



D6.1 Working Paper

Comparing Transnational

Information Suppression

A Comparison of Information Suppression Tactics across China, Russia, Ethiopia, and Rwanda

Version 2 – 7 September 2026

Project Acronym: ARM
Project Full Title: ARM: The Long Arm of Authoritarian States
Call: HORIZON-CL2-2023-DEMOCRACY-01
Topic: Horizon-CL2-2023-DEMOCRACY-01-02
Type of Action: Horizon-RIA
Grant Number: 101132437
Project URL: <https://cordis.europa.eu/project/id/101132437>

DELIVERABLE 6.1	WORKING PAPER SYNTHESIS
Related Work Package	WP6
Deliverable Lead	UiT
Author(s)	Lisa Garbe Gunhild Hoogensen Gjørsv Amanuel Kebede Pauline Lemaire Simon Turner Mariëlle Wijermars Yue Xie
Contact	media@arm-project.eu
Start date / Project Duration	1 Jan 2024 – 38 months
Type of Deliverable (R, DEM, DEC, Other)	R
Dissemination Level (PU, CO, CI)	PU
Date of Last Update	7 September 2026



Table of Contents

1.	Introduction	1
1.1	Mechanisms of Information Suppression	2
2.	A Typology for Comparing Information Suppression	3
2.1	The three stages of information suppression	3
2.2	The Actor Dimension	4
2.3	The Target Dimension	5
2.4	Mechanisms of Information Suppression	5
3.	Methodology	7
4.	Comparing China, Russia, Rwanda, and Ethiopia.....	7
4.1	Transnational Information Control	8
4.2	Transnational Repression.....	12
5.	Tactics of Information Suppression	16
5.1	Production-stage tactics	17
5.2	Dissemination-stage tactics.....	25
5.3	Salience-stage Tactics	28
6.	Comparison.....	33
6.1	Bottleneck vs Relationship-specific Control	33
6.2	Preventive versus Reactive Infrastructure	34
6.3	Great powers vs regional powers	34
7.	Key takeaways	35
8.	References	37



List of Figures

Figure 1. Digital Information Control Over Time 8

Figure 2. Digital Information Control in 2024 9

Figure 3. Coordinated Influence Operations Campaigns on YouTube 11

Figure 4. Incidents of transnational repression over time 13

Figure 5. Incidents of transnational repression by category 14



List of Tables

Table 1. Production-stage tactics.....	17
Table 2. Dissemination-stage tactics	25
Table 3. Salience-stage tactics	28



1. Introduction

Authoritarian governments increasingly seek to suppress information beyond their borders: they co-opt citizens living abroad, repress activists and exiles overseas, finance large-scale image campaigns aimed at foreign publics, and deploy covert networks to influence foreign debates. These practices vary not only in the types of tactics employed, but also in their strategic goals, target audiences, timing, and degree of coercion. For instance, prior research shows both how authoritarian governments use transnational forms of repression targeting diasporas and exiled populations¹ as well as transnational forms of persuasion, such as public diplomacy or online influence campaigns to shape international perceptions and legitimise their rule abroad through softer forms of influence.² There is substantial variation across authoritarian regimes in which tactics they use, when (context and conditions), who implements them, and who they target.

Some of this variation reflects differences in what a regime is trying to achieve at a given time: a regime primarily concerned with pre-empting diaspora mobilisation against it at home pursues a different strategy than one primarily concerned with shaping how its foreign policy is received internationally or protecting an overseas investment relationship. But strategy is not always chosen freely. It is also shaped by what a regime is capable of doing: coercing a specific critic abroad requires a hold over that individual, such as consular reach or a family still resident in the country of origin, while shaping what information a foreign or diaspora audience encounters requires mostly resources but no relationship with any particular person at all. Regimes with weaker diplomatic, legal, or economic reach beyond their borders are accordingly not necessarily less active, but differently active, relying more heavily on relationship-based tactics that do not require major financial or human resources. Strategic objectives and capacity are not directly observable in the way a lawsuit or a visa denial is, and this working paper treats them as an interpretive lens for making sense of the tactics it documents, rather than as independently measured variables.

This working paper provides an overview of the different forms of transnational **information suppression** tactics employed by China, Russia, Ethiopia, and Rwanda and compares the

¹ Glasius, 'Extraterritorial Authoritarian Practices'; Koinova and Tsourapas, 'How Do Countries of Origin Engage Migrants and Diasporas?'; Michaelsen, 'Exit and Voice in a Digital Age'; Moss, 'Transnational Repression, Diaspora Mobilization, and the Case of The Arab Spring'; Tsourapas, 'Global Autocracies'.

² Demir and Richter, 'Public Diplomacy of Authoritarian Regimes'; Nye, 'Soft Power and Public Diplomacy Revisited'.

types of tactics used by each regime as well their underlying strategic rationale. Specifically, this working paper seeks to answer the following questions:

- What are key differences between the four cases in their information suppression tactics?
- To what extent do smaller countries like Ethiopia and Rwanda follow the tactics by bigger regimes like China and Russia?
- What are limitations in existing data sources capturing information suppression?

The working paper proceeds as follows: Section 1.1 introduces the concept of information suppression. Section 2 develops a typology of information suppression organised around three dimensions: the stage of the information cycle at which suppression occurs (production, dissemination, or salience), the actor who carries it out (state bodies, commercial intermediaries, or private individuals), and the target it is aimed at (information producers, outlets, or audiences). Section 2.4 sets out the mechanisms through which regimes exercise leverage over these actors and targets—coercion, co-optation, and persuasion. Section 3 sets out our mixed-methods approach, combining interviews with journalists, researchers, and diaspora activists, desk research on each regime's transnational activities, and social media analysis of coordinated amplification. The report then proceeds in three steps: it first situates the four cases against existing quantitative indicators of transnational information control and repression (Section 4), before turning to the typology to present illustrative tactics for each stage of the information cycle, drawn from the four cases (Section 5), and closing with a cross-regime comparison of the actors, targets, and stages each regime relies on most (Section 6).

1.1 Mechanisms of Information Suppression

This paper compares the four cases through the concept of information suppression. We define information suppression as “a set of actions to silence information with the purpose of muting dissenting voices or narratives outside a country's borders. It is transnational, highlighting the link between domestic and global tactics of information suppression, with various social groups acting as both agents and targets. Information suppression can also be the result of illiberal practices, targeting the autonomy and dignity of individuals”.^{3,4} These

³ Aalen, Lemaire & De Seta (2026) Information Suppression: Does it belong to FIMI?. ARM Working Paper D1.2.

⁴ While information suppression is inherently transnational, for clarity, many policy actors use the expression “transnational information suppression”. EEAS, *4th Report on Foreign Information Manipulation and Interference Dismantling the FIMI House of Cards*, 4.

actions are intentional. Intentional does not mean they are carried out by one central actor, such as a central authority or government. Regime policy can create conditions in which non-state actors such as firms, digital platforms, diaspora associations and private individuals suppress information on their own initiative. Much of what we describe below works in this manner. Regimes facilitate these activities through at least three distinct mechanisms, each drawing on a different kind of leverage, typically exercised by a different type of actor, and directed at a different target: coercion, co-optation, and persuasion. The typology in Section 2 sets out the stages, actors, and targets through which these mechanisms operate; Section 3 returns to the three mechanisms themselves in fuller detail.

2. A Typology for Comparing Information Suppression

The typology developed in this section classifies *tactics* of information suppression. The purpose is not to assign labels to regimes, but rather to identify and describe the different elements and different stages that play a role in information suppression.

2.1 The three stages of information suppression

Information suppression tactics can be applied at three distinct points in the life of a piece of information:

Production is the stage at which information is first created. At this stage, suppression prevents a critical narrative from being written, researched, or spoken in the first place.

Dissemination is the stage at which information moves from its source or the production stage to a channel capable of disseminating the piece of information and reaching an audience—such as a newspaper, a broadcaster, a platform. Suppression no longer prevents information from existing but prevents it from circulating.

Salience is the stage at which information competes for a target audience's attention. Suppression does not stop information from existing or circulating; rather, it buries it beneath competing material, making it less visible and less likely to be noticed

These stages are defined by function, not by medium or legality: the same act—a lawsuit, a funding offer, a flood of alternative content—can serve a production, dissemination, or salience function depending on where in the cycle it intervenes and to whom it is aimed.

The three stages of information suppression are not independent options a regime chooses freely; they are points along a single chain, and pressure applied early in that chain has

consequences downstream that later applied pressure does not. If someone is silenced at the level of information production, there is nothing left to disseminate and nothing left to compete for attention. Information suppression at this stage is the most complete, but it also requires the deepest leverage over a specific individual. Where that leverage is unavailable, because the information producer is out of reach, uncooperative, or too costly to pursue directly, a regime can fall back on a later stage: it cannot stop the report from being written, but it can pressure the outlet that would carry it, or, failing that, flood the audience's attention so the report is written and published but never read. A regime may also reach for a later stage as a first choice rather than a fallback: out-competing a critical narrative at the salience stage can serve purposes, such as enhancing the regime's own legitimacy, that suppression at the production stage cannot. The three stages therefore function partly as substitutes for one another, and which substitute a regime reaches for is informative about the leverage it holds and the goals it is pursuing.

2.2 The Actor Dimension

Because suppression is not dependent upon a direct order from central or state authorities (Section 1.1), the typology tracks the *who* behind the tactic, distinguishing three types of actors by the kind of leverage they bring to bear.

State bodies, such as ministries, embassies, intelligence services, state prosecutors, apply suppression through coercive, persuasive, or co-optive capacity, by exercising legal or diplomatic power, physical reach, or the ability to threaten family members still resident in the country of origin.

Commercial intermediaries, such as publishers, platforms, advertisers, telecom operators, apply suppression through economic leverage by withholding access, funding, or a business relationship that the target would rather not lose.

Private individuals, such as community leaders, diaspora associations, informal networks, and individuals, apply suppression through normative and social capacity, sharing expectations about what should not be discussed, enforced through reputation and community standing rather than through law or contract.

Distinguishing these three types of actors matters because they are not interchangeable: a state can be sanctioned or called out diplomatically, a commercial intermediary can be regulated, but a norm enforced by private individuals is largely invisible to both instruments, which is precisely why regimes that lack strong state or commercial leverage abroad may come to rely on individuals as primary actors in suppression tactics.

2.3 The Target Dimension

Because suppression can be applied at different points along the chain that connects an information producer to a recipient, the typology also specifies who is targeted by a given tactic.

Information producers, such as academics, reporters, activists, are the individuals who would otherwise produce or carry a critical narrative; targeting them intervenes as far upstream as possible.

Outlets, such as media organisations, publishers, platforms, are not only actors of information suppression but also potential targets. They are the channels through which a producer's material would reach an audience; targeting them intervenes in the middle of the chain, where a single point of leverage can affect everything that passes through it.

Audiences, specifically diaspora communities and host-country publics, are the intended recipients of information; targeting them intervenes at the point of consumption, without needing to reach the producer or the outlet at all.

This dimension matters because it identifies where in the communication chain a regime's leverage actually lies, independent of which stage of the information cycle a tactic operates in.

2.4 Mechanisms of Information Suppression

Information suppression operates primarily through three mechanisms: coercion, co-optation, and persuasion as described in the authoritarianism literature.⁵

Coercion, exercised primarily by state bodies, makes voicing alternative opinions and dissent costly (though not impossible) in principle but unattractive in practice. A report can be kept out of circulation by threatening the information producer's relatives at home, or by exposing a source to legal risk in a jurisdiction the regime controls. Coercion requires power over the producer of the targeted information, which can include preventing the issuing of a passport or threatening their family still resident in the country of origin. The transnational repression literature has documented this type of leverage in detail, from surveillance and

⁵ Gerschewski, 'The Three Pillars of Stability'.

intimidation of exiled dissidents⁶ to the use of consular and legal instruments against critics abroad.⁷

Co-optation works by binding the information producer to the regime through a resource the producer values. Rather than raising the cost of defection through punishment, co-optation raises the cost of defection by creating dependence through funding, access, or standing. In the transnational setting, a researcher may be offered continued fieldwork access or grant funding, or a media outlet may depend on an advertising or content-sharing arrangement it would rather not jeopardize, so that the material in question is never produced or never carried because someone was accommodated. This form of leverage over the producer rather than the message has been documented in the media-capture literature on how authoritarian and illiberal actors acquire influence over independent outlets through ownership, advertising, and access.⁸

Persuasion, our third mechanism, targets the audience rather than the producer, through image campaigns, ready-made material offered to outlets, and coordinated online amplification.⁹ A piece of information can be buried simply by ensuring that whoever searches for it finds an abundance of other material first, a dynamic close to what Roberts describes as flooding.¹⁰ We treat such audience-directed material as suppression when its function is to bury competing information rather than to build genuine belief in an alternative (see Section 2). The audience-directed suppression we describe here shares its target and its instruments with legitimization efforts as described by Gerschewski, but is functionally closer to co-optation and coercion in that its purpose is to displace or silence competing information, not to build belief.

Which mechanism a regime relies on, and which actor carries it out, is not only a matter of preference but of what leverage is available. Coercion requires a hold over an identifiable information producer. Co-optation requires a resource, such as funding, access, or a commercial relationship, the producer or outlet would rather not put at risk. Persuasion requires resources but no hold over, or relationship with, any specific producer or outlet at all. A regime with weak coercive and institutional reach abroad can still act through this third route via private individuals or commercial intermediaries.

⁶ Michaelsen, 'Exit and Voice in a Digital Age'; Moss, 'Transnational Repression, Diaspora Mobilization, and the Case of The Arab Spring'.

⁷ Dukalskis et al., 'The Long Arm and the Iron Fist'; Tsourapas, 'Global Autocracies'.

⁸ Guriev and Treisman, 'Informational Autocrats'.

⁹ Elshehawy et al., 'Illiberal Communication and Election Intervention during the Refugee Crisis in Germany'; Mattingly and Yao, 'How Soft Propaganda Persuades'.

¹⁰ Censored.

3. Methodology

This paper draws on a mixed-methods case comparison of information suppression tactics used by China, Russia, Ethiopia, and Rwanda. Evidence is assembled from three sources: qualitative interviews with journalists, researchers, and diaspora activists who have direct experience of suppression tactics; desk research drawing on NGO and investigative reporting, and existing academic literature on each regime's transnational activities; and social media analysis tracing patterns of coordinated amplification and content flooding relevant to the salience stage. Triangulating across these sources is particularly important given the limitations of more quantifiable indicators, discussed below. Much of what suppression does leaves no public trace by design, so no single source is sufficient on its own, and interview material is often the only way to recover tactics—a permit quietly refused, a relative contacted at home—that desk research alone would miss.

The report proceeds in three steps. It first situates the four cases against existing quantitative indicators of transnational information control—V-Dem's Digital Society Project and Google's Threat Analysis Group data on the salience dimension, and Freedom House's Transnational Repression Database on the production dimension (Section 4). This step establishes the aggregate scale and broad cross-country pattern of suppression activity before turning to more fine-grained tactic-level evidence, and it also makes concrete what these existing indicators can and cannot capture. The report then works through the typology developed in Section 2, presenting, for each stage of the information cycle, production, dissemination, and salience, illustrative examples of tactics drawn from the four country cases (Section 5). This stage-by-stage presentation is organised around tactics rather than countries, in keeping with the typology's premise that it classifies tactics, not regimes, and that any given case may appear at more than one stage; a short synthesis of which actors and targets predominate is included at the end of each stage-specific subsection. Finally, the report turns to an explicit cross-regime comparison, examining how the four regimes differ in the relative weight they place on different actors, different targets, and different stages of the information cycle overall, and asking what these differences reveal about the leverage each regime does and does not have.

4. Comparing China, Russia, Rwanda, and Ethiopia

To assess levels of information suppression across China, Russia, Rwanda, and Ethiopia, this section draws on three existing data sources, each capturing a different aspect of the phenomenon. Section 4.1 covers expert-coded data from the Varieties of Democracy (V-

Dem) project on digital information control¹¹ and YouTube's Threat Analysis Group (TAG) data on coordinated influence operations. Section 4.2 covers Freedom House's Transnational Repression Database. Together, these sources provide complementary but partial views of information suppression: V-Dem and TAG speak primarily to the suppression of information salience (flooding, platform-level takedowns), while Freedom House's incident data speaks primarily to suppression of information production (silencing individuals before they can produce or circulate information at all). Section 4.3 discusses the limitation of these data sources.

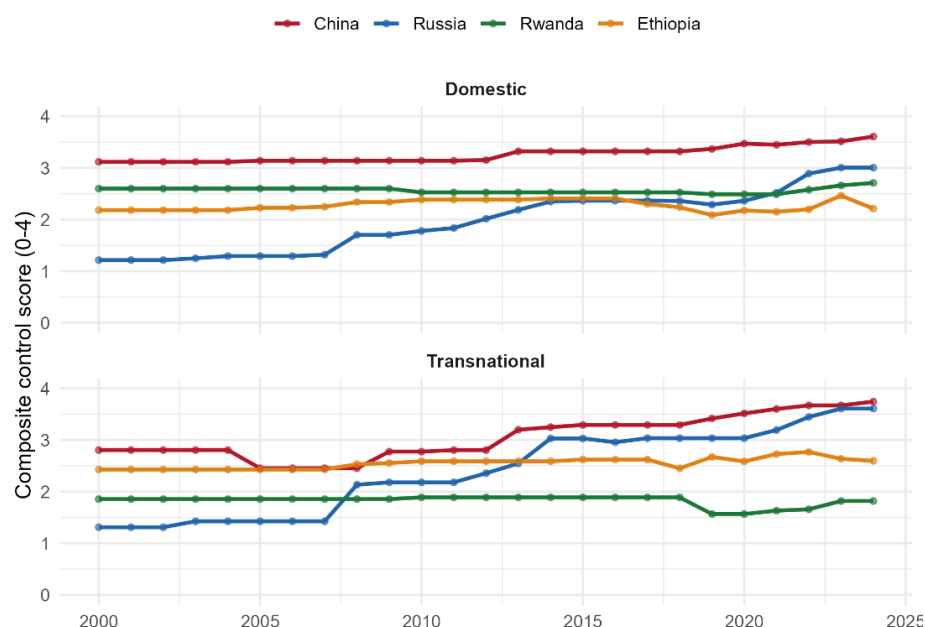
4.1 Transnational Information Control

The Varieties of Democracy (V-Dem) project's Digital Society Project (DSP) offers one of the few cross-nationally comparable measures that extends into the transnational sphere.¹² Drawing on assessments from multiple country experts per country-year, V-Dem/DSP codes both governments' and parties' use of social media to disseminate misleading information targeting foreign audiences, alongside domestic technical (including surveillance, content censorship) and legal (including regulatory scope, defamation-law abuse) control indicators.

Figure 1. Digital Information Control Over Time

¹¹ Mechkova et al., *Measuring Internet Politics*.

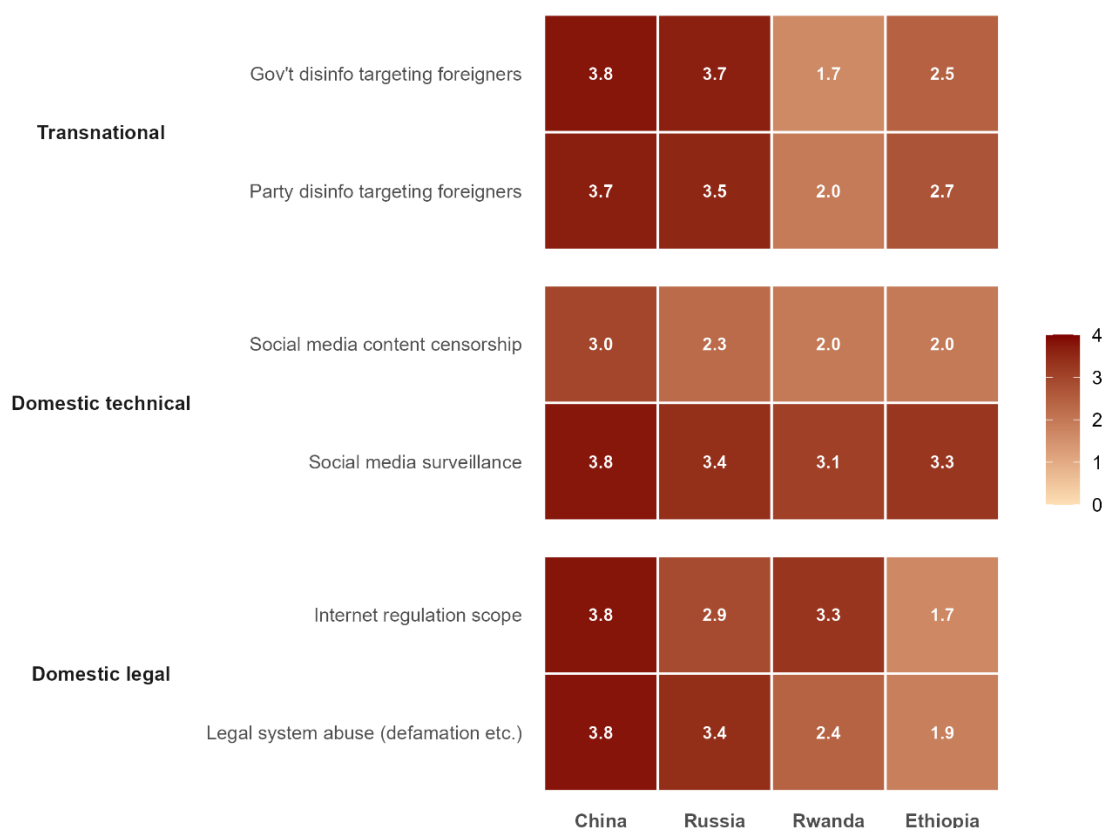
¹² Note that V-Dem is based on expert assessments which, despite rigorous reliability tests and measurement models, is subject to subjective judgements Coppedge et al., 'V-Dem Comparisons and Contrasts with Other Measurement Projects'.



Note. Digital information control over time, by country and category, 2000–2024. Domestic control is an unweighted average of four indicators (social media surveillance, social media content censorship, internet regulation scope, and legal system abuse); Transnational control is an unweighted average of two indicators (government and party disinformation targeting foreign audiences). Scores are reverse-coded from V-Dem/DSP's original `_osp` variables so that 0 = no control and 4 = maximum control. Source: V-Dem Digital Society Project.

Figure 1 shows that composite control scores have generally increased for China and Russia across both the domestic and transnational dimensions since 2000, with Russia's rise particularly sharp on the transnational dimension climbing from roughly 1.3 in the early 2000s to above 3.5 by 2024, converging with China's already-high level. Rwanda and Ethiopia, by contrast, show comparatively stable trajectories: both rank at a medium-to-high level on domestic control throughout the period, but display no meaningful increase in either domestic or transnational control since 2000.

Figure 2. Digital Information Control in 2024



Note. Digital information control by country and indicator, 2024. Cell values show the reverse-coded score for each indicator (0 = no control, 4 = maximum control), grouped into transnational, domestic technical, and domestic legal control. Source: V-Dem Digital Society Project.

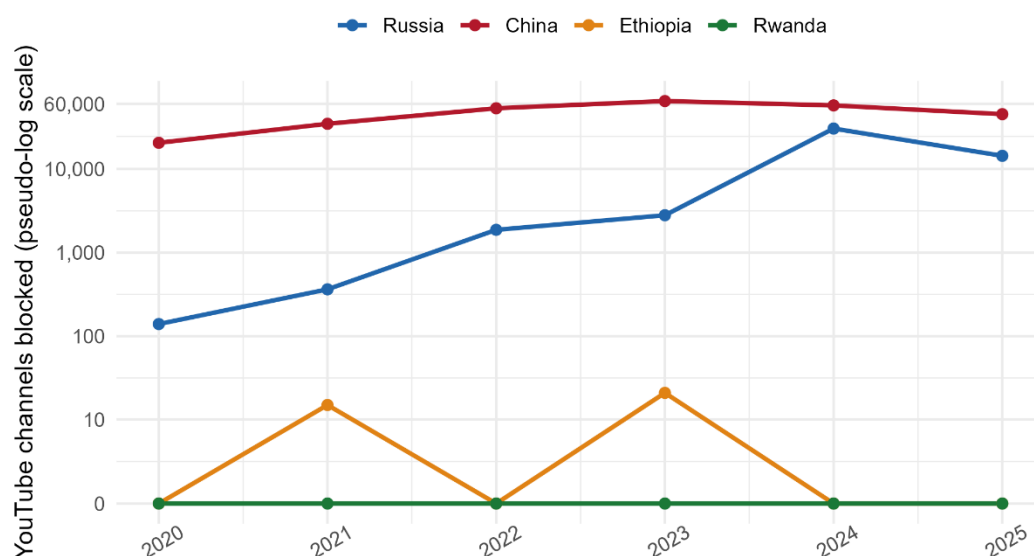
Figure 2 provides a disaggregated snapshot for 2024. On domestic control, V-Dem data suggest that all four countries are active along both the technical and legal dimensions. While China scores highest on nearly every domestic indicator, Russia, Rwanda, and Ethiopia are far from inactive: Rwanda, for instance, scores higher than Russia on the scope of internet-content regulation (3.3 vs. 2.9). Where the four countries diverge sharply is on the transnational dimension: China and Russia score consistently high on both government- and party-disseminated disinformation targeting foreign audiences (3.5–3.8), while Rwanda and Ethiopia score markedly lower (1.7–2.7). It is worth noting that V-Dem's transnational indicators capture only what we term suppression of information salience targeting foreign publics (e.g., flooding foreign information environments with misleading content); they do not capture other transnational tactics, such as targeted repression of exiled critics or legal harassment (see Section 4.2) abroad, meaning the "transnational control" measured here is considerably narrower than the concept as we use it elsewhere in this paper.

This pattern is underlined by data from Google. Google's Threat Analysis Group (TAG) publishes quarterly bulletins reporting the number of YouTube channels removed for coordinated influence operations, with suspected country of origin. As Figure 3 shows, TAG identified large and rising numbers of Russia- and China-linked channels between 2020 and 2025. Russia's count exceeded 30,000 in 2024, driven substantially by a single recurring network Google attributes to a Russian consulting firm; in July 2024 alone, TAG reported terminating 7,319 YouTube channels linked to this network, supportive of Russia and critical of Ukraine and the West.¹³ Ethiopia-linked takedowns, by contrast, were sporadic and small (never exceeding roughly 20 channels annually)—for example, in its Q4 2023 bulletin, TAG reported removing 21 channels linked to Ethiopia covering domestic Ethiopian political topics, alongside eight AdSense accounts disabled for the same activity.¹⁴ Rwanda-linked takedowns were entirely absent throughout the observation period.

Figure 3. Coordinated Influence Operations Campaigns on YouTube

¹³ <https://blog.google/threat-analysis-group/tag-bulletin-q3-2024/>

¹⁴ <https://blog.google/threat-analysis-group/tag-bulletin-q4-2023/>



Note. YouTube channels blocked for coordinated influence operations, by suspected country of origin, Q1 2020–Q1 2026. Y-axis uses a pseudo-log transformation, which compresses large values. Google recorded zero blocked channels for Rwanda during the observation period. Source: Google TAG / Influence Operations Bulletins.

4.2 Transnational Repression

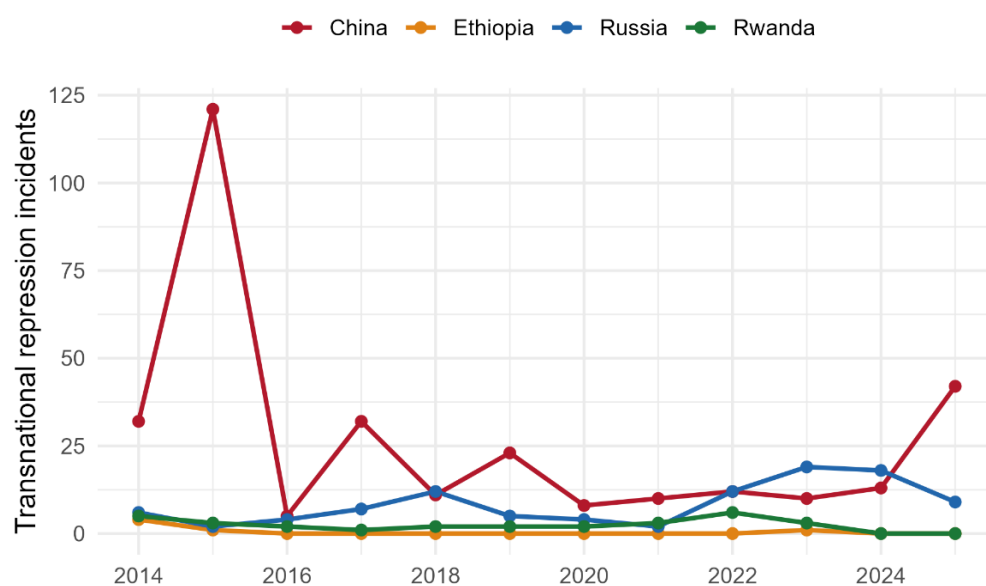
This section draws on Freedom House's Transnational Repression Database (v7), which defines transnational repression as "governments reaching across borders to silence dissent among diasporas and exiles, including through assassinations, illegal deportations, abductions, digital threats, Interpol abuse, and family intimidation." Freedom House codes seven physical incident types: Assassination/assassination attempt; Assault; Credible threat (a threat serious enough that host-country law enforcement takes protective action); Detention (held over 12 hours at the origin state's request); Rendition (forcible return without legal process, including abductions and effectively unprotected deportations); Unlawful deportation (forcible return with some due-process violations to a country where persecution is likely); and Unexplained disappearance. These practices correspond most closely to what we label **suppression of information production**, since they aim at preventing information from being produced by removing or threatening the people who would do so.

The dataset covers 1,375 incidents across 54 origin and 107 host countries. China alone accounts for 23% of all documented incidents worldwide and the ten largest origin states (China, Türkiye, Russia, Tajikistan, Egypt, Turkmenistan, Cambodia, Iran, Uzbekistan, and Belarus) together account for roughly 75% of all incidents. Neither Rwanda nor Ethiopia appear among these top ten.

Figure 4 shows the number of transnational repression incidents per year for each country, between 2014 and 2025. China records by far the highest counts, with a pronounced 2015 spike (121 incidents) followed by a more moderate, fluctuating pattern through 2024 and a rise to 42 incidents in 2025. Russia shows a low, flat count through 2019, then a clear upward trend from 2020 onward, peaking at 19 incidents in 2023. Ethiopia and Rwanda remain consistently low throughout the period, with Rwanda recording zero incidents in both 2024 and 2025.

This shift lines up with a documented change in Russian state behaviour: prior to the full-scale invasion of Ukraine in February 2022, the Kremlin's use of transnational repression was comparatively narrow and selective, concentrated on high-profile former insiders, oligarchs, and defectors. Following the invasion, mass emigration broadened the pool of potential targets considerably, and previously rare tactics such as coercion-by-proxy against family members inside Russia became common.¹⁵ Rwanda and Ethiopia remain consistently low throughout the period, with Rwanda recording zero incidents in both 2024 and 2025.

Figure 4. Incidents of transnational repression over time



Note. Figure displays overall number of incidents for each country; source: Freedom House¹⁶

¹⁵ Schenkan et al., *Perpetrators and Methods of Transnational Repression and Possible Counter Strategies*.

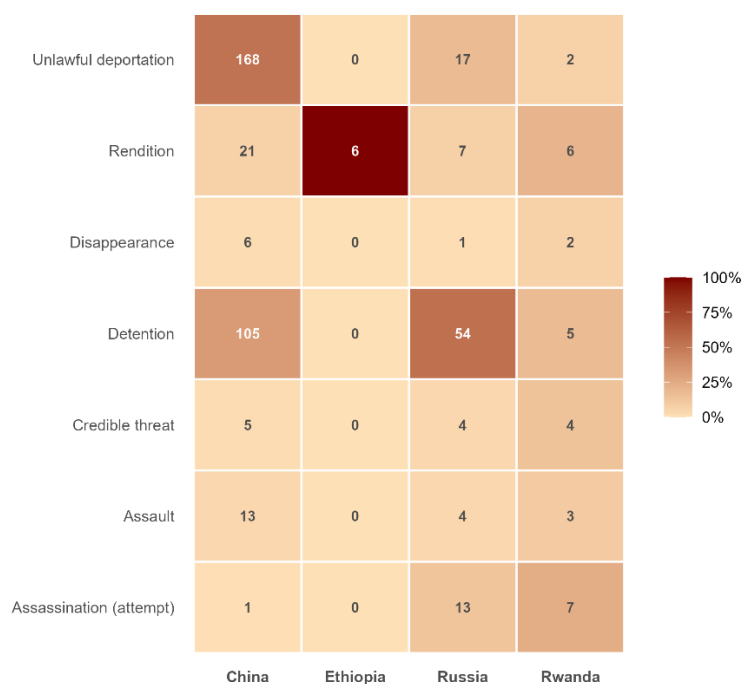
¹⁶ Freedom House, 'Transnational Repression'.

Figure 5 disaggregates these incidents by type. China's incidents are concentrated in unlawful deportation (168) and detention (105). Russia's incidents are led by detention (54) but include a disproportionate 13 assassination attempts, notably higher than China's single case and higher than Russia's global share of assassination incidents overall. This divergence has a documented structural explanation: host-origin state cooperation, required for detention and deportation, is significantly more likely when both host and origin states are authoritarian; when the host state is a well-functioning democracy less willing to cooperate, origin states are pushed toward direct physical attacks instead.¹⁷ China's deportation-heavy profile is consistent with extensive cooperation from host states, including non-democracies and states economically dependent on China; Russia's elevated assassination share is consistent with a higher proportion of its targets residing in democracies unwilling to cooperate through formal channels.

Rwanda's much smaller incident count is nonetheless weighted toward assassination attempts (7) and credible threats (4) relative to its total broadly consistent with the same mechanism (Rwanda's targets are disproportionately located in democracies) and with qualitative accounts describing Rwanda's transnational repression as targeted at specific high-profile exiled critics rather than broad-based. Ethiopia's entries are limited almost entirely to rendition (6 incidents, no other incident types reported).

Figure 5. Incidents of transnational repression by category

¹⁷ Schenckkan et al., *Perpetrators and Methods of Transnational Repression and Possible Counter Strategies*; Michaelsen and Ruijgrok, 'Autocracy's Long Reach'.



Note. Transnational repression incidents by origin country and incident type, Transnational Repression Database v7. Cell values show raw incident counts; colour shows each incident type's share of that country's total documented incidents (i.e., colours are calculated within columns, not across the whole table); source: Freedom House

2.3. Limitations

Each data source presented above captures a different, partial aspect of transnational information suppression, and none should be read as comprehensive on its own.

Freedom House's Transnational Repression Database deliberately limits its scope to *physical* incidents, in order to maintain consistent, verifiable open-source coding. According to a recent study¹⁸ by the European Parliament (EP), five categories of transnational repression are considered too difficult to document comprehensively through open-source data to be reliably quantified, and are therefore excluded from Freedom House' core incident count: **coercion-by-proxy** (threats or harassment of family members remaining in the origin country), **digital transnational repression** (hacking, spyware, doxxing, and online harassment), **Interpol abuse** (misuse of Red Notices and diffusions to detain or intimidate),

¹⁸ Schenkkan et al., *Perpetrators and Methods of Transnational Repression and Possible Counter Strategies*.

mobility controls (passport cancellation, denial of consular services, revocation of nationality), and **financial transnational repression** (weaponising anti-money-laundering compliance systems to freeze exiles' bank access).

This is a significant limitation from our perspective as this data omits incidents that are increasingly present as reported in the next section. The same EP study notes an emerging, still under-documented cluster of transnational repression cooperation "increasingly in East Africa," suggesting regional dynamics involving Rwanda or Ethiopia may be developing in ways not yet reflected in the current data collection effort by Freedom House.

V-Dem's transnational indicators, as discussed in Section 4.1, capture only disinformation-based suppression of information salience and are themselves based on expert perception rather than documented incidents. In addition, the indicators explicitly focus on disinformation targeting foreign audiences neglecting diaspora as an important target itself.

While these indicators provide important starting points for comparing levels of information suppression across countries, they are limited in scope. Understanding the full scope of information suppression, and how its composition differs across regimes with different capacities and institutional repertoires, therefore requires triangulating these quantitative sources against the more detailed information.

5. Tactics of Information Suppression

This section works through the typology developed in Section 2, asking of each tactic the same two questions: *which actor* carries it out, and *whom* does it target. It does not claim to be a comprehensive inventory of every tactic each regime has ever used; rather, it presents the tactics and associated techniques that emerged as most relevant across our interviews, desk research, and social media analysis, organised by the stage of the information cycle at which they operate.

Sections 5.1 to 5.3 follow the same structure: an overview of what the stage involves, the tactics and associated techniques observed for each of the four cases, a summary table of tactics, actors, and targets, and a short synthesis of which actors and targets predominate at that stage. The three sections are best read together rather than in isolation. As the discussion moves from production toward salience, the underlying mechanism tends to shift from coercion toward persuasion, and the actors involved tend to shift from state bodies acting directly toward commercial intermediaries and private individuals acting on the state's behalf.

5.1 Production-stage tactics

Production-stage tactics intervene before a critical narrative exists, targeting the producers who would otherwise create it. Because they remove information at its source, these are the most complete forms of suppression, but the intervening actor also requires the deepest leverage over a specific individual (Section 2.1); most of the tactics below work through **coercion**, exercised by state bodies directly or through private individuals acting as intermediaries. Table 1 provides an overview of production-stage tactics.

Table 1. Production-stage tactics

TACTIC	ACTOR	TARGET
Restricting access to locations and data sources	state bodies	producers
Extra-legal intimidation	state bodies; private individuals	producers; audiences
Legal/regulatory deterrence	state bodies	producers
Surveillance and monitoring of producers	state bodies; private individuals	producers
Media capture (production stage)	state bodies	outlets

Tactic 1. Restricting access to locations and data sources: Regimes deny or complicate the visas, accreditation, and access needed for producers to work in or on the country, raising the practical cost of independent research and reporting. Case Study 1 provides an example for this tactic in Ethiopia.

Actor: state bodies; **Target:** producers (journalists, academics, researchers)

- The most direct form is the refusal of a visa, a visa renewal, or press accreditation, which removes the producer from the field entirely. The pattern is present in all four cases. For China, 3 to 9 percent of researchers report visa denials.¹⁹ In Russia several foreign correspondents lost or were denied accreditation.²⁰ In Rwanda, a

¹⁹ ARM Project, *China's Information Control Practices*, 12.

²⁰ Juzefovičs et al., *Russian Information Suppression as FIMI*, 19.

Human Rights Watch researcher was barred from entering in the country in 2024.²¹ In Ethiopia, several foreign journalists were detained and/or expelled since 2021.²²

Case 1. Ethiopia: Revocation of accreditation and expulsions as instruments of suppressing production

The Ethiopian state has increasingly resorted to revocation of press credentials and subsequent expulsion of journalists to deny access to the country in general, and conflict zones in particular, thereby suppressing information production. This has been the case during the Tigray war (2020-2022) but has accelerated in the past year as the state faces multiple armed insurgencies. At the very start of the war in November 2020, the Ethiopian Broadcasting Authority suspended the press licence of a Reuters journalist and sent warning letters to the BBC and DW.²³ In May 2021, it revoked the press accreditation a new York times reporter, accusing him of lacking impartiality and reporting fake news.²⁴ In May 2022, the government withdrew the accreditation the economist's correspondent in Addis Ababa, informing him to leave the country in 48 hours.²⁵ In February 2024, a French reporter writing for Africa Intelligence was detained for a week, accused of 'conspiracy to create chaos' after interviewing a member of the Oromo Liberation Front.²⁶ In February 2026, the government declined to renew the accreditation of three Reuters journalists based in Addis Ababa after Reuters reported that the country is hosting a secret training camp for the Rapid Support Forces (RSF) of Sudan.²⁷ Another French journalist was expelled in June 2026 after authorities revoked her press accreditation and residence permit.²⁸ these cases illustrate an escalating trend of using press credentials, in combination with detentions and expulsions, as a mechanism of controlling what foreign media can access and report, effectively suppressing information at the production stage.

- A more indirect variant raises the cost of access through procedural friction rather than outright denial, taking the form of repeated in-person visits, demands for interviewee lists in advance, and requirements for notarised documentation. For China, 7 to 14 percent of surveyed researchers report difficulties obtaining a visa on these grounds.²⁹ Rwanda requires researchers to apply for permits at least three months in advance through a process that varies by research type and ministry, submitting a full project description along with copies of every questionnaire and interview protocol – a practice that effectively serves as deterrent.³⁰ Ethiopia combines the deliberately onerous annual renewal of media licenses with the denial of access to conflict zones, as observed in Tigray³¹.

²¹ Human Rights Watch, *Human Rights Watch Submission to the Universal Periodic Review of Rwanda (51st Session)*, 2.

²² Pohjonen et al., *Information Suppression in Ethiopia*, 20.

²³ Addis Standard, 'Facebook'.

²⁴ RSF, 'RSF Condemns NYT Reporter's Unprecedented Expulsion from Ethiopia'.

²⁵ The Economist Group, 'Press Statement: The Economist'.

²⁶ Paravicini, 'Ethiopian Police Arrest French Journalist, Employer Says'.

²⁷ Reuters, 'Ethiopia Revokes Accreditation of Reuters Journalists'.

²⁸ Observer, 'French Journalist Augustine Passilly Expelled from Ethiopia'.

²⁹ ARM Project, *China's Information Control Practices*, 12.

³⁰ Loyle, 'Overcoming Research Obstacles in Hybrid Regimes', 927.

³¹ Pohjonen et al., *Information Suppression in Ethiopia*, 16–17.

- Access may also be constrained at the level of sources rather than places, including archives, libraries, surveys, and census data. Restricting access to these sources degrades work that depends on the documentary record rather than on field presence. For China, between 3 and 14 percent of surveyed researchers report being denied entry to a library, archive, or specific materials.³² Russia has restricted access to archival sources (e.g. on state repression) and various types of governmental data, including key economic and demographic data and court statistics.³³ In Rwanda, the constraint is legal in character: weak implementation of the Right to Information Law and an extensive research-permitting system leave researchers with limited access in practice.³⁴ In Ethiopia, denial of access to information is a routine bureaucratic practice, with government offices obstructing or refusing requests outright.³⁵
- *Effect:* This tactic degrades the quality and scope of research and reporting by cutting producers off from the field, the documentary record, or both. Its reach extends beyond the work it blocks directly. Because access is renewable and discretionary the prospect of a future refusal encourages self-censorship in the choice of topic or angle, so that producers narrow their own work to preserve continued entry.

Tactic 2. Extra-legal intimidation. Threats delivered directly or through intermediaries induce fear in a producer without formal legal process, discouraging them from producing or continuing critical work. Case study 2 provides an example of this tactic in the Russian case.

Actor: state bodies and private individuals; **Target:** producers (researchers, journalists, human rights defenders), with spillover to audiences

³² ARM Project, *China's Information Control Practices*, 12.

³³ <https://novayagazeta.eu/en/articles/2025/10/08/in-the-dark-en>
<https://www.timeshighereducation.com/news/locked-out-archives-scholars-forced-study-russia-afar>
<https://www.themoscowtimes.com/2025/08/01/russia-limits-access-to-key-economic-and-demographic-data-amid-downturn-concerns-a90068>
<https://www.themoscowtimes.com/2026/04/21/russia-removes-2-decades-of-court-statistics-from-public-access-a92561>

³⁴ Loyle, 'Overcoming Research Obstacles in Hybrid Regimes', 927.

³⁵ Pohjonen et al., *Information Suppression in Ethiopia*, 16–17.

- Information producers are often threatened directly. These threats range from pressure to cooperate during an encounter to explicit verbal warnings, usually after critical work has been produced or presented. Unlike more indirect threats, this requires the actor to accept some visibility, since the direct threat is more likely to be tracked to its source. In China it appears mainly as pressure to cooperate.³⁶ In Rwanda, this has taken the form of government representatives warning researchers in person against returning to the country after a public presentation touching on sensitive topics³⁷ In Ethiopia, it extends to a sustained threat campaign directed at an individual academic.³⁸ In Russia, this takes both an institutional and an individual form: regulatory warnings that push outlets toward self-censorship or closure,³⁹ and direct encounters with security services in which journalists are questioned and cautioned in person.⁴⁰ In the case of Russia, more dangerous tactics, including assassination attempts (abroad), have also been recorded.⁴¹

Case 2. Russia: Indirect intimidation to suppress information production

Following Russia's full-scale invasion of Ukraine in 2022, more than 1,500 journalists left the country.⁴² Russian authorities have responded, in part, by targeting the relatives of exiled journalists, a means of exerting pressure on those who can no longer be reached through domestic legal channels. CPJ documents two cases: the search of the parents' home of Alesya Marokhovskaya, exiled editor-in-chief of the investigative outlet iStories, in Magadan in December 2024, and the search of the relatives' apartment of investigative journalist Aleksandra Garmazhapova in St. Petersburg in October 2025, both conducted in connection with foreign-agent criminal proceedings against journalists residing abroad.⁴³ In Russian-occupied Ukrainian territories, RSF documents a more direct variant where FSB agents visited the homes of journalists' relatives, seizing equipment, and issuing threats.⁴⁴ CEPA's 2026 analysis of Russian independent media in exile identifies "intimidation of relatives" as a documented form of transnational repression directed at the exiled Russian press, alongside criminal convictions in absentia and surveillance in the country of residence. The cumulative effect is a form of coercive reach that extends beyond Russian territorial borders, using second-degree contacts as the instrument of pressure.

- Intimidation frequently reaches the information producer indirectly, through a second-degree contact rather than the target. Authorities approach a family member, a friend, or a colleague, and the warning travels back to the producer, exerting real pressure

³⁶ ARM Project, *China's Information Control Practices*, 12,16.

³⁷ Jessee, 'Rwanda's Subtle Forms of Intimidation'.

³⁸ Pohjonen et al., *Information Suppression in Ethiopia*, 20.

³⁹ 'Russian Newspaper Novaya Gazeta Suspends Publication Following Official Warning'.

⁴⁰ CPJ Europe and Central Asia, 'Russia's Repression Record'.

⁴¹ Weiss, 'Blood Simple. Several Russian Journalists and Activists Were Poisoned in Europe'.

⁴² Roshchin, 'An Ecosystem of Truth'.

⁴³ CPJ Europe and Central Asia, 'Russia's Repression Record'.

⁴⁴ RSF, 'Journalists' Families Increasingly Targeted with Intimidation Tactics by Repressive Regimes | RSF'.

while leaving no formal record against the target. In China, authorities contact the family or friends of the researcher.⁴⁵ In Rwanda the warning often arrives by implication, surfacing in fieldwork where stories about what befell earlier critics leave the researcher to infer the risks.⁴⁶ In Ethiopia it takes the form of routine harassment through third parties.⁴⁷

- *Effect:* This tactic induces fear and self-censorship without recourse to formal process, which makes it difficult to contest and easy to deny. It rarely suppresses a project outright. More often it reshapes the work from within, softening findings, narrowing focus, or steering the producer away from the most sensitive material.

Tactic 3. Legal/regulatory deterrence. Broad or vaguely worded legislation raises the legal risk of producing coverage, deterring coverage independent of any individual threat. The risk may attach either to the subject matter, making certain topics dangerous to cover, or to the speaker, making certain actors' output dangerous: While primarily directed at domestic targets, this can also affect international producers.

Actor: state bodies; **Target:** producers (researchers, journalists, human rights defenders)

- Restrictive legislation on terrorism, hate speech, media, civil society, or emergency powers makes an entire topic legally risky to cover, so that coverage is deterred before any producer is approached. It is well documented for Rwanda and Ethiopia. In Rwanda it works through genocide-ideology and sectarianism laws that lack clear safeguards, leaving their scope open to interpretation.⁴⁸ In Ethiopia, it operates through overlapping instruments, combining anti-terrorism and hate-speech legislation with repeated states of emergency, whose broad definitions have been used to prosecute journalists connected to the Amhara insurgency.⁴⁹
- Legislation attaches criminal liability or a stigmatising legal status to actors on the basis of their foreign funding, affiliations, or access to information, so that their entire output becomes risky regardless of topic. It is well documented for China and Russia. In China it works through the 2023 Counter-Espionage Law, whose broadened and undefined definition of espionage attaches legal risk to gathering or transmitting information deemed relevant to national security, leaving foreign businesses, NGOs

⁴⁵ ARM Project, *China's Information Control Practices*, 12.

⁴⁶ Jessee, 'The Danger of a Single Story'.

⁴⁷ Pohjonen et al., *Information Suppression in Ethiopia*, 17.

⁴⁸ Michalakea et al., *Information Suppression in Rwanda*, 13.

⁴⁹ Pohjonen et al., *Information Suppression in Ethiopia*, 19.

with foreign donors or foreign staff, journalists, and researchers unsure where the line falls and inclined to avoid sensitive subjects altogether.⁵⁰ In Russia it operates through the 2012 “foreign agent” and 2015 “undesirable organisations” laws, which designate persons and organisations by their foreign funding or connection rather than by anything they publish: those labelled must mark all of their output as “foreign agent” material and face escalating restrictions, while any cooperation with an “undesirable” organisation is itself criminalised.⁵¹

- *Effect:* The tactic works because the risk sits with the coverage rather than with any individual threat, so producers hold back before anyone approaches them. Sometimes it is the topic that becomes too risky to touch, avoided regardless of who would cover it; other times it is the producer, whose foreign ties make their whole output feel risky no matter the subject.

Tactic 4. Surveillance and monitoring of producers. Regimes monitor a producer’s activities and contacts directly or through intermediaries, both to intimidate and to enable more targeted suppression.

Actor: state bodies and private individuals (e.g., local fixers, informants); **Target:** producers

- At the digital end, regimes deploy spyware against critics and their contacts, giving them access to a target’s communications, location, and devices. In China it works through LightSpy, a modular phone implant spread by watering-hole attacks against iOS users in Hong Kong and linked to China-based operators.⁵² In Russia the FSB planted Monokle-type spyware on the phone of an activist accused of aiding Ukraine, covertly returning the device so it could keep monitoring him, as documented by the Citizen Lab.⁵³ Rwanda famously used NSO’s software Pegasus against journalists and opposition figures and extending to foreign politicians and officials well beyond

⁵⁰ McCarthy and Gan, ‘China Has Widened Its Counter-Espionage Law. Experts Say Foreign Businesses Should Be Worried’.

⁵¹ Reporters Without Borders (RSF), *Independent Media Are the Primary Targets of Kremlin Laws against ‘Foreign Agents’ and ‘Undesirable Organisations’*.

⁵² Cao et al., *Operation Poisoned News: Hong Kong Users Targeted with Mobile Malware via Local News Links*.

⁵³ Quintin et al., *Something to Remember Us By: Device Confiscated by Russian Authorities Returned with Monokle-Type Spyware Installed*.

this country's own territory (see case study 3).⁵⁴ Pegasus was also found on the devices of Russian journalists in exile in Latvia and Lithuania.⁵⁵

Case 3. Rwanda's use of NSO's Pegasus spyware to monitor journalists and human rights defenders

In September 2018, initial investigations by the Citizen Lab revealed that Rwanda was among countries identified as possibly using Pegasus, a surveillance software, and using targeting materials with political themes, indicating that this software was possibly used against political opponents rather than to conduct criminal investigations⁵⁶. Three years later, investigations led by Amnesty International's Security Lab showed that Rwanda had been using Pegasus to spy on political opponents and their family members in exile, including in Belgium, as well as on human rights defenders and on journalists⁵⁷. A few months later, Belgian intelligence services confirmed that the phones of two Belgian journalists, a husband and wife, had been infected by Pegasus, very likely from Rwanda⁵⁸. NSO, the company behind the software, confirmed in 2024 that it has not had users in Rwanda since 2021⁵⁹. Deploying this type of spyware to monitor the activities of journalists, human rights defenders or politicians abroad makes it possible for the regime to target producers with other tactics, such as threats or smear campaigns aiming to suppress the dissemination of unwanted information or making it less salient.

- Regimes also work through people, recruiting local fixers, drivers, or contacts as informants who report on a producer's movements. This form leaves the lightest technical trace, since it relies on ordinary social relationships rather than any tool. In the Chinese case, human surveillance is well documented, with many accounts of correspondents followed in the field, interviewees pressured into silence, and local intermediaries enlisted as informants. Knowledge workers in China are regularly summoned for questioning ("invited for tea") and asked about their own work and that of others, turning professional networks into a channel for monitoring. In China, surveillance is often not diffuse, but sometimes deliberately overt as visibility itself serves an intimidation function.⁶⁰ Similar practices have been documented in Rwanda, but there, surveillance is generally experienced as more diffuse and producers often only realise what has been going on at a later stage.⁶¹ Russia

⁵⁴ Amnesty International, *Rwandan Authorities Chose Thousands of Activists, Journalists and Politicians to Target with NSO Spyware*.

⁵⁵ 'Exiled, Then Spied On'.

⁵⁶ 'HIDE AND SEEK'.

⁵⁷ 'Rwandan Authorities Chose Thousands of Activists, Journalists and Politicians to Target with NSO Spyware'.

⁵⁸ *Le Monde*, 'Des journalistes belges espionnés via le logiciel Pegasus'.

⁵⁹ Reynaud and Rueckert, 'Au Rwanda, opposants et proches du régime ciblés par le logiciel espion Pegasus pendant des années'.

⁶⁰ Dukalskis, 'Controlling Critical Messengers: Foreign Correspondents in China'; Lim, 'Foreign Correspondence in China'.

⁶¹ Michalakea et al., *Information Suppression in Rwanda*, 16.

actively seeks to infiltrate activist circles, both domestically and internationally, often employing coercion.⁶²

- A more intrusive form goes after the record of the work itself, with officials asking for or seizing research notes and interviewee lists. In China, officials confiscate notes and computers;⁶³ in Rwanda they demand a researcher's materials.⁶⁴ This overlaps with intimidation, since the request itself works as a warning, and it exposes not only the producer but the sources behind the work.
- *Effect:* This enables downstream suppression, feeding into forms of targeted intimidation, and so functions as a precondition for other tactics rather than an endpoint in its own right.

Tactic 5. Media capture (production stage). Regimes secure direct influence over who owns or manages a media outlet, shaping what that outlet is willing to produce before any single article is written.

Actor: state bodies; **Target:** outlets

- Regimes secure direct influence over who manages and runs an outlet. In China this operates through Chinese-owned international outlets, whose management reflects state perspectives as a condition of that control.⁶⁵ In Russia it works both through outlets the state stands up directly, such as RT Balkan,⁶⁶ and through ownership transfers that move existing intermediaries into Kremlin-aligned hands, as when Yandex ceded its news aggregator and homepage to VK, itself controlled through a holding tied to a close Putin associate.⁶⁷
- *Effect:* Control over ownership affects both what gets produced and what gets disseminated.
-

⁶² Times, 'Ex-Pussy Riot Member Says She Helped the FSB Spy on Kremlin Critics'.

⁶³ ARM Project, *China's Information Control Practices*, 12.

⁶⁴ Thomson, "That Is Not What We Authorised You to Do ...".

⁶⁵ ARM Project, *China's Information Control Practices*, 40.

⁶⁶ Juzefovičs et al., *Russian Information Suppression as FIMI*, 18.

⁶⁷ Vendil Pallin, 'Internet Control through Ownership', 24–25; Kravets-Meinke, 'The Sad Fate of Yandex: From Independent Tech Startup to Kremlin Propaganda Tool'.

5.2 Dissemination-stage tactics

Dissemination-stage tactics do not prevent information from existing but prevent it from reaching a channel capable of carrying it to an audience. Several tactics at this stage operate through persuasion directed at outlets rather than pure coercion, and media capture in particular continues directly from the production-stage tactic of the same name: the outlet, initially a target, becomes the acting party once captured. Table 2 provides an overview of dissemination-stage tactics.

Table 2. Dissemination-stage tactics

TACTIC	ACTOR	TARGET
Undermining the credibility of producers	state bodies; private individuals	producers; outlets
Media capture (dissemination stage)	commercial intermediaries	audiences
Extending domestic legal jurisdiction over audiences abroad	state bodies; commercial intermediaries	audiences
Legal and regulatory deterrence via lawfare	state bodies; private individuals	outlets; producers
Influencing platform moderation policies	state bodies; private individuals	outlets

Tactic 1. Undermining the credibility of producers. Coordinated harassment or discrediting campaigns reduce the reach of a producer's work by attacking their credibility rather than the content itself.

Actor: state bodies and private individuals; **Target:** producers, with spillover to outlets

- Sustained harassment and smear campaigns, including dogpiling, are the most common form. In China they involve personal insults, character assassination, and coordinated harassment directed at diaspora-based academics.⁶⁸ In Russia, smear campaigns have targeted both domestic and international information producers, such as a Swedish investigative journalist.⁶⁹ In Rwanda the regime organises discrediting campaigns around critical publications, including a bot- and AI-imagery-

⁶⁸ ARM Project, *China's Information Control Practices*, 15–16.

⁶⁹ Juzefovičs et al., *Russian Information Suppression as FIMI*, 11.

assisted campaign against the Forbidden Stories investigation.⁷⁰ In Ethiopia they escalate into a threat campaign against a named Norwegian academic.⁷¹

- A second form mobilises aligned private individuals to co-sign open letters and petitions that discredit critical reporting. In China's case, following the Wall Street Journal's 'Sick Man of Asia' headline in 2020, a petition was launched by private individuals demanding an apology and retraction while denouncing the newspaper's "poor judgement". The petition gathered over 115,000 signatures, reflecting both genuine grassroot action and Chinese state media mobilisation.⁷² In Rwanda, academics and journalists co-signed a statement attacking the Forbidden Stories investigation for relying too heavily on perpetrator testimony.⁷³
- *Effect:* This tactic discredits producers in the eyes of the audience without needing to remove their reporting; it also feeds back into production by deterring further work on sensitive topics.

Tactic 2. Media capture (dissemination stage). Once an outlet has been captured (Section 5.1), it enforces informal restrictions on its own coverage, shaping what content actually reaches an audience without further state action.

Actor: commercial intermediaries (the now-captured outlet); **Target:** audiences

- Through state-company partnerships, the state coerces a platform or company into disciplining its own conduct. In China, after Jack Ma's 2020 fall, Alibaba began policing itself, so that minimal state pressure now keeps it aligned with the state's preferences.⁷⁴
- *Effect:* This pushes outlets toward informal self-restriction, shaping what content is readily available without any formal act of censorship.

Tactic 3. Extending domestic legal jurisdiction over audiences abroad. Domestic law and platform rules are extended to reach citizens abroad, so that diaspora audiences remain governed by home-country restrictions regardless of their physical location.

Actor: state bodies and commercial intermediaries; **Target:** audiences (diaspora)

Dukalskis, *Making the World Safe for Dictatorship*, 147; Michalakea et al., *Information Suppression in Rwanda*, 22.⁷⁰ {Citation}

⁷¹ Kruhaug, 'Norsk Professor Trues På Livet Av Etiopiere: – Det Pågår En Aktiv, Koordinert Hatkampanje Mot Meg'.

⁷² Tracy, 'Inside The Wall Street Journal, Tensions Rise Over "Sick Man" China Headline'.

⁷³ Michalakea et al., *Information Suppression in Rwanda*, 22.

⁷⁴ Keane, 'China's Record Fine against Alibaba Spells the End of Big Tech's Romance with the State'.

- The state extends its data and privacy law to citizens abroad, so that diaspora users of state-linked platforms remain governed from home wherever they live. In China, users of Chinese-owned platforms remain subject to domestic surveillance and censorship regardless of their location.⁷⁵ In Russia, diaspora users of home-grown platforms such as VKontakte stay within reach of Russian law, which requires these services to retain communications and surrender them to the FSB.⁷⁶
- The state carries its domestic censorship criteria abroad through the platforms it owns, so that overseas users meet home-country restrictions through the service itself. In China, dual terms-of-service regimes on TikTok, AliExpress, and AI platforms such as DeepSeek leak domestic censorship criteria to overseas users.⁷⁷
- *Effect:* This tactic restricts what diaspora audiences can access even outside the regime's territorial jurisdiction, while facilitating the spread of state-aligned content instead.

Tactic 4. Legal and regulatory deterrence via lawfare. Costly litigation or regulatory complaints are used to deter publication or investigation, regardless of whether the underlying claim succeeds.

Actor: state bodies and private individuals; **Target:** outlets and producers

- Regimes and their supporters deploy SLAPP suits (Strategic Lawsuits Against Public Participation) and defamation or data-protection litigation to deter publication or investigation, so that the cost of defending a case suppresses critical work regardless of whether the underlying claim succeeds. In Russia, oligarchs brought a series of lawsuits against the journalist Catherine Belton and her publisher over *Putin's People*.⁷⁸ In Rwanda, regime-aligned individuals and organisations used genocide-denial complaints and lawsuits to pressure critics, both through the BBC's editorial complaint mechanism and through the French courts.⁷⁹
- *Effect:* This tactic limits the spread of specific content (books, films) and deters future investigation, independent of whether any suit succeeds.

⁷⁵ Knockel et al., *We Chat, They Watch: How International Users Unwittingly Build up WeChat's Chinese Censorship Apparatus*.

⁷⁶ Andreeva et al., *Data Localization Laws: Russian Federation*.

⁷⁷ ARM Project, *China's Information Control Practices*, 29–31.

⁷⁸ Juzefovičs et al., *Russian Information Suppression as FIMI*, 13.

⁷⁹ Michalakea et al., *Information Suppression in Rwanda*, 23–24.

Tactic 5. Influencing platform moderation policies. Coordinated reporting or algorithmic manipulation is used to trigger a platform's own moderation systems against critical content, achieving removal without direct state action.

Actor: state bodies and private individuals; **Target:** outlets/platforms (commercial intermediaries), whose own systems are exploited

- State-affiliated actors use algorithmic manipulation and mass reporting to trigger the platform's own removal of critical content. In Ethiopia, coordinated mass reporting during the Tigray war was used to trigger the platform's moderation systems against critical content and force its removal.⁸⁰
- *Effect:* It facilitates dissemination of state-aligned content by suppressing critical content through the platform's own moderation systems rather than direct state action.

5.3 Salience-stage Tactics

Salience-stage tactics do not prevent information from existing or circulating; they prevent it from being noticed, by burying it beneath a larger volume of competing information. This is the stage at which persuasion aimed at audiences most clearly shades into suppression: the tactics below are labelled as suppression specifically because their documented purpose is to bury competing content rather than to build genuine belief in an alternative piece of information. Salience-stage tactics require the least relationship-specific leverage of the three stages and are correspondingly the most accessible to actors, including private individuals and commercial intermediaries, who lack the coercive or institutional reach needed to act earlier in the information cycle. Table 3 provides an overview of salience-stage tactics.

Table 3. Salience-stage tactics

TACTIC	ACTOR	TARGET
Burying information and reducing its visibility	state bodies; private individuals	audiences
Amplifying pro-government narratives	state bodies; private individuals	audiences
Undermining the credibility of producers	state bodies; private individuals	audiences

⁸⁰ Pohjonen et al., *Information Suppression in Ethiopia*, 27–28.

Tactic 1. Burying information and reducing its visibility. Rather than removing critical content, regimes reduce its visibility by flooding attention or cultivating norms that discourage audiences from seeking it out or sharing it.

Actor: state bodies and private individuals; **Target:** audiences (diaspora)

- Aligned actors flood the information space through coordinated social media campaigns, drowning critical content beneath a larger volume of competing posts so that audiences are less likely to encounter it. In China this is the core strategy behind the so-called '50 Cent Party' of state-directed internet commentators: fabricating posts with the purpose of distracting and flooding discussions with innocuous content to cover up sensitive topics. Previously, it has been estimated that around 448 million social media comments per year are created by the 50 Cent Party, with bursts of posts timed to mirror naturally viral patterns but at moments of the government's choosing.⁸¹ In Ethiopia, AI-generated content was used to dilute critical narratives around a port-securing deal, burying them under a mass of aligned material.⁸² Russia has actively sought to obstruct public understanding of its military actions and war crimes in Ukraine by disseminating many false or misleading narratives.⁸³
- Aligned actors cultivate norms and social pressure that lead audiences to police their own speech. In China, diaspora knowledge professionals avoid topics that are highly sensitive in the Chinese context, such as human-rights abuses in Xinjiang and the status of Taiwan, leaving these perspectives unvoiced in public debate.⁸⁴ A similar mechanism appears to be at play among Rwandan diasporas: many report that those who criticise the regime are immediately accused of being genocide deniers, in digital smear campaigns or through anonymous phone calls to their employer or to family members, leading to high degrees of self-censorship.⁸⁵
- *Effect:* This tactic makes critical information harder for audiences to find, which in turn reduces the incentive to disseminate it and, further upstream, reduces the incentive to produce it in the first place.

⁸¹ King et al., 'How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, Not Engaged Argument'; Roberts, *Censored*.

⁸² Pohjonen et al., *Information Suppression in Ethiopia*, 37–38.

⁸³ 'The Bucha Massacre'.

⁸⁴ ARM Project, *China's Information Control Practices*, 47.

⁸⁵ Michalakea et al., *Information Suppression in Rwanda*, 45–47.

Case 4. China: Flooding social media with 'beautiful Xinjiang'

As international criticism of human rights abuses in Xinjiang peaked, Chinese state media increasingly produced apolitical content to shift the focus away rather than contest it directly. A systematic analysis of all Xinjiang-related videos posted on YouTube by CGTN and Xinhua's New China TV between 2018 and 2020 shows output spiking with episodes of contention – US legislation, document leaks, sanctions – and, from mid-2020, a shift away from rebuttals towards development, culture, and nature content.⁸⁶ In September 2020, as Washington debated restrictions on Xinjiang cotton, the two channels posted 197 videos totalling almost 400 hours, including near-daily fixed-camera landscape livestreams of up to twelve hours, a strategy of presenting 'other news' to divert public scrutiny of the human rights record. A Dutch open-source investigation of more than fifteen thousand tweets posted between 2019 and 2023 under #xinjiang and #beautifulxinjiang traced a network of self-described Xinjiang residents posting "beautiful scenery" of Xinjiang amplified by CGTN, diplomats, and state-linked accounts. The researchers found that one needs to scroll through more than thirty depoliticised clips before encountering a first critical video.⁸⁷ By saturating feeds with scenery, food, and cultural content, such social media campaigns raise the cost of encountering critical information, reflecting suppression at the salience stage.

Tactic 2. Amplifying pro-government narratives. Regimes flood the information environment with pro-government content, or operate outlets that appear independent, so that state-aligned material crowds out critical narratives by volume rather than by removing them.

Actor: state bodies and private individuals; **Target:** audiences (diaspora and foreign publics)

- Coordinated actors flood the information environment through inauthentic or automated accounts, amplifying pro-government content so that it crowds out critical narratives by sheer volume. In China's case, the number of diplomats and state media on international social media has drastically increased since 2021, and researchers have identified networks of automated accounts amplifying state outlets as such.⁸⁸ In Rwanda, analysis of X during the M23-DRC offensive showed pro-regime accounts dominating the discussion, using AI-generated caricatures, scheduled posting, and other markers of coordinated inauthentic behaviour.⁸⁹ In

⁸⁶ Alpermann and Malzer, "In Other News".

⁸⁷ Goldenberg and Osieck, 'De Zwitserse Alpen lopen tot in Xinjiang'.

⁸⁸ Schliebs et al., *China's Public Diplomacy Operations*; Bradshaw et al., *Industrialized Disinformation: 2020 Global Inventory of Organized Social Media Manipulation*; Bailey and Howard, *The Instigators and Targets of Organised Social Media Manipulation*.

⁸⁹ Michalakea et al., *Information Suppression in Rwanda*, 38–39.

Ethiopia, flooding was used to push pro-regime narratives and bury anti-war voices during the Tigray conflict (see case 4).⁹⁰

- The content of messages is tailored to foster engagement among broad communities, using visuals, memes, or emotionally charged language, sometimes using AI tools. For example, memes have been observed coming from Chinese state-affiliated actors, as a type of strategic content for spreading discontent about democracy and its functioning.⁹¹ Russophone Estonian influencers share satiric and sarcastic videos to propagate Russian propaganda⁹², or the use of imagery glorifying the Rwandan president and military⁹³. Crafting messages that have a high potential to be further shared or liked increases the effectiveness of flooding strategies relying on coordinated inauthentic behaviour, as real audiences are more likely to also distribute them further.
- Aligned actors operate outlets that pose as independent local news while covertly serving the state, so that state-aligned material reaches audiences under the appearance of neutral reporting. In China, a network of at least 123 websites operates covertly from China as ostensibly local outlets across multiple regions, including EU countries, often run through commercial PR intermediaries that obscure the state's role.⁹⁴ Russia has spread disinformation related to its invasion of Ukraine through the Voice of Europe website, also using it as a vehicle to pay politicians for spreading pro-Russian narratives, and through websites and social media impersonating authentic Western media ('Doppelgänger' influence operation).⁹⁵
- *Effect:* This tactic limits the reach and credibility of critical information by outcompeting it in volume and can make pro-regime content the effective majority of what audiences encounter.

⁹⁰ Pohjonen et al., *Information Suppression in Ethiopia*, 31–32.

⁹¹ Jacobs and Carley, '#WhatIsDemocracy'.

⁹² Juzefovičs et al., *Russian Information Suppression as FIMI*, 38.

⁹³ Michalakea et al., *Information Suppression in Rwanda*, 27.

⁹⁴ ARM Project, *China's Information Control Practices*, 44–45.

⁹⁵ 'Doppelgänger - Media Clones Serving Russian Propaganda - EU DisinfoLab'; *Russian Network That 'paid European Politicians' Busted, Authorities Claim*.

Case 5. Ethiopia: Pro-government narratives during the Tigray war and beyond

Online campaigns by government and pro-government actors aimed at controlling the narrative on contested issues and bury competing information has become a key tactic in information suppression. Digital campaigns by the Ethiopian government and its supporters during the Tigray war (2020-2022) are a clear illustration of this phenomenon. Amid international pressure on the government to open humanitarian access to the Tigray region and end the conflict through negotiated settlement, the Ethiopian government and its supporters resorted to online information operations, especially on Twitter/X.⁹⁶

The campaigns aimed at achieving two interrelated objectives. First, they aimed to portray the adversary - the Tigray People's Liberation Front (TPLF) - as an existential threat to Ethiopia's sovereignty and territorial integrity, thereby helping mobilise domestic constituencies for war. Second, they attempted to paint the West (broadly representing the US, EU/Europe, Western media, and human rights organisations) as interventionist and neo-colonial, seeking to influence global perceptions and reduce pressure and potential punitive measures like sanctions. The most visible of these campaigns was represented by the #NoMore campaign in mid-2021, which generated significant engagement online and briefly resulted in on-the-ground protests on the streets of cities in Europe and the US in support of the Ethiopian government.

The blueprint of this digital mobilisation has since become a core modus operandi of the Ethiopian government's efforts to control online conversations on critical issues that matter to its survival and legitimacy. The government's media army has become central to these efforts, flooding online spaces with pro-government narratives. Key among these has been the country's quest for access to the red sea, which has seen a spike in AI-generated propaganda in support of the effort⁹⁷, as well as its campaign to elevate urban corridors as a tool of regime legitimacy.⁹⁸

Tactic 3. Undermining the credibility of producers. Coordinated online messages attacking the producers drown their message and make it inaudible.

Actor: state bodies and private individuals; **Target:** audiences (diaspora and foreign publics)

- Co-opting the language of fact-checking, adopting an objective posture in language to push regime-aligned narratives, propagating disinformation and making information much less visible. China has adopted this format, for instance in its 2021 government-released report "Fact Check: Lies on Xinjiang-related issues versus the truth" as well as various other campaigns and online videos that use a debunking format to sideline critical international reporting as disinformation.⁹⁹ This technique has been used by

⁹⁶ Kebede and Pohjonen, "Adwa, Not AGOA".

⁹⁷ Tesfaye and Pohjonen, *AI and Visual Propaganda in Ethiopia's Red Sea Discourse*.

⁹⁸ Tesfaye Kebede, 'Ethiopia's Urban Renewal Projects and Turn toward Aesthetic Propaganda'.

⁹⁹ Alpermann and Malzer, "In Other News".

Ethiopian authorities during the Tigray War¹⁰⁰. Russia, similarly, has employed pseudo-factchecking to deflect accusations about war crimes in Ukraine.¹⁰¹

- Coordinated smear campaigns involving aligned actors attain such scales that they dominate the information landscape. In China's case, foreign reporting on Xinjiang triggered coordinated discrediting campaigns combining state media, diplomats, and nationalist users. The BBC's coverage was met with a documented party-state effort to discredit the broadcaster, with individual researchers being subjected to an online harassment campaign.¹⁰² In Ethiopia, this took the form of a campaign discrediting Amnesty International's reporting on a massacre in Axum during the Tigray War, including a dedicated hashtag¹⁰³. This can also be observed in online information campaigns relying on memes and caricatures to discredit public figures and distract from the events, as was the case in Rwanda during the M23 invasion of Goma in the DRC in early 2025¹⁰⁴.
- *Effect*: Unwanted information or critical narratives are diluted, as the information space is dominated by regime-aligned narratives mocking or attacking the credibility of producers or actors.

6. Comparison

The stage-by-stage presentation in Section 5 organises tactics by where they intervene in the information cycle. This section turns to what the resulting pattern reveals about how the four regimes differ from one another, and what follows from those differences for research and policy.

6.1 Bottleneck vs Relationship-specific Control

The sharpest structural distinction between the four cases is not one of degree but of kind. Media capture, that is securing durable influence over a platform, outlet, or piece of infrastructure rather than over an individual, appears exclusively in the China and Russia cases across both production and dissemination of information: Chinese platforms that export domestic censorship criteria to diaspora users regardless of physical location,

¹⁰⁰ Pohjonen et al., *Information Suppression in Ethiopia*, 34.

¹⁰¹ Alyukov and Zavadskaya, “It’s Not That Simple, We Don’t Know the Whole Truth”.

¹⁰² Zhang and Wallis, *Trigger Warning*.

¹⁰³ Pohjonen et al., *Information Suppression in Ethiopia*, 33.

¹⁰⁴ Michalakea et al., *Information Suppression in Rwanda*, 30–31.

Chinese-owned international outlets (e.g., CGTN), Russia's direct outlet-building (RT Balkan) and its acquisition of existing intermediaries (the Yandex–VK transfer). Neither Rwanda nor Ethiopia records a comparable tactic.

This distinction matters because bottleneck control changes the underlying economics of suppression. Every other tactic identified in this paper, including extra-legal intimidation, surveillance, lawfare, or coordinated harassment is relationship-specific: it requires identifying a producer and applying leverage to that individual, and its reach is bounded by how many such relationships a regime can sustain. Media capture instead secures a bottleneck through which information must pass. Once captured, a platform or outlet suppresses continuously and at whatever scale its user base reaches, without the regime needing to identify individual targets at all. This is a plausible mechanism behind the scale differences documented in Section 4: China's and Russia's substantially higher volumes across all three quantitative indicators are consistent with an infrastructural capability that Rwanda and Ethiopia do not possess, rather than simply a difference in intent or resolve.

6.2 Preventive versus Reactive Infrastructure

A second distinction concerns continuity rather than capability. Russia's and China's salience-stage activities operate independently of any specific preceding event. Ethiopia's and Rwanda's documented salience-stage tactics, by contrast, cluster around acute crises, such as coordinated flooding during the Tigray conflict or amplification tied to the M23-DRC offensive. In China's and Russia's case there exists a background infrastructure, while in Ethiopia or Rwanda suppression is mobilised reactively around specific triggering events.

Sustaining salience-stage suppression as standing infrastructure, independent of any triggering event, is a distinct and more resource-intensive undertaking than mobilising it once around a specific crisis. This is consistent with China's and Russia's substantially greater scale across all three quantitative indicators in Section 4 and suggests that continuity of salience-stage activity is itself a capacity-linked feature of the four cases.

6.3 Great powers vs regional powers

The two different patterns of suppression outlined in 6.1 and 6.2 may themselves follow from a difference in the position each country occupies on the global stage. Russia and China each have a permanent seat on the UN security council and, as such, are recognised as great powers on the international stage. Their foreign policy agendas also aim at fostering multipolarity and limiting western dominance. This foreign policy interest is reflected in how each country has decided to invest resources in the type of infrastructure that makes it possible to create bottlenecks, for example by taking control over digital platforms that are

popular beyond their borders and using them to extend their control of the information space, including by exporting norms via these platforms, as discussed in section 4.2 and 4.3.

By contrast, Ethiopia and Rwanda occupy a different type of position on the international stage. Both are developmental states that have focused their efforts on economic development, received comparatively large support from donors, and presented themselves as reliable security allies for Western powers.¹⁰⁵ Ethiopia and Rwanda each pursue their own foreign policy goals centred on ensuring their survival and continued development. Ethiopia maintains its position as a diplomatic hub in the region in the face of mounting internal conflicts, while nurturing ambitions to secure access to the Red Sea. Rwanda positions itself as a development success story and as a business and tourism hub in the region, while pursuing a dual policy of neutralising genocide perpetrators and supporters of the former regime exiled in the DRC and securing access to rare minerals. However, because both remain dependent on western donors for part of their budget, they cannot afford to deploy infrastructure-based information suppression tactics observed in Russia and China. Instead, they rely on more relational tactics, targeting specific populations or individuals who threaten their preferred narratives. Because the population capable of producing or amplifying threatening narratives is bounded and largely identifiable, relationship-specific tools are often sufficient. These tactics also are usually less observable and less intrusive, since they target only small populations, thereby limiting the risk of alienating important donors.

This difference in international standing may also explain why more preventive patterns are observed in China and Russia, compared to Ethiopia and Rwanda. The former have much less to lose from being perceived as proactive, given the greater power they enjoy. A contest for international opinion among great powers is by nature continuous requiring sustained investment in standing infrastructure. Ethiopia's and Rwanda's reactive mobilisation around the Tigray conflict and the M23–DRC offensive, respectively, is consistent with suppression driven by a salient crisis threatening their survival and risking their reputation among donors, rather than by a sustained contest for international standing.

7. Key takeaways

This working paper compares transnational information suppression across China, Russia, Ethiopia, and Rwanda. Four takeaways stand out:

TAKE-AWAY 1: Comparative data is limited

¹⁰⁵ Matfess, 'Rwanda and Ethiopia'.

- V-Dem data captures mainly salience-stage suppression (flooding); Freedom House captures mainly production-stage physical incidents
- Five categories – coercion-by-proxy, digital repression, Interpol abuse, mobility controls, financial repression – are excluded from Freedom House's count as too hard to verify
- Dissemination-stage tactics (media capture, lawfare) aren't captured by any quantitative source

TAKE-AWAY 2: Actors differ in tactic and scope

- China and Russia rely on infrastructure over which the state retains some control (e.g., captured platforms, state outlets, partnerships between state and technology companies) that operates continuously at scale
- Ethiopia and Rwanda rely on relationship-specific tactics targeting identifiable individuals
- China alone accounts for 23% of global transnational repression incidents

TAKE-AWAY 3: Smaller cases have less infrastructure, not necessarily less activity

- Rwanda outscores Russia on domestic internet-content regulation; both smaller states are highly active in visa denial, permitting friction, and legal deterrence
- What they lack is bottleneck capability such as platform or outlet ownership with cross-border reach
- Their salience-stage suppression is more reactive, likely reflecting donor dependence and less capacity to absorb visibility risks

TAKE-AWAY 4: Pay more attention to actors and targets

- Information stage alone (production/dissemination/salience) shows *where* suppression intervenes, not *who* wields leverage over *whom*
- State coercion dominates upstream; commercial intermediaries and private individuals take on more of the work downstream, possibly without direct state instruction
- Private-individual pressure is largely invisible to diplomatic or regulatory tools that can check a state or company; effective counter-measures depend on identifying the actor, not just the stage

8. References

- Addis Standard. 'Facebook'. Accessed 24 August 2026.
https://www.facebook.com/permalink.php?story_fbid=3487298434651460&id=177352718979398.
- Alpermann, Björn, and Michael Malzer. "In Other News": China's International Media Strategy on Xinjiang—CGTN and New China TV on YouTube'. *Modern China* 50, no. 2 (2024): 135–78. <https://doi.org/10.1177/00977004231169008>.
- Alyukov, Maxim, and Margarita Zavadskaya. "It's Not That Simple, We Don't Know the Whole Truth": The Effects of Pseudo Fact Checking in Wartime Russia'. *Perspectives on Politics*, 2026, 1–25.
- Amnesty International. *Rwandan Authorities Chose Thousands of Activists, Journalists and Politicians to Target with NSO Spyware*. Amnesty International, 2021.
<https://www.amnesty.org/en/latest/press-release/2021/07/rwandan-authorities-chose-thousands-of-activists-journalists-and-politicians-to-target-with-nso-spyware/>.
- Andreeva, Ksenia, Anastasia Kiseleva, and Alena Neskormyuk. *Data Localization Laws: Russian Federation*. Morgan Lewis, 2021. <https://www.morganlewis.com/-/media/files/publication/outside-publication/article/2021/data-localization-laws-russian-federation.pdf>.
- ARM Project. *China's Information Control Practices*. D2.1. 2026. <https://www.arm-project.eu/wp-content/uploads/2026/03/D2.1-Working-Paper-CN-2.pdf>.
- Bailey, Hannah, and Philip N. Howard. *The Instigators and Targets of Organised Social Media Manipulation*: Oxford University: Internet Institute, 2022.
- Bradshaw, Samantha, Hannah Bailey, and Philip N. Howard. *Industrialized Disinformation: 2020 Global Inventory of Organized Social Media Manipulation*. Computational Propaganda Project at the Oxford Internet Institute, 2021.
- Cao, Elliot, Joseph C. Chen, William Gamazo Sanchez, Lilang Wu, and Ecular Xu. *Operation Poisoned News: Hong Kong Users Targeted with Mobile Malware via Local News Links*. 2020. https://www.trendmicro.com/en_us/research/20/c/operation-poisoned-news--hong-kong-users-targeted-with-mobile-ma.html.
- Coppedge, Michael, John Gerring, Staffan I. Lindberg, Svend-Erik Skaaning, and Jan Teorell. 'V-Dem Comparisons and Contrasts with Other Measurement Projects'. SSRN Scholarly Paper No. 2951014. Social Science Research Network, 2017.
<https://doi.org/10.2139/ssrn.2951014>.
- CPJ Europe and Central Asia. 'Russia's Repression Record'. *Committee to Protect Journalists*, 17 February 2026. <https://cpj.org/2026/02/russias-repression-record/>.

- Demir, Vedat, and Carola Richter. 'Public Diplomacy of Authoritarian Regimes: An Introduction'. In *The Public Diplomacy of Authoritarian Regimes*, edited by Vedat Demir and Carola Richter. Springer Nature Switzerland, 2025. https://doi.org/10.1007/978-3-031-97705-3_1.
- 'Doppelganger - Media Clones Serving Russian Propaganda - EU DisinfoLab'. Accessed 28 August 2026. <https://www.disinfo.eu/doppelganger>.
- Dukalskis, Alexander. 'Controlling Critical Messengers: Foreign Correspondents in China'. In *Making the World Safe for Dictatorship*, by Alexander Dukalskis. Oxford University Press, 2021.
- Dukalskis, Alexander. *Making the World Safe for Dictatorship*. Oxford university press, 2021.
- Dukalskis, Alexander, Saipira Furstenberg, Sebastian Hellmeier, and Redmond Scales. 'The Long Arm and the Iron Fist: Authoritarian Crackdowns and Transnational Repression'. *Journal of Conflict Resolution* 68, no. 6 (2024): 1051–79. <https://doi.org/10.1177/00220027231188896>.
- EEAS. *4th Report on Foreign Information Manipulation and Interference Dismantling the FIMI House of Cards*. 2026.
- Elshehawy, Ashrakat, Konstantin Gavras, Nikolay Marinov, Federico Nanni, and Harald Schoen. 'Illiberal Communication and Election Intervention during the Refugee Crisis in Germany'. *Perspectives on Politics* 20, no. 3 (2022): 860–78. <https://doi.org/10.1017/S1537592721003108>.
- 'Exiled, Then Spied on: Civil Society in Latvia, Lithuania, and Poland Targeted with Pegasus Spyware'. *Access Now*, n.d. Accessed 21 August 2026. <https://www.accessnow.org/publication/civil-society-in-exile-pegasus/>.
- Freedom House. 'Transnational Repression'. Accessed 18 August 2026. <https://freedomhouse.org/report/transnational-repression>.
- Gerschewski, Johannes. 'The Three Pillars of Stability: Legitimation, Repression, and Co-Optation in Autocratic Regimes'. In *Comparing Autocracies in the Early Twenty-First Century*. Routledge, 2015. <https://api.taylorfrancis.com/content/chapters/edit/download?identifierName=doi&identifierValue=10.4324/9781315779676-4&type=chapterpdf>.
- Glasius, Marlies. 'Extraterritorial Authoritarian Practices: A Framework'. *Globalizations* 15, no. 2 (2018): 179–97. <https://doi.org/10.1080/14747731.2017.1403781>.
- Goldenberg, OR, and Chris Osieck. 'De Zwitserse Alpen lopen tot in Xinjiang'. *De Groene Amsterdammer*, 26 July 2023. <https://www.groene.nl/artikel/de-zwitserse-alpen-lopen-tot-in-xinjiang>.

- Guriey, Sergei, and Daniel Treisman. 'Informational Autocrats'. *Journal of Economic Perspectives* 33, no. 4 (2019): 100–127. <https://doi.org/10.1257/jep.33.4.100>.
- 'HIDE AND SEEK: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries'. *The Citizen Lab*, n.d. Accessed 21 August 2026. <https://citizenlab.ca/research/hide-and-peek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/>.
- Human Rights Watch. *Human Rights Watch Submission to the Universal Periodic Review of Rwanda (51st Session)*. UN Human Rights Council, 2025. https://www.hrw.org/sites/default/files/media_2025/07/UPR51_Rwanda_HRW.pdf.
- Jacobs, Charity S., and Kathleen M. Carley. '#WhatIsDemocracy: Finding Key Actors in a Chinese Influence Campaign'. *Computational and Mathematical Organization Theory* 30, no. 2 (2024): 127–47. <https://doi.org/10.1007/s10588-023-09380-9>.
- Jessee, Erin. 'Rwanda's Subtle Forms of Intimidation'. *Times Higher Education*, 2013. <https://www.timeshighereducation.com/comment/opinion/rwandas-subtle-forms-of-intimidation/2009974.article>.
- Jessee, Erin. 'The Danger of a Single Story: Iconic Stories in the Aftermath of the 1994 Rwandan Genocide'. *Memory Studies* 10, no. 2 (2017): 144–63. <https://doi.org/10.1177/1750698016673236>.
- Juzefovičs, Jānis, Vineta Kleinberga, Una Aleksandra Bērziņa Čerenkova, et al. *Russian Information Suppression as FIMI*. D3.1. ARM Project, 2026. <https://www.arm-project.eu/wp-content/uploads/2026/03/D2.1-Working-Paper-CN-2.pdf>.
- Keane, Michael. 'China's Record Fine against Alibaba Spells the End of Big Tech's Romance with the State'. *The Conversation*, 2021. <https://theconversation.com/chinas-record-fine-against-alibaba-spells-the-end-of-big-techs-romance-with-the-state-158878>.
- Kebede, Amanuel Tesfaye, and Matti Pohjonen. "Adwa, Not AGOA": Digital Propaganda and Strategic Narratives during the Ethiopian Civil War of 2020 to 2022'. *Media, War & Conflict*, 17 December 2025, 17506352251403008. <https://doi.org/10.1177/17506352251403008>.
- King, Gary, Jennifer Pan, and Margaret E. Roberts. 'How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, Not Engaged Argument'. *American Political Science Review* 111, no. 3 (2017): 3. <https://doi.org/10.1017/S0003055417000144>.
- Knockel, Jeffrey, Christopher Parsons, Lotus Ruan, Ruohan Xiong, Jedidiah Crandall, and Ron Deibert. *We Chat, They Watch: How International Users Unwittingly Build up WeChat's Chinese Censorship Apparatus*. No. 127. 2020. <https://citizenlab.ca/research/we-chat-they-watch/>.
- Koinova, Maria, and Gerasimos Tsourapas. 'How Do Countries of Origin Engage Migrants and Diasporas? Multiple Actors and Comparative Perspectives'. *International Political*

- Science Review* 39, no. 3 (2018): 311–21.
<https://doi.org/10.1177/0192512118755843>.
- Kravets-Meinke, Daria. 'The Sad Fate of Yandex: From Independent Tech Startup to Kremlin Propaganda Tool'. *ZOIS Spotlight*, 2024. <https://www.zois-berlin.de/en/publications/zois-spotlight/the-sad-fate-of-yandex-from-independent-tech-startup-to-kremlin-propaganda-tool>.
- Kruhaug, Nils-Inge. 'Norsk Professor Trues På Livet Av Etiopiere: – Det Pågår En Aktiv, Koordinert Hatkampanje Mot Meg'. *Aftenposten*, 2021.
<https://www.aftenposten.no/verden/i/weK825/norsk-professor-trues-paa-livet-av-etiopiere-det-paagaar-en-aktiv-koordinert-hatkampanje-mot-meg>.
- Le Monde*. 'Des journalistes belges espionnés via le logiciel Pegasus'. Pixels,Projet Pegasus. 30 September 2021. https://www.lemonde.fr/pixels/article/2021/09/17/des-journalistes-belges-espionnes-via-le-logiciel-pegasus_6095080_4408996.html.
- Lim, Linette. 'Foreign Correspondence in China: Authoritarian Media Control and Journalistic Responses'. *The International Journal of Press/Politics*, 18 October 2025, 19401612251379585. <https://doi.org/10.1177/19401612251379585>.
- Loyle, Cyanne E. 'Overcoming Research Obstacles in Hybrid Regimes: Lessons from Rwanda*'. *Social Science Quarterly* 97, no. 4 (2016): 923–35.
<https://doi.org/10.1111/ssqu.12346>.
- Matfess, Hilary. 'Rwanda and Ethiopia: Developmental Authoritarianism and the New Politics of African Strong Men'. *African Studies Review* 58, no. 2 (2015): 181–204.
<https://doi.org/10.1017/asr.2015.43>.
- Mattingly, Daniel C., and Elaine Yao. 'How Soft Propaganda Persuades'. *Comparative Political Studies* 55, no. 9 (2022): 1569–94.
<https://doi.org/10.1177/00104140211047403>.
- McCarthy, Simone, and Nectar Gan. 'China Has Widened Its Counter-Espionage Law. Experts Say Foreign Businesses Should Be Worried'. *CNN Business*, 2023.
<https://www.cnn.com/2023/04/27/china/china-counter-espionage-law-revision-intl-hnk/index.html>.
- Mechkova, Valeriya, Daniel Pemstein, Brigitte Seim, and Steven Wilson. *Measuring Internet Politics: Digital Society Project (DSP) Annual Report V4*. Technical Report, V-dem Democracy, 2022. https://digitalsocietyproject.org/wp-content/uploads/2022/08/DSP_working_paper_1_v4.pdf.
- Michaelsen, Marcus. 'Exit and Voice in a Digital Age: Iran's Exiled Activists and the Authoritarian State'. *Globalizations* 15, no. 2 (2018): 248–64.
<https://doi.org/10.1080/14747731.2016.1263078>.

- Michaelsen, Marcus, and Kris Ruijgrok. 'Autocracy's Long Reach: Explaining Host Country Influences on Transnational Repression'. *Democratization* 31, no. 2 (2024): 290–314. <https://doi.org/10.1080/13510347.2023.2267448>.
- Michalakea, Taygeti, Pauline Lemaire, Fateme Pourhasanzade, Simon Turner, David Herbert, and Guillaume Nicaise. *Information Suppression in Rwanda*. ARM Project, 2026. <https://www.arm-project.eu/wp-content/uploads/2026/03/D4.1-Working-Paper-RW.pdf>.
- Moss, Dana M. 'Transnational Repression, Diaspora Mobilization, and the Case of The Arab Spring'. *Social Problems* 63, no. 4 (2016): 480–98. <https://doi.org/10.1093/socpro/spw019>.
- Nye, Joseph S. 'Soft Power and Public Diplomacy Revisited'. *The Hague Journal of Diplomacy* 14, nos 1–2 (2019): 7–20. <https://doi.org/10.1163/1871191X-14101013>.
- Observer, Ethiopia. 'French Journalist Augustine Passilly Expelled from Ethiopia'. *Ethiopia Observer*, 12 June 2026. <https://www.ethiopiaobserver.com/2026/06/12/french-journalist-augustine-passilly-expelled-from-ethiopia/>.
- Paravicini, Giulia. 'Ethiopian Police Arrest French Journalist, Employer Says'. *Africa. Reuters*, 6 March 2024. <https://www.reuters.com/world/africa/ethiopian-police-arrest-french-journalist-employer-says-2024-02-26/>.
- Pohjonen, Matti, Amanuel Kebede, and Lovise Aalen. *Information Suppression in Ethiopia*. D5.1. ARM Project, 2026. <https://www.arm-project.eu/wp-content/uploads/2026/03/D5.1-Working-Paper-ET.pdf>.
- Quintin, Cooper, Rebekah Brown, and John Scott-Railton. *Something to Remember Us By: Device Confiscated by Russian Authorities Returned with Monokle-Type Spyware Installed*. No. 181. The Citizen Lab, 2024. <https://citizenlab.ca/research/device-confiscated-by-russian-authorities-returned-with-monokle-type-spyware-installed/>.
- Reporters Without Borders (RSF). *Independent Media Are the Primary Targets of Kremlin Laws against 'Foreign Agents' and 'Undesirable Organisations'*. n.d. <https://rsf.org/en/russia-independent-media-are-primary-targets-kremlin-laws-against-foreign-agents-and-undesirable>.
- Reuters*. 'Ethiopia Revokes Accreditation of Reuters Journalists'. *Media & Telecom*. 14 February 2026. <https://www.reuters.com/business/media-telecom/ethiopia-revokes-accreditation-reuters-journalists-2026-02-14/>.
- Reynaud, Florian, and Phineas Rueckert. 'Au Rwanda, opposants et proches du régime ciblés par le logiciel espion Pegasus pendant des années'. *International, Pixels. Le Monde*, 29 May 2024. https://www.lemonde.fr/international/article/2024/05/29/au-rwanda-opposants-et-proches-du-regime-cibles-par-le-logiciel-espion-pegasus-pendant-des-annees_6236172_3210.html.

- Roberts, Margaret. *Censored: Distraction and Diversion Inside China's Great Firewall*. Princeton University Press, 2018. <https://doi.org/10.23943/9781400890057>.
- Roshchin, Mikhail Komin, Evgeny. 'An Ecosystem of Truth: Russian Independent Media in Exile'. *CEPA*, 25 June 2026. <https://cepa.org/comprehensive-reports/an-ecosystem-of-truth-russian-independent-media-in-exile/>.
- RSF. 'Journalists' Families Increasingly Targeted with Intimidation Tactics by Repressive Regimes | RSF'. 31 March 2026. <https://rsf.org/en/journalists-families-increasingly-targeted-intimidation-tactics-repressive-regimes>.
- RSF. 'RSF Condemns NYT Reporter's Unprecedented Expulsion from Ethiopia'. 21 May 2021. <https://rsf.org/en/rsf-condemns-nyt-reporter-s-unprecedented-expulsion-ethiopia>.
- Russian Network That 'paid European Politicians' Busted, Authorities Claim*. 28 March 2024. <https://www.bbc.com/news/world-europe-68685604>.
- 'Russian Newspaper Novaya Gazeta Suspends Publication Following Official Warning'. *Committee to Protect Journalists*, 28 March 2022. <https://cpj.org/2022/03/russian-newspaper-novaya-gazeta-suspends-publication-following-official-warning/>.
- 'Rwandan Authorities Chose Thousands of Activists, Journalists and Politicians to Target with NSO Spyware'. *Amnesty International*, 19 July 2021. <https://www.amnesty.org/en/latest/press-release/2021/07/rwandan-authorities-chose-thousands-of-activists-journalists-and-politicians-to-target-with-nso-spyware/>.
- Schenkkan, Nate, Zselyke Csaky, Emile Dirks, and Alexander Dukalskis. *Perpetrators and Methods of Transnational Repression and Possible Counter Strategies*. n.d.
- Schliebs, M., H. Bailey, J. Bright, and P. N. Howard. *China's Public Diplomacy Operations: Understanding Engagement and Inauthentic Amplification of PRC Diplomats on Facebook and Twitter*. Programme on Democracy and Technology, Oxford University, 2021. <https://ora.ox.ac.uk/objects/uuid:427320a1-c677-40d4-b4a5-1759e563e7ed>.
- Tesfaye, Amanuel, and Matti Pohjonen. *AI and Visual Propaganda in Ethiopia's Red Sea Discourse*. n.d. Accessed 24 August 2026. <https://www.arm-project.eu/publication/ai-and-visual-propaganda-in-ethiopias-red-sea-discourse/>.
- Tesfaye Kebede, Amanuel. 'Ethiopia's Urban Renewal Projects and Turn toward Aesthetic Propaganda'. *Global Voices*, 11 March 2026. <https://globalvoices.org/2026/03/11/aesthetic-propaganda-ethiopias-urban-renewal-projects-and-the-visual-turn-in-digital-authoritarianism/>.
- 'The Bucha Massacre: Mapping a Year of Kremlin Denial - Representation in Ireland'. Accessed 28 August 2026. https://ireland.representation.ec.europa.eu/news-and-events/news/bucha-massacre-mapping-year-kremlin-denial-2023-04-03-0_en.

- The Economist Group. 'Press Statement: The Economist'. Accessed 24 August 2026.
<https://www.economistgroup.com/press-centre/the-economist/press-statement-the-economist>.
- Thomson, Susan M. "'That Is Not What We Authorised You to Do ... ": Access and Government Interference in Highly Politicised Research Environments'. In *Surviving Field Research*. Routledge, 2009.
- Times, The Moscow. 'Ex-Pussy Riot Member Says She Helped the FSB Spy on Kremlin Critics'. The Moscow Times, 24 August 2026.
<https://www.themoscowtimes.com/2026/08/24/ex-pussy-riot-member-says-she-helped-the-fsb-spy-on-kremlin-critics-a93568>.
- Tracy, Marc. 'Inside The Wall Street Journal, Tensions Rise Over "Sick Man" China Headline'. Business. *The New York Times*, 23 February 2020.
<https://www.nytimes.com/2020/02/22/business/media/wall-street-journal-sick-man-china-headline.html>.
- Tsourapas, Gerasimos. 'Global Autocracies: Strategies of Transnational Repression, Legitimation, and Co-Optation in World Politics'. *International Studies Review* 23, no. 3 (2021): 616–44. <https://doi.org/10.1093/isr/viaa061>.
- Vendil Pallin, Carolina. 'Internet Control through Ownership: The Case of Russia'. *Post-Soviet Affairs* 33, no. 1 (2017): 16–33.
<https://doi.org/10.1080/1060586X.2015.1121712>.
- Weiss, Michael. 'Blood Simple. Several Russian Journalists and Activists Were Poisoned in Europe'. The Insider, 15 August 2023. <https://theins.press/en/politics/264280>.
- Zhang, Albert, and Jacob Wallis. *Trigger Warning: The CCP's Coordinated Information Effort to Discredit the BBC*. Australian Strategic Policy Institute, 2021.
<https://www.jstor.org/stable/resrep29690>.