

D6.3 Catalogue of TTPs

Version 1 – 30 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 6.3	D6.3 CATALOGUE OF TTPS
Related Work Package	WP6
Deliverable Lead	WZB
Authors	Pauline Lemaire (CMI) Lisa Garbe (WZB) ARM Project Team
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	30 September 2026
Project Website	www.arm-project.eu

Funded by the European Union.

D6.3 Catalogue of the Tactics, Techniques and Procedures of Information Suppression

Funded by the European Union.

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 6.3	**CATALOGUE OF TTPS**
Related Work Package	WP6
Deliverable Lead	UiT
Author(s)	Pauline Lemaire & The ARM Project
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	30 September 2026

Table of Contents

1. Introduction 5

2. Production-stage TTPs 7

2.1 Tactic 1. Restricting access to locations and data sources. 7

2.1.1 Visa denials or non-renewals; accreditation refusals 7

2.1.2 Leverage strict requirements to secure permits, visas, or licences 8

2.1.3 Restricting access to source material or data 9

2.2 Tactic 2. Extra-legal intimidation. 11

2.2.1 Direct threats 11

2.2.2 Indirect threats 12

2.3 Tactic 3. Legal/regulatory deterrence. 13

2.3.1 Restrictive legislation on certain topics 13

2.3.2 Legislation stigmatising or criminalising specific actors 13

2.4 Tactic 4. Surveillance and monitoring of producers 14

2.4.1 Digital Surveillance 14

2.4.2 In-person surveillance 15

2.4.3 Direct requests for interviewee lists or research notes 16

2.5 Tactic 5. Media capture. 17

2.5.1 Influencing who manages and runs an outlet 17

3. Dissemination-stage TTPs 18

3.1 Tactic 1. Undermining the credibility of producers 18

3.1.1 Sustained harassment and smear campaigns 18

3.1.2 Leverage networks of supporters abroad to co-sign open letters and petitions 19

3.2 Tactic 2. Media capture. 20

3.2.1 Coercing company behaviour 20

3.3 Tactic 3. Extending domestic legal jurisdiction over audiences abroad. 20

3.3.1 Extending data and privacy law beyond domestic territory 20

3.3.2 Exporting censorship criteria via domestically grown platforms 21

3.4 Tactic 4. Legal and regulatory deterrence. 21

3.4.1 Lawfare 22

Funded by the European Union.

3.5 Tactic 5. Influencing platform moderation policies....22
3.5.1 Algorithmic manipulation or mass reporting....22
4. Salience-stage TTPs....23
4.1 Tactic 1. Burying information and reducing its visibility....23
4.1.1 Flooding....23
4.1.2 Norms and social pressure....24
4.2 Tactic 2. Amplifying pro-government narratives....25
4.2.1 Flooding....25
4.2.2 Crafting engaging messages....26
4.2.3 Disguised or covert news outlets....26
4.3 Tactic 3. Undermining the credibility of producers....27
4.3.1 Co-opting the language of fact-checking....27
4.3.2 Coordinated smear campaigns....28
5. References....30

1. Introduction

This catalogue systematically presents the tactics and techniques of information suppression that were identified over the course of the ARM project. It builds upon four cases studies (China, Russia, Rwanda, and Ethiopia). The catalogue does not claim to be exhaustive, as new techniques are constantly adopted. Rather, its purpose is to present an overview of what we were able to identify, so that it can serve as a reference to researchers and analysts in the field of Foreign Information Manipulation and Interference (FIMI) when they analyse FIMI incidents. It can also be a useful tool for human rights defenders, journalists, or researchers who are trying to identify whether they are targeted by information suppression, as it presents a collection of examples that can serve to support reflections.

WHAT IS INFORMATION SUPPRESSION

This catalogue considers that information suppression is "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.[1]" Information suppression can include practices such as censorship (for example when targeting foreign journalists or researchers who seek to enter a country), but it defers from censorship in so far as there must be a transnational dimension. Repression targeting local journalists in their own country is censorship, but not information suppression. Information suppression can also include practices of transnational repression – when a regime represses its own citizens beyond its borders – but only in so far as information or knowledge is being targeted (for example, when journalists in exile are targeted, but not when an entire community is monitored). Many practitioners choose to use the expression "Transnational Information Suppression".[2]

WHAT ARE TACTICS, TECHNIQUES, AND PROCEDURES (TTPS)

When describing information suppression, the catalogue uses the vocabulary of Tactics and Techniques. This comes from the term "Tactics, Techniques, and Procedures" (TTPs) from the field of cybersecurity. TTPs are used by analysts to identify and analyse the actions of actors conducting Foreign Information Manipulation and Interference (FIMI) operations.

Tactics are the operational goals that actors are trying to accomplish. This is used to describe stages of an information campaign. Techniques are the actions taken to accomplish

[1] Aalen et al., *Information Suppression: Does It Belong to FIMI?*, 19.
[2] EEAS, *4th Report on Foreign Information Manipulation and Interference Dismantling the FIMI House of Cards*, 4.

tactics. Procedures are the specific combination of techniques across multiple tactics that indicate intent and may be unique for different actors[3]. The present catalogue focuses on tactics and techniques of information suppression, as these are the most useful tools to unpack information suppression incidents. In line with what most practitioners do, we use the expression TTPs, even if we only discuss tactics and techniques.

HOW THIS CATALOGUE IS ORGANISED

The catalogue is organised around the three stages of the information cycle: production, dissemination, and salience. The production stage describes all aspects linked to the production of information or knowledge: collecting documents, conducting interviews or survey data for example, as well as being able to travel or to film. The dissemination stage covers activities linked to disseminating information (or knowledge), including publishing, teaching, or sharing on social media for example. The salience stage describes the visibility of information. Activities to limit (or suppress) the visibility of information frequently occur online, and are often related to propaganda: spreading counternarratives, or diversionary stories, to drown critical information and make it difficult to find.

These stages of the information cycle offer a useful entry point to identify tactics and techniques for information practitioners, who can start from an incident to reflect on the stage at which it occurs before consulting the catalogue. It is also useful for analysts looking to identify tactics or techniques they might not have considered before by focusing on information itself, rather than on a specific type of incident.

Each tactic is then presented, and specific techniques are organised along the tactics to which they correspond. Note that the same technique can be used to accomplish different goals (or tactics), and that the same tactic can be used at different stages of the information cycle. In those cases, the technique or tactic is reproduced and described in multiple places. Each technique presented includes the typical perpetrators that are involved, the typical targets, and the potential impact of the technique on information. This is accompanied by an example from each of the case countries where it was observed.

HOW TTPS WERE IDENTIFIED

Evidence was collected through desk-based research, drawing from reports by civil society organisations, media reports, and academic literature. This desk-based research was followed by in-depth interviews with journalists, researchers, and members of the relevant diasporas as well as the qualitative and quantitative analysis of social media posts. In the case of China, evidence also includes findings from a survey among China experts, while in

[3] EEAS, *1st EEAS Report on Foreign Information Manipulation and Interference Threats. Towards a Framework for Networked Defence*.

the case of Russia, we also draw on focus group discussions with Russophone communities in Latvia and Estonia.

2. Production-stage TTPs

TTPs that affect information or knowledge at the production stage typically occur before or as it is produced, targeting information producers, and making their work more difficult. They are usually identified through interviews, surveys, or through personal accounts, as they are most often not observed by those who do not experience them directly.

2.1 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. This tactic degrades the quality and scope of research and reporting. State authorities leverage their discretionary powers to restrict what can be investigated, but also to encourage self-censorship as they can influence research topics or the angle of investigations.

2.1.1 Visa denials or non-renewals; accreditation refusals

This is the most direct technique: state authorities deny a visa, refuse to renew it, or deny specific accreditations (for the press for example).

Actors: State authorities: Bureaucrats (at embassies or ministries); border control officers;
Targets: Individuals who produce information or knowledge: journalists; academics; other researchers in the civil society sector.
Impact: Reliable first-hand accounts become difficult to get, affecting the quality of information and knowledge produced. This also affects what can be researched or covered. It can also lead to self-censorship, for example choosing specific angles or topics to protect one's prospects to return to the country later.

CHINA:
According to a survey run in the Winter 2025, 3% of academic researchers and 9% of non-academic researchers focusing on China report visa denials.[4]

RUSSIA:
Several foreign correspondents lost or were denied accreditation.[5] In August 2021, a senior BBC journalist in Moscow was expelled from Russia when the country refused to extend her accreditation. Russian authorities presented the decision as a response to refusals or delays by the British authorities to issue visas to Russian journalists. This incident is not isolated, and other foreign journalists have been expelled in the same way, for example a Spanish journalist working for El Mundo was expelled in 2024.[6]

RWANDA
In Rwanda, a Human Rights Watch researcher was barred from entering in the country in 2024.[7] This is the fourth researcher from that organisation who has been denied entry since 2008. An academic researcher reported having been told their visa was invalid upon arriving in Rwanda, following a critical presentation she had made at a conference.[8]

ETHIOPIA
In Ethiopia, since 2020, journalists for Reuters, the New York Times and the Economist saw their accreditation suspended, while a French journalist was detained in 2024, and another French journalist was expelled that same year[9]

2.1.2 Leverage strict requirements to secure permits, visas, or licences

This is a more indirect variant of the same tactic. State authorities implement strict and complex procedures to secure research permits, visas, or licenses. Instead of directly denying access, creating administrative hurdles makes the work of journalists and researchers more difficult or, in some cases, impossible.

Actors: State authorities, bureaucrats.
Targets: Individuals who produce information or knowledge: journalists; academics; other researchers in the civil society sector.

[4] ARM Project, *China's Information Control Practices*, 12.
[5] Juzefovičs et al., *Russian Information Suppression as FIMI*, 19.
[6] *Reuters*, 'Russia Declines to Renew Visa of Spanish Reporter for El Mundo'.
[7] Human Rights Watch, *Human Rights Watch Submission to the Universal Periodic Review of Rwanda (51st Session)*, 2.
[8] Jessee, 'Rwanda's Subtle Forms of Intimidation', 2013.
[9] Garbe et al., *Comparing Transnational Information Suppression: A Comparison of Information Suppression Tactics across China, Russia, Ethiopia, and Rwanda*, 17.

Impact: This affects what can be researched or covered. It can lead to self-censorship, for example choosing specific angles or topics to protect one's prospect to return to the country later. It can also be a deterrent, discouraging researchers and journalists from engaging in complex processes.

CHINAERROR! BOOKMARK NOT DEFINED.
According to the winter 2025 survey, 7% of surveyed academics and 14% of non-academic researchers reported having struggled to get a visa due to bureaucratic hurdles.[10]

RWANDA
Rwanda requires researchers to apply for permits at least three months in advance through a process that varies by research type and ministry. The process also requires being in the country to be completed, and researchers have reported on how complex they experienced the process to be, and how it influenced what they could or could not do in the country.[11]

ETHIOPIA
Ethiopia combines the deliberately onerous annual renewal of media licenses with the denial of access to conflict zones, as observed in Tigray[12].

2.1.3 Restricting access to source material or data

Access can also be constrained at the level of sources, rather than locations. For example, this includes restricting access to archives, libraries, surveys, or census data. This type of restriction affects investigations and research that depends on documentary records instead of or in addition to traveling to locations.

Actors: State authorities, bureaucrats.
Targets: Individuals who produce information or knowledge: journalists; academics; other researchers in the civil society sector.
Impact: This affects the quality of research and reporting, as it limits what can be verified (in the case of investigations that triangulate between testimonials and documents). It can also affect the topics that can be covered.

[10] ARM Project, *China's Information Control Practices*, 12.
[11] Jessee, 'Conducting Fieldwork in Rwanda'; Loyle, 'Overcoming Research Obstacles in Hybrid Regimes'; Jessee, 'Rwanda's Subtle Forms of Intimidation', 19 December 2013.
[12] Pohjonen et al., *Information Suppression in Ethiopia* (ARM Project, 2026), 16–17.

CHINA

3% of non-academic researchers and 14% of academic researchers surveyed in winter 2025 report having been denied entry to a library, archive, or specific materials.[13]

RUSSIA

Russia has restricted access to archival sources (e.g. on state repression) and various types of governmental data, including key economic and demographic data as well as court statistics.[14]

RWANDA

Access to data is limited in two ways. First, the country's legislation on the Right to Information Law makes it possible to refuse access to information on grounds that lack precise limits, and there are no provisions for how one can complain if a demand is rejected.[15] Second, researchers report difficulties in accessing opinion surveys or census data[16], while others have doubts as to whether the data they do manage to access has been manipulated[17].

ETHIOPIA

Ethiopia's 2026 Access to Information Proclamation enables the government to deny access to a broadly defined category of information related to 'enemies and insurgents'.[18] Together with the 2025 Disaster Risk Management Proclamation, which prohibits 'providing false information or making exaggerated requests with the intention of procuring humanitarian aid',[19] the production of information critical to the government's handling of conflicts and disasters is effectively suppressed. Denial of access to information is a routine bureaucratic practice, with government offices obstructing or refusing requests outright.[20]

---

[13] ARM Project, *China's Information Control Practices*, 12.
[14] 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
[15] Never Again Rwanda and Citizen Rights and Development, 'Republic of Rwanda Joint Submission to the UN Universal Periodic Review Fourth Cycle of the UPR Working Group'.
[16] Loyle, 'Overcoming Research Obstacles in Hybrid Regimes'.
[17] Ansoms et al., 'Statistics versus Livelihoods'; Reyntjens, 'Lies, Damned Lies and Statistics'.
[18] Endale, 'Freedom Of Information Bill Draws Fire From Opposition MPs'.
[19] Ethiopian Disaster Risk Management Proclamation No. 1386/2025.
[20] Pohjonen et al., *Information Suppression in Ethiopia* (ARM Project, 2026), 16–17.

2.2 Tactic 2. Extra-legal intimidation.

Threats delivered directly or through intermediaries to those who produce information without formal legal process. Such threats produce fear and can discourage people from producing or continuing critical work.

2.2.1 Direct threats

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.

Actors: State authorities as well as private individuals supporting the regime.
Targets: Individuals who produce information or knowledge: journalists; academics; other researchers in the civil society sector, including from the diaspora.
Impact: Threats can induce fear and encourage information producers to adjust their angle, reformulate their findings, change their focus, or abandon their work.

CHINA

China researchers report facing pressures in the form of being interviewed by the authorities ("being invited for tea") or being invited to cooperate with the authorities.[21]

RWANDA

These types of threats have taken the form of government representatives warning researchers in person against returning to the country after a public presentation touching on sensitive topics.[22]

ETHIOPIA

Foreign academics facing direct threats, being labelled an enemy by government authorities, or receiving death threats from individuals.[23]

RUSSIA

Threats can take the shape of official warnings that push outlets toward self-censorship or closure.[24] Other forms of threats include direct encounters with security services in which

[21] ARM Project, *China's Information Control Practices*, 12,16.
[22] Jessee, 'Rwanda's Subtle Forms of Intimidation', 2013.
[23] Pohjonen et al., *Information Suppression in Ethiopia* (2026), 20; Kruhaug, 'Norsk Professor Trues På Livet Av Etiopiere: – Det Pågår En Aktiv, Koordinert Hatkampanje Mot Meg'.
[24] 'Russian Newspaper Novaya Gazeta Suspends Publication Following Official Warning'.

journalists are questioned and cautioned in person.[25] In the case of Russia, more aggressive tactics, including assassination attempts (abroad), have also been recorded.[26] Russian journalists in exile have been particularly targeted.[27]

2.2.2 Indirect threats

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 while leaving no formal record against the target.

Actors: State authorities; other individuals.
Targets: Information producers are the main target, but their personal networks are targeted to reach them.
Impact: Indirect threats induce fear within the personal network of information producers, who can then pressure them to abandon their work. It also isolates information producers. They are difficult to document and easily deniable, and can lead to adjustments in the work, including softening findings or changing angle.

CHINA

27% of the surveyed academic researchers report that state authorities have contacted their friends or acquaintances, while it is also the case for 20% of the surveyed non-academic researchers.[28]

RUSSIA

Russian journalists in exile have seen their family members being threatened by the authorities, including in cases where the authorities searched the homes of their parents[29]

RWANDA

Indirect threats in Rwanda can surface by implication during fieldwork, where stories about what befell earlier critics leave the researcher to infer the risks.[30]

[25] CPJ Europe and Central Asia, 'Russia's Repression Record'.
[26] Weiss, 'Blood Simple. Several Russian Journalists and Activists Were Poisoned in Europe'.
[27] RSF, 'Journalists' Families Increasingly Targeted with Intimidation Tactics by Repressive Regimes | RSF'; CPJ Europe and Central Asia, 'Russia's Repression Record'.
[28] ARM Project, *China's Information Control Practices*, 12.
[29] CPJ Europe and Central Asia, 'Russia's Repression Record'.
[30] Jessee, 'The Danger of a Single Story'.

2.3 Tactic 3. Legal/regulatory deterrence.

Broad or vaguely worded legislation raises the legal risk of covering certain topics, deterring information producers from investigating these topics, even without issuing direct threats. While primarily directed at domestic targets, this can also affect international producers.

2.3.1 Restrictive legislation on certain topics

Legislation targeting terrorism, hate speech, media, civil society, or emergency powers, if worded broadly or vaguely, can make an entire topic legally risky to cover, so that the information cannot actually be produced.
Actors: State authorities
Targets: Information producers such as journalists and researchers, including those in exile.
Impact: Certain topics or issues become too risky to cover, and information is not produced.

RWANDA

Genocide-ideology and sectarianism laws lack clear safeguards, leaving their scope open to interpretation, deterring investigations that would for example focus on the possible legacies of the genocide.[31]

ETHIOPIA

This technique 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.[32] The 2026 Access to Information proclamation enlarges the government's opportunity to criminalise the spread of information related to security and insurgency.

2.3.2 Legislation stigmatising or criminalising specific actors

Legislation that criminalises or stigmatises the status of actors based on characteristics such as foreign ties (funding or affiliation) or on access to information, so that their entire output becomes risky regardless of topic.
Actors: State authorities
Targets: Information producers
Impact: If information producers themselves are criminalised, then they become unable to conduct their activities. If potential sources of information are criminalised and stigmatised, then producers are deterred from engaging with these sources, and from covering the topic.

[31] Michalakea et al., *Information Suppression in Rwanda*, 13.
[32] Pohjonen et al., *Information Suppression in Ethiopia* (ARM Project, 2026), 19.

CHINA

The 2023 Counter-Espionage Law broadened the definition of espionage and made it vaguer. This law attaches legal risk to gathering or transmitting information deemed relevant to national security, leaving foreign businesses, NGOs with foreign donors or foreign staff, journalists, and researchers unsure where the line falls and inclined to avoid sensitive subjects altogether.[33]

RUSSIA

The 2012 "foreign agent" and 2015 "undesirable organisations" laws 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.[34]

2.4 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.

2.4.1 Digital Surveillance

Regimes deploy spyware against critics and their contacts, giving them access to a target's communications, location, and devices.
Actors: State authorities including law enforcement or intelligence services
Targets: Information producers including journalists, researchers from civil society organisations or academia, including diasporas and exiles.
Impact: The digital surveillance of those who produce knowledge and information, or of their contacts, enables other suppression activities (such as threats). If the information producer becomes aware of digital surveillance, it can also lead to self-censorship.

[33] McCarthy and Gan, 'China Has Widened Its Counter-Espionage Law. Experts Say Foreign Businesses Should Be Worried'.
[34] Reporters Without Borders (RSF), *Independent Media Are the Primary Targets of Kremlin Laws against 'Foreign Agents' and 'Undesirable Organisations'*.

CHINA

In China, LightSpy, a modular phone implant spread by watering-hole attacks was used against iOS users in Hong Kong and is linked to China-based operators.[35]

RUSSIA

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.[36] Spyware Pegasus was also found on the devices of Russian journalists in exile in Latvia and Lithuania.[37]

RWANDA

The regime famously used NSO's software Pegasus against journalists and opposition figures in exile, as well as against journalists and foreign officials.[38] NSO, the company behind the software, confirmed in 2024 that it has not had users in Rwanda since 2021[39].

ETHIOPIA

The use of surveillance software to monitor the activities of Ethiopians abroad has also been documented by the Citizen Lab[40]. A series of surveillance software are used to target diasporic media in the United States, researchers in the United Kingdom and the United States, as well as other individuals in Germany for example.

2.4.2 In-person surveillance

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.
Actors: State authorities; individuals coerced or paid to act as informants
Targets: Journalists, researchers from civil society organisations, academic researchers
Impact: This technique enables other techniques of suppression, such as designing effective

[35] Cao et al., *Operation Poisoned News: Hong Kong Users Targeted with Mobile Malware via Local News Links*.
[36] Quintin et al., *Something to Remember Us By: Device Confiscated by Russian Authorities Returned with Monokle-Type Spyware Installed*.
[37] 'Exiled, Then Spied On'.
[38] Amnesty International, *Rwandan Authorities Chose Thousands of Activists, Journalists and Politicians to Target with NSO Spyware*.
[39] Reynaud and Rueckert, 'Au Rwanda, opposants et proches du régime ciblés par le logiciel espion Pegasus pendant des années'.
[40] Marczak et al., *Champing at the Cyberbit: Ethiopian Dissidents Targeted with New Commercial Spyware*.

threats. It can be hard to detect, but if the information producer is aware of it, it can also influence their willingness to produce critical coverage.

CHINA

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 diffused, but sometimes deliberately overt as visibility itself serves as an intimidation function.[41]

RWANDA

In Rwanda, local contacts and researchers' host organisations are frequently pressured to monitor activities, as are the fixers of journalists. Surveillance is generally experienced as more diffused. Producers often only realise what has been going on at a later stage.[42]

RUSSIA

Russia actively seeks to infiltrate activist circles, both domestically and internationally, often employing coercion.[43]

2.4.3 Direct requests for interviewee lists or research notes

This more intrusive form goes after the record of the work itself, with officials asking for or seizing research notes and interviewee lists.

Actors: State authorities

Targets: Journalists and researchers

Impact: These types of requests act as pressure to limit or influence coverage of a topic. It can also make it impossible to produce information and knowledge in the case of seizures. Importantly, it also exposes informants and sources to repression.

CHINA

Officials have been known to confiscate notes and computers of researchers.[44]

[41] Dukalskis, 'Controlling Critical Messengers: Foreign Correspondents in China'; Lim, 'Foreign Correspondence in China'.
[42] Michalakea et al., *Information Suppression in Rwanda*, 16.
[43] Times, 'Ex-Pussy Riot Member Says She Helped the FSB Spy on Kremlin Critics'.
[44] ARM Project, *China's Information Control Practices*, 12.

RWANDA

Researchers have reported being asked to regularly submit the lists of those they wanted to interview or had interviewed, or to share their research notes.[45]

2.5 Tactic 5. Media capture.

State authorities can secure direct influence over who owns or manages a media outlet.

2.5.1 Influencing who manages and runs an outlet

State authorities secure direct influence over who manages and runs an outlet by taking control of a media outlet.
Actors: State authorities or aligned individuals
Targets: Media outlets
Impact: Authorities can influence what the media is willing to produce or cover, independent of journalists' risk appetite.

CHINA

This operates through Chinese-owned international outlets. Despite being run by international managers and including international journalists, the ownership structure means these outlets reflect the perspective of the Chinese state.[46]

RUSSIA

In the case of Russia, this is observable for outlets behind which Russian authorities stand, such as RT Balkan,[47] as well as through ownership transfers that move existing platforms into the hands of state-aligned owners. For example, this is the case for Yandex which ceded its news aggregator and homepage to VK, itself controlled through a holding tied to a close associate of Putin.[48]

[45] Thomson, '"That Is Not What We Authorised You to Do … "'.
[46] ARM Project, *China's Information Control Practices*, 40.
[47] Juzefovičs et al., *Russian Information Suppression as FIMI*, 18.
[48] Vendil Pallin, 'Internet Control through Ownership', 24–25; Kravets-Meinke, 'The Sad Fate of Yandex: From Independent Tech Startup to Kremlin Propaganda Tool'.

3. Dissemination-stage TTPs

Dissemination-stage TTPs prevent information 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. Note that tactics that can target the producing of information can also target its dissemination.

3.1 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.

3.1.1 Sustained harassment and smear campaigns

Sustained harassment and smear campaigns including dogpiling are the most common techniques observed to undermine the credibility of producers and outlets.
Actors: State authorities; paid individuals (influencers); aligned individuals
Targets: Information producers and their organisations
Impact: Such campaigns can affect the reach of critical information by dismissing its quality, creating doubts for audiences. A secondary effect is that it can also affect the willingness of journalists and researchers to continue their work, leading to downstream reduction in the production of new information on sensitive topics.

CHINA

These types of campaigns in the context of China involve personal insults, character assassination, and coordinated harassment directed at diaspora-based academics.[49] I

RUSSIA

Smear campaigns target international information producers, as in the case of a Finnish investigative journalist where Russian troll factories spun an old minor drug conviction to paint them as a drug dealer.[50]

[49] ARM Project, *China's Information Control Practices*, 15–16.
[50] Juzefovičs et al., *Russian Information Suppression as FIMI*, 11.

RWANDA

The Rwandan regime has a history of organising discrediting campaigns around critical publications[51], including a bot- and AI-imagery-assisted campaign against those involved in an investigation of state repression in Rwanda published across several European outlets.[52]

ETHIOPIA

Such campaigns in the Ethiopian context have targeted foreign academics[53]. One of them faced a widespread smear campaign following their analysis of the war in Tigray, which included accusations by Ethiopian intelligence services of being paid by an opposition group. The campaign led to the cancellation of public events where the academic was supposed to participate.[54]

3.1.2 Leverage networks of supporters abroad to co-sign open letters and petitions

A second form mobilises aligned private individuals to co-sign open letters and petitions that discredit critical reporting.
Actors: Aligned individuals, sometimes recognised journalists or academics
Targets: Journalists, other information producers and their organisations
Impact: These types of activities can sow doubts regarding the quality and validity of critical information or knowledge, slowing the dissemination of the piece. It can also deter information producers from covering similar topics again, to avoid losing credibility.

CHINA

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.[55]

RWANDA

This technique was used when academics and journalists co-signed a statement attacking an investigation shedding light on the repressive character of the Rwandan regime. The

[51] Dukalskis, *Making the World Safe for Dictatorship*, 147.
Michalakea et al., *Information Suppression in Rwanda*, 22; Wack et al., *Old Despots, New Tricks - An AI-Empowered Pro-Kagame/RPF Coordinated Influence Network on X*.[52]
[53] Pohjonen et al., *Information Suppression in Ethiopia* (2026), 20.
[54] Kruhaug, 'Norsk Professor Trues På Livet Av Etiopiere: – Det Pågår En Aktiv, Koordinert Hatkampanje Mot Meg'.
[55] Tracy, 'Inside The Wall Street Journal, Tensions Rise Over "Sick Man" China Headline'.

statement attacked the investigation for relying too heavily on the testimony of genocide perpetrators, and for being “old news”.[56]

3.2 Tactic 2. Media capture.

State authorities or actors aligned with the state take control of media outlets or platform companies.

3.2.1 Coercing company behaviour

Through state-company partnerships, the state coerces a platform or company into disciplining its own conduct.
Actors: State authorities or aligned actors; media outlets or platforms once captured.
Targets: Media outlets; once those are captured, critical information itself.
Impact: Captured companies enforce informal restrictions and policies, limiting the availability of critical content for users or audiences.

CHINA

In China, after CEO Jack Ma's 2020 fall from grace, his company, Alibaba began policing itself, so that minimal state pressure now keeps it aligned with the state's preferences.[57]

3.3 Tactic 3. Extending domestic legal jurisdiction over audiences abroad.

Domestic law and platform rules are extended to reach citizens abroad, so that diaspora audiences, and sometimes foreign citizens, are governed by home-country restrictions regardless of their physical location.

3.3.1 Extending data and privacy law beyond domestic territory

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.
Actors: State authorities and commercial intermediaries
Targets: Audiences in the diaspora
Impact: This makes it possible to apply the same kind of surveillance and control to those

[56] Michalakea et al., *Information Suppression in Rwanda*, 22.
[57] Keane, ‘China’s Record Fine against Alibaba Spells the End of Big Tech’s Romance with the State’.

citizens who reside abroad, for example limiting the kind of information citizens abroad can access.

CHINA
Users of Chinese-owned platforms who registered using a China-based phone number but reside abroad remain subject to domestic surveillance and censorship regardless of their place of residence.[58]

RUSSIA
Russia legislation requires that home-grown platforms such as VKontakte retain communications from Russian citizens regardless of their country of residence and surrender them to the FSB.[59]

3.3.2 Exporting censorship criteria via domestically grown platforms

National domestic censorship criteria leaks abroad through domestically grown platforms, so that overseas users meet home-country restrictions through the service itself.
Actors: State authorities via domestically grown companies (applying state legislation)
Targets: Platform users abroad, including from the diaspora
Impact: This limits the dissemination of unwanted information or knowledge about the regime among the diaspora as well as among foreign citizens outside the country's jurisdiction.

CHINA
China-grown platforms that also operate internationally have deployed dual terms-of-service regimes, to differentiate between Chinese and China-based users on the one hand, and international users on the other hand. However, research has documented that the international version of these platforms does tend to leak Chinese censorship criteria to users overseas.[60]

3.4 Tactic 4. Legal and regulatory deterrence.

Legal or regulatory provisions are leveraged against published information or knowledge that criticises the regime, or that is considered sensitive.

[58] Sherman, 'Russia Is Weaponizing Its Data Laws against Foreign Organizations'; Andreeva et al., *Data Localization Laws: Russian Federation*.
[59] Andreeva et al., *Data Localization Laws: Russian Federation*.
[60] ARM Project, *China's Information Control Practices*, 30–39.

3.4.1 Lawfare

Regimes and their supporters deploy SLAPP suits (Strategic Lawsuits Against Public Participation) and defamation or data-protection litigation to limit the dissemination of sensitive information or knowledge. The cost of defending a case suppresses critical work regardless of whether the underlying claim succeeds.
Actors: State authorities or private individuals who are aligned with the regime
Targets: Journalists, researchers, and publishers, including media outlets
Effects: Limits the dissemination of specific content (books, documentary films) and can also deter from conducting new investigations on similar topics.

RUSSIA
A telling example is the case of the series of lawsuits brought by Russian oligarchs and a Russia-owned company against the journalist Catherine Belton and her publisher over her book *Putin's People*.[61] This type of lawsuit (or here, series of lawsuits) is designed to be complex and costly, limiting the diffusion of the content, exhausting the author and publisher, and deterring further investigations on the topic.

RWANDA
A similar technique is used in the case of Rwanda, where regime-aligned individuals and organisations complained through genocide-denial complaints and lawsuits to pressure critics. This has been observed both in the UK, where the BBC's editorial complaint mechanism was used against a documentary, and through the French courts, where a lawsuit was launched against a journalist for denying the genocide.[62]

3.5 Tactic 5. Influencing platform moderation policies.

Influence or abuse platform moderation policies to ensure critical or sensitive information is removed from these platforms without direct state intervention.

3.5.1 Algorithmic manipulation or mass reporting

State-affiliated or state-aligned actors use algorithmic manipulation or coordinate to report critical content en masse, so that the platform itself removes it. There is no visible state intervention, meaning that the state can plausibly deny its involvement.

[61] Juzefovičs et al., *Russian Information Suppression as FIMI*, 13.
[62] Michalakea et al., *Information Suppression in Rwanda*, 23–24.

Actors: State authorities passing for private individuals; aligned private individuals
Target: Media outlets or online platforms
Impact: Information or knowledge that is critical of the regime is downgraded by the platform, which does not show the content to other users or takes it down. This can also facilitate the dissemination of propaganda instead.

ETHIOPIA

Coordinated mass reporting was used during the Tigray war to trigger Twitter's moderation systems against critical content and force its removal, including via the use of campaigns calling users to report specific content.[63]

4. Salience-stage TTPs

Salience-stage TTPs affect the circulation of information or knowledge at a large scale, preventing it from being noticed by burying it beneath a larger volume of competing information. These TTPs can be very close to those of disinformation and are, in fact, often conflated with them. Such TTPs also concern information suppression when they do lead to critical information being buried and less visible.

4.1 Tactic 1. Burying information and reducing its visibility.

Instead of removing critical content, regimes reduce its visibility using techniques that rely on mass sharing of other types of content, or leveraging norms around what is acceptable to share and discuss publicly.

4.1.1 Flooding

Aligned actors flood the information space through coordinated social media campaigns, drowning critical content under a larger volume of unrelated posts so that audiences are less likely to encounter it.
Actors: State authorities and private individuals (sometimes unknowingly) sharing the content
Targets: Broader audiences, including diaspora
Impact: Information or knowledge becomes more difficult to find and is not seen by

[63] Pohjonen et al., *Information Suppression in Ethiopia* (ARM Project, 2026), 27–28.

audiences. This, in turn, affects its dissemination (if no one sees it, it is not shared further), and can discourage those who produce information from continuing, since it is not seen.

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.[64] This technique has been observed in the face of criticism of the human rights situation in the Xianjiang province: bursts of content showing the scenery and nature in the province were observed during periods when criticism was peaking abroad[65]

RUSSIA

Russia has actively sought to obstruct public understanding of its military actions and war crimes in Ukraine by disseminating many false or misleading narratives.[66]

4.1.2 Norms and social pressure

Aligned actors cultivate norms and social pressure that lead audiences to police their own speech.

Actors: State authorities and private individuals in the diaspora

Targets: Diaspora

Impact: Individuals abide by the norm and do not share critical information, thereby limiting its salience.

CHINA

Knowledge professionals in the Chinese diaspora 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.[67]

RWANDA

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

[64] King et al., 'How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, Not Engaged Argument'; Roberts, *Censored*.
[65] Alpermann and Malzer, '"In Other News"'.
[66] 'The Bucha Massacre'.
[67] ARM Project, *China's Information Control Practices*, 47.

smear campaigns or through anonymous phone calls to their employer or to family members, leading to high degrees of self-censorship.[68]

4.2 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.

4.2.1 Flooding

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.
Actors: State authorities; private individuals (sometimes unknowingly) sharing these messages
Targets: Global audiences and diaspora
Impact: Pro-regime narratives represent most of the content available on specific topics, burying other information and making it less accessible. This also means that more critical information is not disseminated further and can discourage the production of new information on the same topic.

CHINA

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.[69]

RWANDA

In the case of 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.[70]

ETHIOPIA

The Ethiopian regime used flooding to push its narrative and bury anti-war voices during the Tigray conflict, painting the West (broadly representing the US, EU/Europe, Western media,

[68] Michalakea et al., *Information Suppression in Rwanda*, 45–47.
[69] 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:*
[70] Michalakea et al., *Information Suppression in Rwanda*, 38–39.

and human rights organisations) as interventionist and neo-colonial, seeking to influence global perceptions and reduce pressure and potential punitive measures like sanctions. [71] AI-generated content was also used to popularize the government's agenda of securing access to the sea. [72]

4.2.2 Crafting engaging messages

The content of messages is tailored to foster engagement among broad communities, using visuals, memes, or emotionally charged language, sometimes using AI tools. This technique is used to better flood the information environment, as more engaging messages will be shared by more individuals, ensuring flooding campaigns are more effective.
Actors: State authorities (including paid influencers); state aligned individuals
Targets: Global audiences
Impact: Well-crafted messages are easily shared by audiences and are omnipresent in the information space, limiting the reach of unwanted or critical information.

CHINA

Memes have been observed coming from Chinese state-affiliated actors, as a type of strategic content for spreading discontent about democracy and its functioning.[73]

RUSSIA

Russophone Estonian influencers share satiric and sarcastic videos to propagate Russian propaganda[74].

RWANDA

This is observed in the case of Rwanda: imagery glorifying the Rwandan president and military is omnipresent in social media posts[75], while flooding campaigns also use memes and other imagery to engage users, for example during the M23 invasion of Goma in the Democratic Republic of Congo[76].

4.2.3 Disguised or covert news outlets

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

[71] Pohjonen et al., *Information Suppression in Ethiopia* (ARM Project, 2026), 31–32.
[72] Pohjonen et al., *Information Suppression in Ethiopia* (ARM Project, 2026), 37–38.
[73] Jacobs and Carley, '#WhatIsDemocracy'.
[74] Juzefovičs et al., *Russian Information Suppression as FIMI*, 38.
[75] Michalakea et al., *Information Suppression in Rwanda*, 27.
[76] Michalakea et al., *Information Suppression in Rwanda*, 39.

reporting.
Actors: State authorities or state-aligned actors
Targets: Global audiences
Impact: These techniques support the flooding of the information space, as such outlets help reinforce the perception that pro-government narratives are more independent than they really are, while also making sure the same narrative is omnipresent and outcompetes more critical narratives.

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.[77]

RUSSIA
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).[78]

4.3 Tactic 3. Undermining the credibility of producers.

State authorities and/or aligned individuals coordinate online to organise widespread messaging campaigns attacking information producers (or sometimes, media outlets), drowning their message and making it inaudible.

4.3.1 Co-opting the language of fact-checking

This technique consists of crafting narratives that adopt the same space as fact-checkers, but instead of citing reliable sources and unpacking information to verify it, messages push regime-aligned narratives, propagating disinformation and making information much less visible.
Actors: State authorities or aligned individuals
Targets: Journalists, researchers, and global audiences
Impact: Co-opting fact-checking dilutes critical information that does not reach audiences

[77] ARM Project, *China's Information Control Practices*, 44–45.
[78] 'Doppelganger - Media Clones Serving Russian Propaganda - EU DisinfoLab'; *Russian Network That 'paid European Politicians' Busted, Authorities Claim*.

and undermines the credibility of producers. Both reduce the salience of the piece of information, which gets demoted and does not reach audiences.

CHINA

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.[79]

ETHIOPIA

During the Tigray war (2020-2022), the Ethiopian government used a Twitter account dedicated to fact-checking to reframe the war as a “law-enforcement operation”, and to deny reports of humanitarian crises and documented evidence of atrocities.[80]

RUSSIA

Russia, has deployed a broad network of pseudo-factchecking social media accounts, websites, and TV channels, most recently used to deflect accusations about war crimes in Ukraine, but which had been used before to defend the regime’s response to Covid 19, and which it is now expanding beyond its borders.[81]

4.3.2 Coordinated smear campaigns

In some cases, smear campaigns (see technique “harassment and smear campaign”, which targets the dissemination stage, p18) involving aligned actors attain such scale that they dominate the information landscape. In those cases, they can affect salience if they become so dominant that it is all one can find about the targeted person.
Actors: State authorities and aligned private individuals
Targets: Journalists and researchers, outlets
Impact: Narratives mocking or criticising messengers become dominant, hiding unwanted or critical information.

[79] Alpermann and Malzer, ‘“In Other News”’.
[80] Pohjonen et al., *Information Suppression in Ethiopia* (ARM Project, 2026), 34.
[81] Alyukov and Zavadskaya, ‘“It’s Not That Simple, We Don’t Know the Whole Truth”’, 4–5.

CHINA

Foreign reporting on Xinjiang triggered coordinated discrediting campaigns combining state media, diplomats, and nationalist users. The BBC's coverage was met with a documented coordinated effort by the state-party to discredit the broadcaster, with individual researchers being subjected to an online harassment campaign.[82]

ETHIOPIA

During the Tigray war, a widespread campaign discrediting Amnesty International's reporting on a massacre in Axum – including a dedicated hashtag – was organised by pro-government actors on Twitter.[83]

RWANDA

This was also observed in online information campaigns relying on memes and caricatures to discredit public figures and distract from the events, as was the case during the M23 invasion of Goma in the DRC in early 2025.[84]

[82] Zhang and Wallis, *Trigger Warning*.
[83] Pohjonen et al., *Information Suppression in Ethiopia* (ARM Project, 2026), 33.
[84] Michalakea et al., *Information Suppression in Rwanda*, 30–31.

5. References

Aalen, Lovise, Pauline Lemaire, and Gabriele De Seta. *Information Suppression: Does It Belong to FIMI?* Working Paper D1.2. ARM Project, 2026.

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*, 6 May 2026, 1–25. https://doi.org/10.1017/S153759272610454X.

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

Ansoms, An, Esther Marijnen, Giuseppe Cioffo, and Jude Murison. 'Statistics versus Livelihoods: Questioning Rwanda's Pathway out of Poverty'. *Review of African Political Economy* 44, no. 151 (2017): 47–65. https://doi.org/10.1080/03056244.2016.1214119.

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.

CPJ Europe and Central Asia. 'Russia's Repression Record'. *Committee to Protect Journalists*, 17 February 2026. https://cpj.org/2026/02/russias-repression-record/.

‘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.

EEAS. *1st EEAS Report on Foreign Information Manipulation and Interference Threats. Towards a Framework for Networked Defence*. EU External Action Service, 2023. https://www.eeas.europa.eu/sites/default/files/documents/2023/EEAS-DataTeam-ThreatReport-2023..pdf.

EEAS. *4th Report on Foreign Information Manipulation and Interference Dismantling the FIMI House of Cards*. 2026.

Endale, Ashenafi. ‘Freedom Of Information Bill Draws Fire From Opposition MPs’. News. *The Reporter Ethiopia*, 11 April 2026. https://www.thereporterethiopia.com/50193/.

Ethiopian Disaster Risk Management Proclamation No. 1386/2025 (2025). https://www.refworld.org/legal/legislation/natlegbod/2025/en/150426.

‘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/.

Garbe, Lisa, Gunhild Hoogensen Gjørv, Amanuel Kebede, et al. *Comparing Transnational Information Suppression: A Comparison of Information Suppression Tactics across China, Russia, Ethiopia, and Rwanda*. D6.1. ARM Project, 2026.

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. ‘Conducting Fieldwork in Rwanda’. *Canadian Journal of Development Studies / Revue Canadienne d’études Du Développement* 33, no. 2 (2012): 266–74. https://doi.org/10.1080/02255189.2012.687356.

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. ‘Rwanda’s Subtle Forms of Intimidation’. Times Higher Education, 19 December 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.

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.

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.

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.

Marczak, Bill, Geoffrey Alexander, Sarah McKune, John Scott-Railton, and Ron Deibert. *Champing at the Cyberbit: Ethiopian Dissidents Targeted with New Commercial Spyware*. The Citizen Lab, 2017. https://citizenlab.ca/research/champing-cyberbit-ethiopian-dissidents-targeted-commercial-spyware/.

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.

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.

Never Again Rwanda and Citizen Rights and Development. 'Republic of Rwanda Joint Submission to the UN Universal Periodic Review Fourth Cycle of the UPR Working Group'. 17 July 2025. https://uprdoc.ohchr.org/uprweb/downloadfile.aspx?filename=15144&file=EnglishTranslation.

Pohjonen, Matti, Amanuel Kebede, and Lovise Aalen. *Information Suppression in Ethiopia*. ARM Working Paper. 2026.

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. 'Russia Declines to Renew Visa of Spanish Reporter for El Mundo'. Europe. 21 March 2024. https://www.reuters.com/world/europe/russia-declines-renew-visa-spanish-reporter-el-mundo-2024-03-21/.

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.

Reyntjens, Filip. 'Lies, Damned Lies and Statistics: Poverty Reduction Rwandan-Style and How the Aid Community Loves It'. *African Arguments*, 3 November 2015. https://africanarguments.org/2015/11/lies-damned-lies-and-statistics-poverty-reduction-rwandan-style-and-how-the-aid-community-loves-it/.

Roberts, Margaret. *Censored: Distraction and Diversion Inside China's Great Firewall*. Princeton University Press, 2018. https://doi.org/10.23943/9781400890057.

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.

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/.

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.

Sherman, Justin. ‘Russia Is Weaponizing Its Data Laws against Foreign Organizations’. *Brookings*, 27 September 2022. https://www.brookings.edu/articles/russia-is-weaponizing-its-data-laws-against-foreign-organizations/.

‘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.

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.

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.

Wack, Morgan, Darren Linvill, and Patrick Warren. *Old Despots, New Tricks - An AI-Empowered Pro-Kagame/RPF Coordinated Influence Network on X*. No. 5. Media Forensics Hub Reports. 2024. https://open.clemson.edu/mfh_reports/5/.

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.