference, 1020–1025. <https://doi.org/10.1145/3308560.3316740>
- Stryker, R., Conway, B. A., & Danielson, J. T. (2016). What is political incivility? *Communication Monographs*, 83(4), 535–556. <https://doi.org/10.1080/03637751.2016.1201207>
- Stubbs, J., & Bing, C. (2018, August 29). Exclusive: Iran-based political influence operation - bigger, persistent, global. *Reuters*. <https://www.reuters.com/article/world/exclusive-iran-based-political-influence-operation-bigger-persistent-global-idUSKCN1LD2R7/>
- Stuxnet. (2010). Council on Foreign Relations. <https://www.cfr.org/cyber-operations/stuxnet>
- Sun, W. (2006). Introduction: Transnationalism and a global diasporic Chinese media sphere. In *Media and the Chinese diaspora* (pp. 1–25). Routledge.
- Sun, W. (2019). Chinese-language digital/social media in Australia: Double-edged sword in Australia's public diplomacy agenda. *Media International Australia*, 173(1), 22–35. <https://doi.org/10.1177/1329878X19837664>
- Sun, W. (2021). Chinese diaspora and social media: Negotiating transnational space. In *Oxford Research Encyclopedia of Communication*. Oxford University Press. <https://oxfordre.com/communication/display/10.1093/acrefore/9780190228613.001.0001/acrefore-9780190228613-e-1146>
- Sun, W., & Yu, H. (2016). Digital/social media and the Chinese community in Australia. *Media Asia*, 43(3–4), 165–168. <https://doi.org/10.1080/01296612.2016.1277826>
- Sun, W., & Yu, H. (2022). *WeChat and the Chinese Diaspora*. Routledge.
- Sun, W., & Yu, H. (2023). *Digital transnationalism: Chinese-language media in Australia* (Vol. 21). Brill.
- Sun, W., Yue, A., Sinclair, J., & Gao, J. (2011). Diasporic Chinese media in Australia: A post-2008 overview. *Continuum*, 25(4), 515–527. <https://doi.org/10.1080/10304312.2011.576751>
- Sunata, U., & Yıldız, E. (2018). Representation of Syrian refugees in the Turkish media. *Journal of Applied Journalism & Media Studies*, 7(1), 129–151.
- Suslov, M. (2018). Geopolitization of the post-soviet diaspora in the baltic sea region. *Global Affairs*, 4(4–5), 521–535. <https://doi.org/10.1080/23340460.2018.1535255>
- Tan, X., & Tao, Y. (2024). COVID-19, Perceived Foreign Interference, and Anti-Chinese Sentiment: Evidence from Concurrent Survey Experiments in Australia and the United States. *Journal of Intercultural Studies*, 45(3), 433–451. <https://doi.org/10.1080/07256868.2024.2307956>
- Tenove, C. (2019). Networking justice: Digitally-enabled engagement in transitional justice by the Syrian diaspora. *Ethnic and Race Studies*, 42, 1950–1969. <https://doi.org/10.1080/01419870.2019.1569702>
- Tesler, M. (2012). The Return of Old-Fashioned Racism to White Americans' Partisan Preferences in the Early Obama Era. *The Journal of Politics*, 75(1), 110–123. <https://doi.org/10.1017/s0022381612000904>
- The Guardian. (2014, April 3). US secretly created 'Cuban Twitter' to stir unrest and undermine government. <https://www.theguardian.com/world/2014/apr/03/us-cuban-twitter-zunzuneo-stir-unrest>

- The Kremlin's Efforts to Covertly Spread Disinformation in Latin America. (2023, November 7). *United States Department of State*. <https://www.state.gov/the-kremlins-efforts-to-covertly-spread-disinformation-in-latin-america/>
- The Moscow Times. (2021, December 3). Gazprom Gains Control of Russia's Top Social Network. *The Moscow Times*. <https://www.themoscowtimes.com/2021/12/03/gazprom-gains-control-of-russias-top-social-network-a75724>
- The Moscow Times. (2023a, July 14). Russia Tightens Exit Rules for Foreign Businesses – Vedomosti. *The Moscow Times*. <https://www.themoscowtimes.com/2023/07/14/russia-tightens-exit-rules-for-foreign-businesses-vedomosti-a81842>
- The Moscow Times. (2023b, October 12). Netherlands Probes Yandex Taxi App Over Fears of FSB Data Sharing – Bloomberg. *The Moscow Times*. <https://www.themoscowtimes.com/2023/10/12/netherlands-probes-yandex-taxi-app-over-fears-of-fsb-data-sharing-bloomberg-a82751>
- The Mounting Damage of Flawed Elections and Armed Conflict. (2023). Freedom House. <https://freedomhouse.org/report/freedom-world/2024/mounting-damage-flawed-elections-and-armed-conflict>
- Thèmes. (2021, October 16). *RUNE – Genève*. <https://rune-geneve.ch/themes/>
- Thomas, J. (2024, June 15). Operation Overload: Pro-Russians flooding newsrooms with fake news. *Euronews*. <https://www.euronews.com/my-europe/2024/06/15/russia-deliberately-flooding-newsrooms-with-fake-content-to-overwhelm-fact-checkers-study->
- Thompson, P., & Bornat, J. (2017). *The voice of the past: Oral history* (Fourth edition). Oxford University Press.
- Timberg, C., & Romm, T. (2019, May 16). Facebook shuts down Israel-based disinformation campaigns as election manipulation increasingly goes global. *Washington Post*. <https://www.washingtonpost.com/technology/2019/05/16/facebook-shuts-down-israel-based-disinformation-campaigns-election-manipulation-increasingly-goes-global/>
- Tishkov, V. A. (2002). The diaspora as a historical phenomenon. *Anthropology & Archeology of Eurasia*, 41(1), 54–88.
- Tishkov, V. A. (2004). *Chechnya: Life in a war-torn society*. University of California Press.
- Todorova, T. (2013). Bearing Witness to al Nakba in a Time of Denial. In D. Matar, & Z. Harb (Eds.), *Narrating Conflict in the Middle East: Discourse, Image and Communications Practices in Lebanon and Palestine* (pp. 248-270). London: I. B. Tauris.
- Toepfl, F. (2020). Comparing Authoritarian Publics: The Benefits and Risks of Three Types of Publics for Autocrats. *Communication Theory*, 30(2), 105–125. <https://doi.org/10.1093/ct/qtz015>
- Tölölyan, K. (1991). The Nation-State and Its Others: In Lieu of a Preface. *Diaspora: A Journal of Transnational Studies*, 1(1), 3–7. <https://doi.org/10.1353/dsp.1991.0008>
- Tolz, V. (2017). From a threatening “Muslim migrant” back to the conspiring “West:” race, religion, and nationhood on Russian television during Putin’s third presidency. *Nationalities Papers*, 45(5), 742–757. <https://doi.org/10.1080/00905992.2017.1282449>
- Tolz, V., & Harding, S. (2015). From “Compatriots” to “Aliens”: The Changing Coverage of Migration on Russian Television. *The Russian Review*, 74(3), 452–477. <https://doi.org/10.1111/russ.12025>
- Topak, Ö. E., Mekouar, M., & Cavatorta, F. (2022). An Assemblage of New Authoritarian Practices in Turkey. In *New Authoritarian Practices in the Middle East and North Africa*. Edinburgh University Press.

- Topak, O., Mekouar, M., & Cavatorta, F. (Eds.). (2022a). *New Authoritarian Practices in the Middle East and North Africa*. Edinburgh University Press. <https://www.cambridge.org/core/books/new-authoritarian-practices-in-the-middle-east-and-north-africa/54F9C3EC181DCBAC695FDE9AFA3DDEB0>
- Treasury Sanctions Iranian Entities for Attempted Election Interference. (2024, August 7). U.S. Department of the Treasury. <https://home.treasury.gov/news/press-releases/sm1158>
- Trilling, D. (2011). Propagandastan. *Foreign Policy*. <https://foreignpolicy.com/2011/11/22/propagandastan/>
- Tumber, H., & Waisbord, S. (Eds.). (2021). *The Routledge Companion to Media Disinformation and Populism* (1st ed.). Routledge. <https://doi.org/10.4324/9781003004431>
- Turkey blocks Instagram amid ‘censorship’ row. (2024, August 2). *Al Jazeera*. <https://www.aljazeera.com/news/2024/8/2/turkey-blocks-instagram-after-censorship-row>
- Turkey restores access to Instagram after 9-day block. (2024, August 10). *Reuters*. <https://www.reuters.com/technology/turkey-restore-access-instagram-minister-says-2024-08-10/>
- Twitter Moderation Research Consortium—X Transparency Center. (n.d.). Retrieved 15 August 2024, from <https://transparency.x.com/en/reports/moderation-research.html>
- Uehling, G. (2018). *Beyond memory: The Crimean Tatars’ deportation and return*. Springer.
- UNESCO. (2023, April 20). *Defamation laws and SLAPPs increasingly “misused” to curtail freedom of expression*. Retrieved from UNESCO: <https://www.unesco.org/en/articles/defamation-laws-and-slapps-increasingly-misused-curtail-freedom-expression>
- United Nations. (2023, October 6). *Widening Digital Gap between Developed, Developing States Threatening to Exclude World’s Poorest from Next Industrial Revolution, Speakers Tell Second Committee | Meetings Coverage and Press Releases [Government Website]*. UN. <https://press.un.org/en/2023/gaef3587.doc.htm>
- United Nations. (2024). *The Sustainable Development Goals Report*. United Nations. <https://unstats.un.org/sdgs/report/2024/The-Sustainable-Development-Goals-Report-2024.pdf>
- United States Central Command. (2023, January 11). *Freedom of Information Act Request: Operation Earnest Voice*. <https://documents2.theblackvault.com/documents/centcom/23-0046.pdf>
- United States Senate Committee on Environment and Public Works (Minority). (2014). *The Chain of Environmental Command: How a Club of Billionaires and Their Foundations Control the Environmental Movement and Obama’s EPA*. United States Senate. <https://archive.org/details/FINALREPORT73014>
- Valeriano, B., & Maness, R. C. (2015). *Cyber War Versus Cyber Realities: Cyber Conflict in the International System*. Oxford University Press.
- Vehkoo, J. (2013). *Crowdsourcing in Investigative Journalism* (10.60625/risj-3gv7-h363; pp. 1–34). Reuters Institute, University of Oxford. <https://ora.ox.ac.uk/objects/uuid:727c20b5-8112-4a87-9816-7fbc0ad71e1a/files/ma2f84e27b2dc92700a92e4af18b7eb02>
- Vejledning Til Tek Tjek. (2023, November). FutureClassroom Lab. <https://futureclassroomlab.dk/wp-content/uploads/2023/11/TEKTJEK-1.2.pdf>
- Voigt-Graf, C. (2005). The construction of transnational spaces by Indian migrants in Australia. *Journal of Ethnic and Migration Studies*, 31(2), 365–384. <https://doi.org/10.1080/1369183042000339972>

- Waller, J. G. (2024). Distinctions With a Difference: Illiberalism and Authoritarianism in Scholarly Study. *Political Studies Review*, 22(2), 365–386. <https://doi.org/10.1177/14789299231159253>
- Waller, J. M. (2016). Putin propaganda picks up ex-Pentagon contractors. American Media Institute Newswire. Retrieved from: <https://web.archive.org/web/20160317024555/http://aminewswire.com/stories/510662541-putin-propaganda-picks-up-ex-pentagon-contractors>
- Ward, M., & Gerstein, J. (2022, March 14). U.S. charges Russian oligarch with making illegal political donations. *POLITICO*. <https://www.politico.com/news/2022/03/14/russian-oligarch-charged-illegal-political-donations-00017090>
- Wardle, C. (2018). The Need for Smarter Definitions and Practical, Timely Empirical Research on Information Disorder. *Digital Journalism*, 6(8), 951–963. <https://doi.org/10.1080/21670811.2018.1502047>
- Wardle, C., & Derakhshan, H. (2017). *Information disorder: Toward an interdisciplinary framework for research and policy making*. Council of Europe Publishing. <https://edoc.coe.int/en/media/7495-information-disorder-toward-an-interdisciplinary-framework-for-research-and-policy-making.html>
- Weber, V. (2019). *The worldwide web of Chinese and Russian information controls*. Center for technology and global affairs, University of Oxford.
- Wernick, A. (1991). *Promotional culture: Advertising, ideology, and symbolic expression*. Sage Publications.
- Wescott, S., Roberts, S., & Zhao, X. (2024). The problem of anti-feminist ‘manfluencer’ Andrew Tate in Australian schools: Women teachers’ experiences of resurgent male supremacy. *Gender and Education*, 36(2), 167–182. <https://doi.org/10.1080/09540253.2023.2292622>
- Wessels, J. (2023). The webinar as a toll for diasporic political communication to counter mis/disinformation about Syria. In *Middle Eastern Diasporas and Political Communication* (pp. 67–85). <https://www.taylorfrancis.com/chapters/edit/10.4324/9781003365419-5/webinar-tool-diasporic-political-communication-counter-mis-disinformation-syria-josepha-wessels>
- Whittaker, J., Costello, W., & Thomas, A. G. (2024). *Predicting Harm Among Incels (Involuntary Celibates): The Roles of Mental Health, Ideological Belief and Social Networking* (Rethinking Extremism). Commission for Countering Extremism, U.K. Government. <https://www.gov.uk/government/publications/predicting-harm-among-incels-involuntary-celibates>
- Wihbey, J. P. (2021). Explanatory Journalism—Bringing Greater Interpretation and Depth to Complex Issues. In *Reporting Beyond the Problem: From Civic Journalism to Solutions Journalism* (pp. 63–81). chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://camd.northeastern.edu/wp-content/uploads/2023/04/Chapter-5-Explanatory-Journalism_Wihbey_Reporting-Beyond-the-Problem_McIntyre_Hopkinson-2021.pdf
- Wihbey, J. P. (2021). Explanatory Journalism—Bringing Greater Interpretation and Depth to Complex Issues. In *Reporting Beyond the Problem: From Civic Journalism to Solutions Journalism* (pp. 63–81). chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://camd.northeastern.edu/wp-content/uploads/2023/04/Chapter-5-Explanatory-Journalism_Wihbey_Reporting-Beyond-the-Problem_McIntyre_Hopkinson-2021.pdf
- Wilson, M. J., Fisher, K., & Seidler, Z. (2024). The Anti-social Network: The Role of the Social Media Manosphere in Young Men’s Lives. In Z. Seidler (Ed.), *Masculinities and Mental Health in Young Men: From Echo Chambers to Evidence* (pp. 187–228). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-64053-7_6
- Wimmer, A., & Glick Schiller, N. (2002). Methodological nationalism and beyond: Nation–state building, migration and the social sciences. *Global Networks*, 2(4), 301–334. <https://doi.org/10.1111/1471-0374.00043>

- Wójcik, A. (2023). Memory Laws, Rule of Law, and Democratic Backsliding: The Case of Poland. *The Journal of Illiberalism Studies*, 3(3), 71-87. Retrieved from <https://www.illiberalism.org/memory-laws-rule-of-law-and-democratic-backsliding/>
- Woolley, S. C., & Howard, P. N. (2018). *OII | Computational Propaganda: Political Parties, Politicians, and Political Manipulation on Social Media*. <https://www.oii.ox.ac.uk/research/publications/computational-propaganda-political-parties-politicians-and-political-manipulation-on-social-media-2>
- World Migration Report 2024 Reveals Latest Global Trends and Challenges in Human Mobility. (2024, May 8). IOM UN Migration. <https://www.iom.int/news/world-migration-report-2024-reveals-latest-global-trends-and-challenges-human-mobility>
- Wyden, R. Sen., Lee, M. Sen., Davidson, W. Rep., & Lofgren, Z. Rep. (n.d.). *Government Surveillance Reform Act*. U.S. Senate. https://www.wyden.senate.gov/imo/media/doc/government_surveillance_reform_act_one_page_summary.pdf
- Xia, Y., Huan, C., & García Marrugo, A. (2024). Fair or biased? A corpus-based study of Australia's early COVID-19 media representation of China. *Social Semiotics*, 1–20. <https://doi.org/10.1080/10350330.2024.2341394>
- Xu, X. (2021). To Repress or to Co-opt? Authoritarian Control in the Age of Digital Surveillance. *American Journal of Political Science*, 65(2), 309–325. <https://doi.org/10.1111/ajps.12514>
- Yang, F. (2023). From ethnic media to ethno-transnational media. In Wechat and the Chinese diaspora: Digital transnationalism in the era of China's rise. Routledge. <https://www-taylorfrancis-com.manchester.idm.oclc.org/books/edit/10.4324/9781003154754/wechat-chinese-diaspora-wanning-sun-haiqing-yu>
- Yu, H., & Li, L. (2022). Chinese digital platforms in Australia: From market and politics to governance. *Media International Australia*. Media International Australia, 185(1), 93–109. <https://doi.org/10.1177/1329878X221095594>
- Yücel, A. (2021). Symbolic annihilation of Syrian refugees by Turkish news media during the COVID-19 pandemic. *International Journal for Equity in Health*, 20(137), 1–11. <https://doi.org/10.1186/s12939-021-01472-9>
- Zannettou, S., Caulfield, T., Setzer, W., Sirivianos, M., Stringhini, G., & Blackburn, J. (2019). *Who Let The Trolls Out? Towards Understanding State-Sponsored Trolls* (arXiv:1811.03130). arXiv. <https://doi.org/10.48550/arXiv.1811.03130>
- Zeno, B. (2017). Dignity and Humiliation: Identity Formation among Syrian Refugees. *Middle East Law and Governance*, 9(3), 282–297. <https://doi.org/10.1163/18763375-00903006>
- Zhao, H. (2000). Jin yi er shi nian lai zhongguo dalu xinyimin ruogan wenti de sikao' (On the new migrants from mainland China over the past two decades). *Huaqiao Huaren Lishi Yanjiu* (Overseas Chinese History Research), 4.
- Ziemer, U. (Ed.). (2013). *East European diasporas, migration, and cosmopolitanism*. Routledge.
- Zuboff, S. (2019). *The Age of Surveillance Capitalism*. Public Affairs.
- Zuckerberg, M. (2024, August 26). *Letter from Mark Zuckerberg to The Honorable Jim Jordan*. <https://x.com/JudiciaryGOP/status/1828201780544504064/photo/1>
- Госдума: 'взбесившийся принтер' или Россия в миниатюре? (2013, February 28). BBC News Русская служба. https://www.bbc.com/russian/russia/2013/03/130303_duma_crazy_printer
- Джордж Оруэлл возглавил рейтинг самых воруемых книг из «Читай-города». (2023, December 26). РБК. <https://www.rbc.ru/rbcfreenews/658abc319a79474a994e150f>

Перечень поручений по итогам заседания Совета по развитию гражданского общества и правам человека (утв. Президентом РФ 12.01.2023 N Пр-19) | ГАРАНТ. (2023, January 12). Гарант. <https://base.garant.ru/406148205/>

Письмо Министерства просвещения РФ от 7 августа 2023 г. N АБ-3318/03 'Об использовании единых учебников истории для 10-11 классов' | Документы ленты ПРАЙМ: ГАРАНТ.РУ. (2023, August 7). <https://www.garant.ru/products/ipo/prime/doc/407421349/>

Разрушение традиционных ценностей и феминитивы. «Свободные новости» публикуют полный текст решения Верховного суда РФ о признании экстремистским «движения ЛГБТ»*. (2024, January 18). <https://fn-volga.ru/news/view/id/219533>

Роман-антиутопия «1984» стал одной из самых продаваемых электронных книг в России. (2022, December 13). Главные новости в России и мире - RTVI. <https://rtvi.com/news/roman-antiutopiya-1984-stal-odnoj-iz-samyh-prodavaemyh-elektronnyh-knig-v-rossii/>

Спикер Госдумы прокомментировал выражение «взбесившийся принтер». (2015, June 1). РБК. <https://www.rbc.ru/politics/01/06/2015/556bfe3b9a794709cfa41942>

Указ Мэра Москвы от 05.03.2020 N 12-УМ (ред. От 15.03.2023) 'О введении режима повышенной готовности'. (2020, March 5). КонсультантПлюс. <https://www.consultant.ru/cons/cgi/online.cgi?from=201990-0&req=doc&rnd=1NxxXw&base=MLAW&n=230843#G413ALUWEfuTpVtr1>

Указ Президента России от 08 мая 2024 г. №314 'Об утверждении Основ государственной политики Российской Федерации в области исторического просвещения' | Документы ленты ПРАЙМ: ГАРАНТ.РУ. (2024, May 8). Гарант. <https://www.garant.ru/products/ipo/prime/doc/408897564/>
