# REPRESSION WITHOUT BORDERS

## TRANSNATIONAL AUTHORITARIANISM IN THE DIGITAL AGE

Human constanta

This report is authored by Katsiaryna Pushkarova and Tatsiana Ziniakova and published by Human Constanta, with cover design by Kseniya Derouga.

December 2025

Email: info@humanconstanta.org
Website: https://humanconstanta.org/
Instagram: https://www.instagram.com/humanconstanta/

# Table of Contents

# Introduction

The recent decades have brought a period of sharp political transformation, which is far from positive. While the post-World War II era once fueled the idea of democratic expansion, a counter-trend has been emerging. As Applebaum notes in her recent work "Autocracy Inc.," "nobody imagined that autocracy and illiberalism would spread to the democratic world instead."[1] International IDEA, in its Global State of Democracy Report, observes "the plight of democracy" occurring at a time of radical uncertainty, illustrated by consistent decline of democratic performance.[2] According to the latest Freedom in the World report, global freedom has been declining for 19 consecutive years, with 60 countries worldwide going through a significant democratic backsliding.[3] This pattern is also reflected in the Rule of Law Index, which similarly finds that the majority of countries are seeing a weakening of the rule of law, largely driven by the rise in authoritarianism.[4] An increasing number of governments across regions appear to be drawing inspiration from a shared "authoritarian playbook," displaying traits such as rejecting democratic rules, delegitimising opponents, tolerating violence, and curtailing civil liberties.[5] In some countries, such repressive measures of control remain contested by the public, while in others they become a routine part of governance,[6] quietly pushing the boundary of what is acceptable. As state power becomes increasingly centralised, restrictions on rights and civic space are tightened, and pressure on independent media, academia, and civil society is growing.

This political change has unfolded in parallel with fast-moving digitalisation. States have already built technology into daily administration through digital service portals and systems, enhancing accessibility and reducing costs.[7] In some contexts, such digital systems have even become the core of life-saving infrastructure. During Russia's full-scale invasion of Ukraine, for example, civilians have been relying on the Air Alarm app and other early-warning digital channels to be informed about incoming strikes, as technology turned into a tool that in practice saves lives.[8] At the same time, weaponising tech tools to exert political control has also proved to be a tempting use case for dictatorships. For example, in 2025, Russia ordered the state-backed Max messenger

[1] 'Anne Applebaum's 'Autocracy, Inc.': Deconstructing the War on Democracy' *Policy Magazine* (2 August 2024) https://www.policymagazine.ca/anne-applebaums-autocracy-inc-deconstructing-the-war-on-democracy/; Anne Applebaum, *Autocracy Inc* (Penguin Books 2024) 27

[2] International IDEA, *The Global State of Democracy 2024: Strengthening the Legitimacy of Elections in a Time of Radical Uncertainty* (International IDEA 2024) 13 https://www.idea.int/democracytracker/sites/default/files/2024-09/the-global-state-of-democracy-2024-strengthening-legitimacy-elections.pdf

[3] Freedom House, *Freedom in the World 2025: The Uphill Battle to Safeguard Rights* (Freedom House 2025) https://freedomhouse.org/sites/default/files/2025-02/FITW_World_2025_Feb.2025.pdf

[4] World Justice Project, *WJP Rule of Law Index Insights 2025* (World Justice Project 2025) https://worldjusticeproject.org/rule-of-law-index/insights

[5] Kevin Douglas Grant, 'Democracy Undone: The Authoritarian's Playbook – Overview' *The GroundTruth Project* (17 October 2019) https://thegroundtruthproject.org/the-authoritarians-playbook-seven-steps-populists-worldwide-are-taking-to-undermine-the-democracies-that-elected-them/

[6] Among the countries highlighted in 2025, Botswana and Sri Lanka illustrate recent democratic pushback against backsliding, contrasted with Georgia and Venezuela, where mobilisation has so far failed; Marina Nord and others, *Democracy Report 2025: 25 Years of Autocratization – Democracy Trumped?* (V-Dem Institute 2025) 43 https://www.v-dem.net/documents/60/V-dem-dr__2025_lowres.pdf

[7] World Bank, *GovTech: The New Frontier in Digital Government Transformation* (World Bank 2020) https://documents1.worldbank.org/curated/en/898571612344883836/pdf/GovTech-The-New-Frontier-in-Digital-Government-Transformation.pdf

[8] Visit Ukraine, 'Air Alarm: An App That Alerts You to Dangers in a Specific Region on Your Smartphone' *Visit Ukraine.Today* (25 April 2025) https://visitukraine.today/blog/143/air-alert-app-that-notifies-about-danger-in-certain-region-in-your-smartphone

to be pre-installed on all new phones, with critics warning that the messenger could facilitate surveillance.[9] The scale on which journalists and human rights defenders are silenced is also no short of a crisis, particularly when aided with a host of digital or hybrid tools – the largely unchecked rise of spyware, persistent attacks on encryption, increased disinformation and abuse on online platforms, and the weaponisation of cybercrime laws.[10] Such leveraging of digital technologies to surveil, repress and manipulate citizens is often described as "digital authoritarianism."[11] This commonly used title, however, does not signify that these tactics are exclusive to autocracies.[12] As Applebaum notes, democracies, including hybrid ones, also deploy surveillance, which in turn helps autocracies normalise their own abuses.[13] For example, ongoing EU debates on the Child Sexual Abuse Regulation ("Chat Control"), which would mandate client-side scanning, illustrate how democratic systems, too, can end up normalising intrusive surveillance.[14] Yet, novel digital control methods can be the government's gateway to authoritarianism, especially when safeguards are weak.

Importantly, this shift in digitally enabled repression now extends well beyond national borders. In itself, the phenomenon of cross-border repression is hardly new – Mussolini's regime targeted Italians abroad, while Stalin ordered Trotsky's assassination in Mexico City in 1940.[15] The primary purpose of these attacks has always been the elimination, intimidation, or neutralisation of political exiles.[16] Both the actors involved and the tools they use, however, have changed. Instead of (or in addition to) relying on abductions, physical assaults, or even assassinations, governments now turn to digital infrastructure and proxy actors (contractors, hacker groups, and others) to project power across borders at a higher speed and at a lower cost, making attribution and accountability more complicated. At the same time, the "success" of such digital operations increasingly depends on the behaviour of private companies and platforms, whose (in-)actions can amplify or limit cross-border reach. Over time, host institutions may also become used to this pressure, tolerating a degree of lawlessness within their own borders.[17] These combined factors mean that the practice is growing in its popularity – a 2021 Freedom House study, one of the first systematic assessments, documented more than 600 cases of transnational repression since 2014 and concluded that these have become "a normal phenomenon."[18] For many exiled activists and

[9] 'Russia orders state-backed Max messenger app to be pre-installed on new phones' *The Guardian* (21 August 2025) https://www.theguardian.com/technology/2025/aug/21/russia-max-app-phones

[10] Access Now, 'Combating Digital Threats to Safeguard Press Freedom' *Access Now* (6 May 2025) https://www.accessnow.org/world-press-freedom-day-2025/

[11] James S. Pearson, 'Defining Digital Authoritarianism' *Philosophy & Technology* 37(2) (2024) 73; Access Now, 'Resisting the Rise of Digital Dictatorship in Eastern Europe and Central Asia' *Access Now* (24 September 2025) https://www.accessnow.org/press-release/resisting-digital-dictatorship-in-eastern-europe-central-asia/

[12] Anne Applebaum, *Autocracy Inc* (Penguin Books 2024) 31; Access Now, *Digital Dictatorship: Authoritarian Tactics and Resistance in Eastern Europe and Central Asia* (Access Now 2022) 5 https://www.accessnow.org/wp-content/uploads/2022/10/Digital-dictatorship-authoritarian-tactics-and-resistance-in-Eastern-Europe-and-Central-Asia-Access-Now.pdf

[13] Anne Applebaum, *Autocracy Inc* (Penguin Books 2024) 70-71

[14] Thorin Klosowski, 'Chat Control Is Back on the Menu in the EU. It Still Must Be Stopped' *Deeplinks Blog (EFF)* (29 September 2025) https://www.eff.org/deeplinks/2025/09/chat-control-back-menu-eu-it-still-must-be-stopped-0

[15] Yossi Shain, *The Frontier of Loyalty: Political Exiles in the Age of the Nation-State* (University of Michigan Press 2005) 190

[16] Anne Applebaum, *Autocracy Inc* (Penguin Books 2024) 112

[17] *Ibid.*

[18] Nate Schenkkan and Isabel Linzer, *Out of Sight, Not Out of Reach: The Global Scale and Scope of Transnational Repression* (Freedom House 2021) 2 https://freedomhouse.org/sites/default/files/2021-02/Complete_FH_TransnationalRepressionReport2021_rev020221.pdf

journalists,[19] this means that fleeing persecution at home no longer guarantees safety. Instead, repression follows them abroad. Reports by Human Rights Watch, Access Now, CitizenLab, and iSANS document cases in which exiles in Europe, North America, and other regions faced coordinated spyware deployment,[20] smear-like influence operations,[21] online intimidation,[22] and phishing.[23] These developments mark a transition from transnational repression as primarily a physical practice to one deeply embedded in digital systems.

Placed within this global landscape, this study focuses on transnational repression against exiles in Europe, understood here primarily as the member states of the Council of Europe. Where relevant, case studies of non-member states are included if their practices affect dissidents living in Europe, particularly those fleeing authoritarian rule or conflict in Eastern Europe, the Caucasus, and the Middle East. Europe is a focal point because upheavals around it, including the war in Ukraine, the post-2020 crackdown in Belarus, renewed repression in Russia, and shrinking civic space in parts of the Caucasus, have driven many activists to seek refuge in nearby European countries. They arrive in a region that is far from uniform, where some states are drifting toward authoritarianism,[24] and others, although perceived as safer, still struggle to provide effective remedies to cross-border coercion. For many, therefore, seeking safety in Europe does not mean an actual "exit" from authoritarianism, as even in exile their freedoms remain constrained.[25] What may look like isolated incidents of such constraint, on closer inspection, appears to be a coordinated system.

This study aims to look at that system in detail, tracing how digital tools are used to suppress dissent across borders. Although digital tools of repression can be employed by a wide range of actors – including non-state groups, private companies, and governments – this study focuses primarily on instances where such tools are deployed, or credibly presumed to be deployed, by authoritarian states. The emphasis is on cases in which repressive practices transcend national borders, allowing regimes to target exiles who have sought refuge in safer jurisdictions. While the analysis acknowledges the roles of host states, digital platforms, and intermediaries that may enable or mitigate these practices, the core concern is state-driven transnational repression originating in autocracies that extend their coercive reach beyond territorial boundaries. The

[19] For example, ProtectDefenders.eu supported nearly 8,700 human rights defenders and activists globally in 2021 versus 10,518 in 2023-2024, while noting it could only meet around 20 per cent of legitimate requests; ProtectDefenders.eu, *Annual Report 2021: The Human Rights Movement at a Crossroad* (ProtectDefenders.eu 2022) https://protectdefenders.eu/2021-annual-report-human-rights-movement-at-a-crossroad/; ProtectDefenders.eu, *Annual Report 2023-2024: Essential Protection for Human Rights Defenders in Critical Times* (ProtectDefenders.eu 2024) 13 https://protectdefenders.eu/wp-content/uploads/2020/07/2024-Annual-Report_ESSENTIAL-PROTECTION-IN-CRITICAL-TIMES.pdf

[20] Access Now, *Exiled, then Spied On: Civil Society in Latvia, Lithuania, and Poland Targeted with Pegasus Spyware* (10 July 2024) https://www.accessnow.org/publication/civil-society-in-exile-pegasus/

[21] Human Rights Watch, *We Will Find You: A Global Look at How Governments Repress Nationals Abroad* (Human Rights Watch 2024) https://www.hrw.org/report/2024/02/22/we-will-find-you/global-look-how-governments-repress-nationals-abroad

[22] Natasza Krawczuk and Yuri Dzhibladze, 'Transnational Repression in Belarus: A Multifaceted Instrument to Silence the Dissent' *International Strategic Action Network for Security (iSANS)* (11 June 2024) https://isans.org/human-rights/transnational-repression-in-belarus-a-multifaceted-instrument-to-silence-the-dissent.html

[23] John Scott-Railton and others, 'Rivers of Phish: Sophisticated Phishing Targets Russia's Perceived Enemies Around the Globe' *The Citizen Lab, University of Toronto* (14 August 2024) https://citizenlab.ca/2024/08/sophisticated-phishing-targets-russias-perceived-enemies-around-the-globe/

[24] Murat Aktas, 'The Rise of Populist Radical Right Parties in Europe' *International Sociology* 39(6) (2024) 591 https://journals.sagepub.com/doi/full/10.1177/02685809241297547

[25] Dana M. Moss, 'Transnational Repression, Diaspora Mobilization, and the Case of the Arab Spring' *Social Problems* 63(4) (2016) 480-98 https://doi.org/10.1093/socpro/spw019

analysis maps these practices, identifies recurring patterns, and formulates recommendations, highlighting how digitalisation has reshaped cross-border repression in Europe.

# Mapping the Toolkit

Authoritarian governments rarely rely on a single tactic when trying to intimidate and silence critics beyond their own borders. Instead, they draw on a mix of digital methods that often overlap and reinforce each other: covert surveillance, phishing, online harassment, information manipulation, and legal or bureaucratic pressure at home that results in digital exclusion abroad. Working in combination, these approaches create a layered system meant to surveil, pressure, isolate, and ultimately silence those who believed that exile would provide them with safety. The following chapters provide an overview of these methods and illustrate them with examples. Crucially, very few of these techniques operate in isolation. Personal data stolen through a phishing attack may later be used to launch smear campaigns, and spyware used to expose an activist's network can lead to harassment aimed at their family members. Even seemingly "low-level" harassment online, such as mocking posts, doxxing, or impersonation, can escalate into offline risks once names, photos, or contacts circulate in hostile channels. What begins as an isolated or seemingly minor digital intrusion often unfolds in stages and evolves into an invasive, multifaceted attack with very real consequences.

Although the realities of exerting transnational pressure are interconnected and multi-layered, for the purposes of this paper, the means of digital transnational repression will be divided into technical (1) and hybrid (2) means of intrusion.

# Part 1. Technical Means

## Surveillance and Spyware

*"It is horrifying to me that they knew everything I was doing, precisely where I was, who I was speaking with, my private thoughts and actions, at any moment they desired."*[26]

- *Rwandan activist on being targeted by Pegasus spyware*

Perhaps the most invisible – and in many ways the most powerful – form of digital repression is covert surveillance. This kind of monitoring often forms the foundation of authoritarian strategies: before targeting an actor or a whole community with wider repression, states typically begin by collecting as much information about them as possible. Autocracies invest heavily in developing the technical capacity to surveil not only their citizens at home but also exiled communities, aiming

[26] Carine Kanimba, 'Statement of Carine Kanimba' (U.S. House of Representatives Permanent Select Committee on Intelligence, 27 July 2022) https://docs.house.gov/meetings/IG/IG00/20220727/115048/HHRG-117-IG00-Wstate-KanimbaC-20220727.pdf

to harvest their data and map their connections, often without leaving any visible trace for ordinary users. The logic behind this tactic is often associated with the Panopticon, a prison design analysed by Michel Foucault, where the mere possibility of constant observation leads people to police their own behaviour, even if no one is actually watching. In the digital age, this effect is strongly amplified as modern technologies create an environment that can be described as even more "panoptic" than the one Foucault originally envisioned.[27] Indeed, modern surveillance capabilities replicate this effect on a global scale. For someone in exile, there is often no way to tell whether their phone, inbox, or online conversations are being monitored. That uncertainty alone can be enough to prompt caution, self-censorship, and leave people with a constant sense of unease.

Sophisticated spyware has become a key weapon in such repression strategies, with Pegasus, developed by the Israel-based NSO Group, being the most notorious example. First exposed by Citizen Lab in 2016, and later documented by the international Pegasus Project coalition, the tool has since been traced to governments worldwide, including multiple European Union member states.[28] Its speciality lies in the extraordinary level of access it provides: a single click on a malicious link sent via apps like WhatsApp or Viber can trigger an exploit that installs the spyware and grants operators access to all of the target's messages, calls, photos, location data, and even the device's microphone and camera.[29] Because this extremely extensive level of access can serve countless purposes, those who are known to have been targeted have come from a wide variety of backgrounds: high-level European Union officials,[30] senior human rights lawyers,[31] and investigative journalists and political activists in diverse European countries such as Spain,[32] France,[33] Hungary,[34] Poland,[35] and others. Those in exile, however, have become particularly frequent targets of spyware, with the risks being even sharper. Indeed, their political activity continues across borders, but unlike senior government officials or those working for major organisations, they are often left to confront such advanced threats alone, without having access to the appropriate training, tools, or institutional support.

[27] Ivan Manokha, 'Surveillance, Panopticism and Self-Discipline in the Digital Age' *Surveillance & Society* 16(2) (2018) 219-37 https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/8346

[28] Bill Marczak and John Scott-Railton, *The Million Dollar Dissident: NSO Group's iPhone Zero-Days Used Against a UAE Human Rights Defender* (The Citizen Lab, University of Toronto 24 August 2016) https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/

[29] Amnesty International, *Forensic Methodology Report: How to Catch NSO Group's Pegasus* (Amnesty International 2021) https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/

[30] Raphael Satter and Christopher Bing, 'Exclusive: Senior EU Officials Were Targeted With Israeli Spyware' *Reuters* (11 April 2022) https://www.reuters.com/technology/exclusive-senior-eu-officials-were-targeted-with-israeli-spyware-sources-2022-04-11/

[31] Shaun Walker and others, 'Pegasus Project: Spyware Leak Suggests Lawyers and Activists at Risk Across Globe' *The Guardian* (19 July 2021) https://www.theguardian.com/news/2021/jul/19/spyware-leak-suggests-lawyers-and-activists-at-risk-across-globe

[32] John Scott-Railton and others, *CatalanGate: Extensive Mercenary Spyware Operation Against Catalans Using Pegasus and Candiru* (The Citizen Lab, University of Toronto 18 April 2022) https://citizenlab.ca/2022/04/catalangate-extensive-mercenary-spyware-operation-against-catalans-using-pegasus-candiru/

[33] '«Projet Pegasus»: Mediapart a été espionné par le Maroc' ['"Pegasus Project": Mediapart Was Spied On by Morocco'] *Mediapart* (19 July 2021) https://www.mediapart.fr/journal/international/190721/projet-pegasus-mediapart-ete-espionne-par-le-maroc

[34] Amnesty International, *Forensic Methodology Report: How to Catch NSO Group's Pegasus* (Amnesty International 2021) https://www.amnesty.org/en/latest/research/2021/07/forensic-methodology-report-how-to-catch-nso-groups-pegasus/

[35] 'Poland: HCLU and other groups intervene in Pegasus case before ECtHR' *IFEX* (17 March 2025) https://ifex.org/poland-hclu-and-other-groups-intervene-in-pegasus-case-before-ecthr/#:~:text=The%20Brejza%20v%20Poland%20case,him%20during%20an%20election%20campaign

Investigations by organisations such as Access Now have revealed numerous cases of opposition actors in exile being targeted with Pegasus, particularly during periods of heightened political activity.  One example is that of Galina Timchenko, co-founder and CEO of the exiled Russian media outlet Meduza, whose phone was infected while she was based in Germany.[36] The breach occurred just as Timchenko was preparing to attend a meeting of Russian media actors in Berlin, in what she later described as an experience similar to "having one's wallet stolen," raising concerns about the potential exposure of her contact list too.[37] Similar attacks have occurred among Belarusian dissidents and members of the political opposition.  Prominent opposition figures Andrei Sannikov (ex-presidential candidate) and Natalia Radzina (editor-in-chief of the independent media outlet Charter 97), for instance, were reported to have been infected with Pegasus around the time they took part in high-level exile forums and strategy meetings in Poland.[38] Another case involved the director of Novaya Gazeta Europe, Yulia Epifanova, whose device was compromised in August 2020, during the same period she was seeking accreditation to a press event hosted by Sviatlana Tsikhanouskaya.[39] These cases already suggest a broader pattern: in several documented instances, infections coincided with strategy meetings or public diaspora events, precisely the times when hostile actors are most interested in gaining new intelligence. Deploying spyware products at those points gives actors a window into real-time discussions, allowing them to witness the organisation and anticipate future plans. Attribution in these cases is unclear, as the investigations do not name an operator and note overlaps suggesting a single Pegasus customer may carry out several attacks.[40] Whether the extracted data was shared with Russian or Belarusian services is also unknown.

Digital repression in Europe extends well past dissidents coming from countries next door. Exiles from Morocco, Saudi Arabia, Syria, Rwanda, and other countries have also been hit by elaborate spyware attacks, illustrating how far-reaching digital repression has become. While in exile in France, Moroccan journalist Hicham Mansouri learned that his phone had been compromised repeatedly, with forensic experts finding more than 20 Pegasus infections within a few months in 2021.[41] In the UK, Saudi dissident Yahya Assiri went to court after claiming that Pegasus spyware had been used against him.[42] Around the same time, investigators of Amnesty International's Security Lab found that the same tool had been turned on relatives of Jamal Khashoggi after his murder in Istanbul,[43] showing how surveillance is often added to other forms of repression. In Belgium, the daughter of Paul Rusesabagina, the well-known Rwandan opposition figure, also

[36] Access Now, 'Hacking Meduza: Pegasus spyware used to target Putin's critic' *Access Now* (13 September 2023) https://www.accessnow.org/publication/hacking-meduza-pegasus-spyware-used-to-target-putins-critic/

[37] Stephanie Kirchgaessner and Andrew Roth, 'Exiled Russian Journalist Hacked Using NSO Group Spyware' *The Guardian* (13 September 2023) https://www.theguardian.com/technology/2023/sep/13/exiled-russian-journalist-galina-timchenko-reportedly-hacked-using-nso-group-spyware

[38] Suzanne Smalley and Daryna Antoniuk, 'The Inside View of Spyware's "Dirty Interference," From Two Recent Pegasus Victims' *The Record* (25 June 2024) https://therecord.media/pegasus-spyware-victims-sannikov-erlikh

[39] Committee to Protect Journalists, 'Pegasus spyware targeted exiled journalists from Russia, Latvia, Belarus, report finds' *CPJ.org* (30 May 2024) https://cpj.org/2024/05/report-pegasus-spyware-targets-exiled-journalists-from-russia-latvia-belarus/

[40] John Scott-Railton and others, *By Whose Authority? Pegasus targeting of Russian & Belarusian-speaking opposition activists and independent media in Europe* (The Citizen Lab, University of Toronto 30 May 2024) https://citizenlab.ca/2024/05/pegasus-russian-belarusian-speaking-opposition-media-europe/

[41] Phineas Rueckert, 'Pegasus: The New Global Weapon for Silencing Journalists' *Forbidden Stories* (18 July 2021) https://forbiddenstories.org/pegasus-the-new-global-weapon-for-silencing-journalists/

[42] Reuters, 'UK-Based Dissident Can Sue Saudi Arabia for Alleged Spyware, Court Rules' *Reuters* (21 October 2024) https://www.reuters.com/world/uk-based-dissident-can-sue-saudi-arabia-alleged-spyware-court-rules-2024-10-21/

[43] Amnesty International, 'Massive Data Leak Reveals Israeli NSO Group's Spyware Used to Target Activists, Journalists, and Political Leaders Globally' *Amnesty International* (19 July 2021) https://www.amnesty.org/en/latest/press-release/2021/07/the-pegasus-project/

reportedly had her devices infected by Pegasus,[44] underscoring how spyware often reaches not just the dissidents themselves but those around them. While these cases have come to light, they represent only a small window into a much larger pattern. Because so many surveillance incidents remain hidden from view, rarely documented or publicly exposed, it is almost impossible for researchers or governments to measure the actual scope of cross-border surveillance. Indeed, it is precisely the covert design of spyware that ensures most incidents remain invisible, making the true extent of such repression practically unknown.

Pegasus may dominate headlines, but it is only one piece of a much wider surveillance market. It often operates in parallel with other products: forensic analysis of exiled Egyptian politician Ayman Nour's device showed simultaneous infections with Pegasus and Predator tools, apparently run by two different government clients, with four spyware processes active.[45] In Italy, authorities reportedly relied on Graphite, another Israeli-made product, to monitor activists involved in migration rights work.[46] Serbian police have been documented using Cellebrite tools to extract data from journalists and civil society members.[47] Some systems do not even need to compromise a device directly: the interception technology sold by Circles exploits SS7 vulnerabilities to capture calls, messages, and location data.[48] Recent reporting shows how this works. Altamides, sold by First Wap, tapped phone-network signalling to track devices worldwide without infecting them, routing through Telecom Liechtenstein.[49] Its clients reportedly included Belarus, Indonesia, Malaysia, Nigeria, Saudi Arabia, Singapore, the UAE, and Uzbekistan – a list that Citizen Lab's Ron Deibert called "a rogue's gallery of human rights-abusing, authoritarian countries."[50] Taken together, such capabilities already enable cross-border tracking at scale: reports suggest Saudi operators have used this access to track phones moving abroad,[51] for example. These state-run interception regimes sit alongside, and are often amplified by, a thriving private market. European countries themselves not only purchase such tools but also host companies like the Intellexa Alliance,[52] which develops and exports spyware systems worldwide. Surveillance is therefore undergoing a structural shift – espionage is no longer confined to intelligence agencies but has become an

[44] Joël Matriche, 'La fille d'un opposant rwandais espionnée par Pegasus en Belgique' ['The daughter of a Rwandan opposition figure spied on by Pegasus in Belgium'] *Le Monde* (19 July 2021) https://www.lemonde.fr/projet-pegasus/article/2021/07/19/la-fille-d-un-opposant-rwandais-espionnee-par-pegasus-en-belgique_6088774_6088648.html

[45] Bojan Perkov and others, *A Privacy Nightmare: Understanding Spyware* (SHARE Foundation 2025) 22 https://sharefoundation.info/wp-content/uploads/2025/09/Spyware.pdf

[46] Amnesty International, 'Italy: New Case of Journalist Targeted With Graphite Spyware Confirms Widespread Use of Unlawful Surveillance' *Amnesty International* (13 June 2025) https://securitylab.amnesty.org/latest/2025/06/italy-new-case-of-journalist-targeted-with-graphite-spyware-confirms-widespread-use-of-unlawful-surveillance/

[47] Amnesty International, 'Serbia: Authorities Using Spyware and Cellebrite Forensic-Extraction Tools to Hack Journalists and Activists' *Amnesty International* (16 December 2024) https://securitylab.amnesty.org/latest/2024/12/serbia-a-digital-prison-spyware-and-cellebrite-used-on-journalists-and-activists/

[48] Bill Marczak and others, *Running in Circles: Uncovering the Clients of Cyberespionage Firm Circles* (The Citizen Lab, University of Toronto 1 December 2020) https://citizenlab.ca/2020/12/running-in-circles-uncovering-the-clients-of-cyberespionage-firm-circles/

[49] Gabriel Geiger *and others*, 'The Surveillance Empire That Tracked World Leaders, a Vatican Enemy, and Maybe You' *Mother Jones* (14 October 2025) https://www.motherjones.com/politics/2025/10/firstwap-altamides-phone-tracking-surveillance-secrets-assad-erik-prince-jared-leto-anne-wojcicki/

[50] Ibid.

[51] Stephanie Kirchgaessner, 'Revealed: Saudis Suspected of Phone-Spying Campaign in US' *The Guardian* (29 March 2020) https://www.theguardian.com/world/2020/mar/29/revealed-saudis-suspected-of-phone-spying-campaign-in-us

[52] Amnesty International, 'Presentation – Predator Files: How European Spyware Threatens Civil Society Around the World' *Amnesty International* (29 December 2023) https://securitylab.amnesty.org/latest/2023/12/presentation-predator-files-how-european-spyware-threatens-civil-society-around-the-world/

increasingly accessible commodity. With companies offering such systems for hire, digital surveillance is faster, cheaper, and easier to deploy than ever, lowering the barrier for governments seeking to suppress dissent across borders.

This spyware market is broad and networked: recent mapping identifies some 561 entities in 46 countries, spanning vendors, suppliers, brokers and investors, explicitly warning that export controls have only “marginal utility” unless accompanied by further measures, like coordinated transparency and due diligence.[53] Moreover, investigations show that European and national state funds have at times even subsidised vendors implicated in unlawful surveillance, including Intellexa-allied entities, underscoring contradictions between Europe’s legal and policy safeguards and its real-life practices.[54] Nonetheless, some accountability is emerging even in this challenging environment, through measures like soft law and strategic litigation: the UK-France Pall Mall Process sets a non-binding code of practice for responsible state use of commercial spyware,[55] while cases on the use of Pegasus have reached Strasbourg, with applications against Poland and Azerbaijan communicated to the European Court of Human Rights.[56] Finally, European human rights jurisprudence is also beginning to address surveillance that extends beyond device compromise and occurs in other, more complex contexts. In Ukraine and the Netherlands v. Russia, the European Court of Human Rights held that “filtration” practices in occupied territories, such as biometric capture and bulk device searches, violated Article 8 rights,[57] serving as an important reminder that unlawful surveillance functions as an instrument of control in both peacetime and war.  In parallel with that, “digital ceasefire” proposals now highlight the importance of ceasing the wider weaponisation of technology in conflict, as such,[58] including the use of intrusive surveillance, highlighting that such practices operate both as targeted monitoring of individuals and as an evolving systemic tool of control over whole populations and territories.

[53] Sarah Graham, Jen Roberts and Nitansha Bansal, ‘Mythical Beasts: Diving into the Depths of the Global Spyware Market’ *Atlantic Council Issue Brief* (10 September 2025) https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/mythical-beasts-diving-into-the-depths-of-the-global-spyware-market/

[54] Vas Panagiotopoulos, ‘Spyware Industry Pockets EU Subsidies While Snooping on Its Citizens’ *Follow the Money* (16 September 2025) https://www.ftm.eu/articles/spyware-industry-eu-subsidies-surveillance-concers

[55] United Kingdom, *The Pall Mall Process: Tackling the Proliferation and Irresponsible Use of Commercial Cyber Intrusion Capabilities* (UK Government 28 February 2025) https://www.gov.uk/government/publications/the-pall-mall-process-declaration-tackling-proliferation-and-irresponsible-use-of-commercial-cyber-intrusion-capabilities/the-pall-mall-process-tackling-the-proliferation-and-irresponsible-use-of-commercial-cyber-intrusion-capabilities

[56] *Brejza v Poland* App no 27830/23 (communicated 3 July 2024); *Javadov and Others v Azerbaijan* App no 30573/22 (communicated on 24 September 2025); *Ganbarova v Azerbaijan* App no 45877/22 (communicated on 24 September 2025)

[57] Deborah Housen-Couriel and Asaf Lubin, ‘Digital Rights in Armed Conflict and the Ukraine v. Russia Decision’ *Lawfare* (18 August 2025) https://www.lawfaremedia.org/article/digital-rights-in-armed-conflict-and-the-ukraine-v.-russia-decision

[58] Access Now, ‘Toward a Digital Ceasefire’ *Access Now* (20 November 2024) https://www.accessnow.org/toward-a-digital-ceasefire/

## Phishing and Digital Lures

*"There is no day when I open my email and I don't have a phishing email."*[59]
*- Editor of an Iranian media organisation in exile*

While spyware tends to dominate many of the current discussions, it often represents the heavy weaponry of digital repression, highly costly for deployers and not too frequently encountered in daily exile life. More often, dissidents are targeted through much more ordinary-looking means: an email attachment that appears usual, a link that raises no suspicion, or a message that seems to come from a trustworthy community network. These are the entry points for phishing: social engineering attacks that exploit trust and human vulnerabilities, rather than relying on higher-level technical sophistication. Phishing can be used to trick a target into revealing their login credentials, granting access to email accounts, inboxes, or contact lists. Even such limited access to the personal data of an activist in exile can reveal their broader networks, details of funders and collaborators, and information on upcoming meetings or political strategies. From there, a malicious link can also open the door to further malicious software deployments, including the installation of spyware. Overall, what makes such attacks effective is their low cost, accessibility, and plausible deniability: unlike commercial spyware, which requires expensive contracts and may leave trails, phishing can be rolled out widely and later dismissed as the work of "fraudsters," complicating attribution. Moreover, once a single account is compromised, attackers often repurpose it to impersonate the victim and send new phishing messages to their contacts. In this way, a single breach can ripple through entire diaspora networks, exploiting trust within them and pulling more people into the breach.

The strength of phishing attacks lies in how believable they feel. Most often, the perpetrators of such campaigns get the targets to open a malicious link or attachment by impersonating a friend or an organisation associated with their field of expertise, as the attempts of phishing are masked by invitations to events, interview requests, and others.[60] Indeed, actors have increasingly impersonated journalists, colleagues, or international organisations to trick exiled activists into clicking malicious links or handing over their credentials. One prominent example involved Farnaz Fassihi, an Iranian dissident journalist with the Wall Street Journal, who was impersonated by attackers. Using her name, they contacted multiple relatives and peers, attempting to gather more people's information.[61] An Iranian filmmaker living in exile in Prague received an email purporting to come from the Wall Street Journal, offering to purchase his work; similarly, an Iranian-born academic in Germany was also invited to a supposed interview under Fassihi's name, framed as a chance to share his achievements "to inspire the youth of our beloved country."[62] These campaigns are tied to Charming Kitten, an Iranian-linked hacking group that systematically exploits professional trust as its main tactic: their lures frequently mimic invitations to Deutsche Welle

[59] Marcus Michaelsen, 'The Silencing Effect of Digital Transnational Repression' *Hivos* (26 February 2020), https://hivos.org/the-silencing-effect-of-digital-transnational-repression/

[60] Marcus Michaelsen, *The Digital Transnational Repression Toolkit, and Its Silencing Effects* (Freedom House, Special Report 2020) https://freedomhouse.org/report/special-report/2020/digital-transnational-repression-toolkit-and-itssilencing-effects

[61] Certfa Lab, 'Fake Interview: The New Activity of Charming Kitten' *Certfa Lab* (30 January 2020) https://blog.certfa.com/posts/fake-interview-the-new-activity-of-charming-kitten/

[62] Raphael Satter and Christopher Bing, 'Exclusive: Iran-linked Hackers Pose as Journalists in Email Scam' *Reuters* (5 February 2020) https://www.reuters.com/article/us-iran-hackers-exclusive-idUSKBN1ZZ1MS/

webinars or CNN interviews on Iranian politics.[63] The aim is consistent: to deceive dissidents in exile into surrendering access to their accounts, thereby exposing their networks and activities.

These tactics have been replicated against exiled communities throughout Europe. Azerbaijani activist, targeted while living in the Netherlands, faced phishing emails impersonating her, sent to government critics and disguised as a fake invitation for a reception at the US Embassy in Baku.[64] The messages carried malware capable of recording screenshots of what the targets were typing. Citizen Lab and Access Now have also documented cases where emails sent to Russian and Belarusian exiles mimicked civil society groups, officials, or trusted colleagues, but were in fact designed to steal passwords, in attacks reportedly linked to the Russian state.[65] Related waves also impersonated donors and grant providers, using funding-themed lures.[66] In June 2025, Citizen Lab similarly reported a Russia-linked technique that tricked targets into generating app-specific passwords, granting inbox access.[67] The level of personalisation of these tactics made detection difficult: in some instances, the fake addresses differed from genuine ones by only a single character.[68] In late 2024, SentinelLabs exposed a related wave of attacks attributed to Ghostwriter, a Belarus-linked group. Activists, opposition members, and Ukrainian military staff in Europe were sent malicious documents via Google Drive. One such document, titled “Political Prisoners,” contained court decisions information, but in fact was designed to infiltrate opposition networks through malicious macros.[69] Kazakhstan has also adopted this model. Dissidents, their lawyers, and family members across Europe once received legal-looking emails that resembled routine paperwork but, with a single click, exposed entire inboxes and private exchanges.[70] These cases highlight that phishing is not only cheap but also easily adaptable to different contexts.

Beyond email, perpetrators increasingly exploit other digital platforms, particularly messaging apps and social media, turning to digital lures and honeypots that similarly exploit users’ trust. A recent Signal case shows this in practice: a Signal phishing wave targeted Belarus-linked public figures in Europe, with attackers posing as “Signal Support,” bypassing encryption, and seizing the targets’

[63] Certfa Lab, ‘Fake Interview: The New Activity of Charming Kitten’ *Certfa Lab* (30 January 2020) https://blog.certfa.com/posts/fake-interview-the-new-activity-of-charming-kitten/

[64] Amnesty International, ‘Azerbaijan: Activists Targeted by “Government-Sponsored” Cyberattack’ *Amnesty International* (10 March 2017) https://www.amnesty.nl/actueel/azerbaijan-activists-targeted-by-government-sponsored-cyberattack

[65] John Scott-Railton and others, ‘Rivers of Phish: Sophisticated Phishing Targets Russia’s Perceived Enemies Around the Globe’ *The Citizen Lab, University of Toronto* (14 August 2024) https://citizenlab.ca/2024/08/sophisticated-phishing-targets-russias-perceived-enemies-around-the-globe/

[66] ‘FSB phished Russian, Belarusian and Ukrainian human rights activists for years, posing as “grant providers” and NGOs’ *The Insider* (14 August 2024) https://theins.ru/en/news/273870

[67] John Scott-Railton, Rebekah Brown and Bill Marczak, ‘Same Sea, New Phish: Russian Government-Linked Social Engineering Targets App-Specific Passwords’ *The Citizen Lab, University of Toronto* (18 June 2025) https://citizenlab.ca/2025/06/russian-government-linked-social-engineering-targets-app-specific-passwords/

[68] ‘Хакеры организовали фишинговую атаку на активистов, журналистов и юристов. К ней может быть причастна ФСБ – расследование’ [‘Hackers organised a phishing attack on activists, journalists and lawyers. The FSB may be involved – investigation’] *Current Time* (14 August 2024) https://www.currenttime.tv/a/hakery-ataki-fishing/33078671.html

[69] Tom Hegel, ‘Ghostwriter | New Campaign Targets Ukrainian Government and Belarusian Opposition’ *SentinelOne Labs* (25 February 2025) hreveals how easily these methods can spread, and more importantly, the logic behind them: by mimicking trusted entry points, such as key platforms and services that exiles depend on, authorities can exploit built-in features to deanonymizettps://www.sentinelone.com/labs/ghostwriter-new-campaign-targets-ukrainian-government-and-belarusian-opposition/

[70] Eva Galperin and others, *I Got a Letter From the Government the Other Day...: Unveiling a Campaign of Intimidation, Kidnapping, and Malware in Kazakhstan* (Electronic Frontier Foundation August 2016) https://www.eff.org/files/2016/08/03/i-got-a-letter-from-the-government.pdf

accounts.[71] This practice is becoming more common, as authoritarian operators often bypass encryption by phishing one-time codes and re-registering accounts, turning "secure" messengers into takeover vectors.[72] Belarusian security forces are also well-known for platform-based attacks that involve cloning Telegram channels and bots, posing as trusted opposition initiatives, and prompting users to click on malicious links that harvest their data. One notable case involved a fake Telegram channel posing as BYPOL, the association of exiled former law enforcement officers. It promoted the so-called "Peramoga 2.0"[73] plan and urged visitors to click on a link to get more details; one man, still in Belarus, clicked and was tracked down shortly after the malicious site harvested his technical data.[74] Importantly, this honeypot attack was combined with an AI-generated video: a deepfake of Sviatlana Tsikhanouskaya urging Belarusians to participate made the lure appear more authentic,[75] showing how AI is already used to streamline such traps. Similar counterfeits have imitated human rights organisations and their helplines,[76] Kastuś Kalinoŭski Regiment[77] recruitment forms,[78] a contact form for the Cyberpartisans hacker group,[79] and others. The sheer number of such traps shows how easy it is for these methods to spread and, more importantly, the logic behind them: by mimicking trusted entry points, such as key platforms and services that exiles depend on, authorities can exploit built-in features to deanonymise users seeking to connect or access information.

These traps are not confined by geography: once set up, counterfeit bots and fake contact points can be accessed from anywhere in the world, making them effective against not only diaspora communities but also sympathetic foreigners. In a rare but notable reported case, German national Rico Krieger was allegedly looking for ways to join the fighting in Ukraine when he came into contact with what appeared to be a recruitment account for the "Western Battalion." In reality, the account was operated by Belarusian security forces; Krieger was later detained inside Belarus and accused of terrorism.[80] While this case involved an unusual chain of events, it underscores how fabricated online identities can cross borders, drawing in targets who may have no prior

[71] RESIDENT.NGO ThreatLab, 'Technical Write-up: Signal Account Takeovers Phishing Campaign Targets Exiled Belarusian Activists 2025' *RESIDENT.NGO* (6 October 2025) https://resident.ngo/lab/writeups/signal-phishing-belarus-2025/

[72] Ron Synovitz, 'Encrypted Messaging Apps Struggle Against Authoritarian Regimes' *Radio Free Europe/Radio Liberty* https://internetfreedom.io/rferl__encrypted-messaging-apps.html

[73] BYPOL's original "Peramoga" is a political mobilisation plan: an anonymous chatbot enrolls supporters into small cells for coordinated, non-violent action; BYPOL, *"Peramoga" Mobilisation Plan* (18 June 2022) https://bypol.org/archives/en/peramoga-mobilization-plan

[74] '«Увидел ссылку, нажал. А вскоре ко мне приехали». Что силовики могут узнать о вас по одному клику' ['"Saw a link, clicked it. They soon came for me." What the security services can learn about you with one click'] *UDF.BY* (28 September 2024) https://udf.name/news/main_news/272773-uvidel-ssylku-nazhal-a-vskore-ko-mne-priehali-chto-siloviki-mogut-uznat-o-vas-po-odnomu-kliku.html

[75] '«Увидел ссылку, нажал. А вскоре ко мне приехали». Что силовики могут узнать о вас по одному клику' ['"Saw a link, clicked it. They soon came for me." What the security services can learn about you with one click'] *Zerkalo.io* (26 September 2024) https://news.zerkalo.io/life/79249.html

[76] Viasna (@viasna96), 'Post #23209' [Telegram channel] (Telegram, 13 December 2023) https://t.me/viasna96/23209

[77] The regiment of Belarusian volunteers within the Armed Forces of Ukraine, formed to protect the territorial integrity of Ukraine from the Russian invasion; The Kastus Kalinouski Regiment, 'About Us' http://Kalinouski.Org

[78] 'Белорус написал в фейковый бот полка Калиновского. Ему перезвонили и пригласили в Витебск "на точку сбора" для отправки в Украину' ['A Belarusian wrote to a fake Kalinouski Regiment bot. He received a call inviting him to Vitebsk "for deployment" to Ukraine'] *Zerkalo.io* (26 September 2023) https://news.zerkalo.io/life/49826.html?tg=9

[79] 'Силовики создают ловушки, чтобы сажать на большие сроки (есть очень коварные). Вот как не попасться' ['Security forces set traps to imprison people for long sentences (some are very devious). Here's how not to fall for them'] *Zerkalo.io* (20 August 2024) https://news.zerkalo.io/life/76173.html

[80] 'BELPOL: теракт, за который Кригера приговорили к расстрелу, был провокацией силовиков. Организация раскрыла новые детали дела' ['BELPOL: the terrorist act for which Kriger was sentenced to execution was a provocation by the security forces. Organisation revealed new details of the case'] *Zerkalo.io* (31 July 2024) https://news.zerkalo.io/life/74656.html

connection to the opposition but who still become targets once they engage. More clear-cut deanonymization cases have also been reported in Belarus. In the case of “Belarusian Hajun,” an exile-run OSINT initiative monitoring Russian military activity in Belarus, their Telegram bot was reportedly compromised, with logs containing user-submitted details accessed by security services.[81] This data was then used to identify and detain contributors inside Belarus: it is reported that at least 106 people have been detained and might have faced prosecution.[82] As CyberPartisans later detailed, investigators triangulated senders using account analytics, metadata, time-location clues, CCTV footage, and Telegram databases.[83] The implications, however, may extend beyond the country’s borders: exiled supporters who interacted with the bot may now be identifiable, leaving them exposed to harassment abroad or increasing their vulnerability if they return. After the bot’s compromise, operators also appear to have pursued further social engineering: in October 2025, phishing emails impersonating a Ukrainian rights group targeted Belarusians and sought data on “Hajun” defendants and other Ukraine-linked cases.[84]

Phishing and related lures tend to surface during periods of heightened tension, exploiting the immediate fears that dissidents face. During Egypt’s “Nile Phish” campaign, for example, colleagues of a human rights lawyer Azza Soliman began receiving phishing emails just within hours of her arrest, each containing a fake arrest warrant as an attachment.[85] The tactic was clear: playing on fear to make recipients more likely to click. The aim of such attacks goes beyond simply stealing credentials, since gaining access to one account also means reaching contact lists, old exchanges, and shared files, which together allow attackers to reconstruct networks and identify sensitive connections.[86] Such a pattern was also observed in the Silencing Across Borders project, which interviewed more than fifty exiled activists, journalists, and digital security trainers from countries including Egypt, Syria, Iran, and Azerbaijan. Many described how the compromise of just one person’s account – the so-called “weakest link” – can set off a chain of reaction, drawing in colleagues, friends, and family, while also fuelling a corrosive sense of doubt.[87] In exile, even the possibility of someone’s account being compromised may become just as harmful as an actual breach. It leads to self-sensorship, disengagement, and produces a climate of mistrust that is itself a powerful tool of repression.[88] Phishing thus rarely marks the end of an operation; instead, it opens the way for broader manipulation, gradually eroding trust and creating vulnerabilities that can then be exploited at the platform level.

[81] ‘Мониторинговый проект «Беларускі Гаюн» останавливает свою работу’ [‘Monitoring Project “Belaruski Hajun” Stops Its Work’] *REFORM.news* (7 February 2025) https://reform.news/monitoringovyj-proekt-belaruski-gajun-ostanavlivaet-svoju-rabotu

[82] Viasna (@viasna96), ‘Post #32379’ [Telegram channel] (Telegram, 17 October 2025) https://t.me/viasna96/32379

[83] ‘«Киберпартизаны» рассказали, как силовики вычисляют людей, которые присылали информацию «Гаюну»’ [‘“Cyberpartisans” explained how the security forces identify people who sent information to “Hajun”’] *Zerkalo.io* (19 September 2025) https://news.zerkalo.io/life/108978.html?c

[84] ‘Белорусам приходят фейковые письма от имени украинских правозащитников’ [‘Belarusians receive fake letters purporting to be from Ukrainian human-rights defenders’] *Nasha Niva* (9 October 2025) https://storage.googleapis.com/nashaniva-by/read.html?page=/ru/378827

[85] John Scott-Railton and others, *Nile Phish: Large-Scale Phishing Campaign Targeting Egyptian Civil Society* (The Citizen Lab, University of Toronto 2 February 2017) https://citizenlab.ca/2017/02/nilephish-report/

[86] Marcus Michaelsen, *Silencing Across Borders: Transnational Repression and Digital Threats Against Exiled Activists from Egypt, Syria, and Iran* (HIVOS 2020) https://www.opentech.fund/wp-content/uploads/2023/11/SILENCING-ACROSS-BORDERS-Marcus-Michaelsen-Hivos-Report.pdf

[87] Ibid.

[88] Ibid.

# Digital Intimidation and Shaming

*"When I first moved here, I was happy. After years of repression for being a female CEO in Iran, I finally felt free in Switzerland. After this year, even Europe is not safe for me."*[89]

- *Iranian activist in exile on the impact of sustained online harassment*

Where spyware compromises devices, and phishing and other lures exploit digital platforms, online intimidation strikes at something more fundamental: the dissidents' sense of psychological and physical safety. Sometimes digital threats come hand in hand with other forms of repression; at other times, they are deployed on their own, with online harassment pursued as an end in itself. In either form, their message is the same: exile does not equal full safety, as intimidation easily crosses borders. What makes online threats particularly accessible to states and other actors is that this tactic requires little to no special technical capacity. All it may take is a single threatening message, a wave of coordinated harassing comments, a leak of sexualised deepfakes, or a mere sign letting dissidents know that their family back home is also being watched and thus put at risk. This, in itself, can be enough to fracture a person's sense of security. Intimidation can instil a sense of lingering fear, promote self-censorship and self-doubt, and, of course, prevent people from becoming more politically engaged to limit further exposure, leading them to silence their own voices. In many cases, the line between digital threats and real-world danger also becomes blurred, and online intimidation functions as a direct projection of authoritarian reach into the everyday lives of exiles.

Intimidation often follows exposure. Once dissidents are identified through phishing, honeypots, or surveillance, their personal data becomes a weapon in the hands of malicious actors. This is where doxxing comes in as another step in the repression pipeline: the deliberate exposure of personal information online to facilitate harassment.[90] The so-called doxxing packages (names, pictures, addresses, affiliations and family ties) have been increasingly blasted across traditional channels,[91] and now even more so online. In Belarus, the state's GUBOPiK channel and allied actors regularly publish coerced "confession" videos of detainees inside the country, often paired with identifying details.[92] For those in exile, the focus shifts more towards smear campaigns and doxxing: pro-government Telegram channels like Yellow Plums (or Yellow Leaks) are known for exposing people's personal data and amplifying smear narratives that threaten and label dissidents.[93] In other words, repression adapts to contexts: forced confessions for those whom the state can detain, and threats, smears, and doxxing for those it can not physically reach. Iran and Russia show

[89] Manisha Ganguly, 'Iranian Activists Across Europe Are Targets of Threats and Harassment' *The Guardian* (22 September 2023) https://www.theguardian.com/world/2023/sep/22/iranian-activists-across-europe-are-targets-of-threats-and-harassment

[90] Freedom House, *Freedom on the Net 2018: United Kingdom* (Freedom House 2018) https://freedomhouse.org/country/united-kingdom/freedom-net/2018

[91] 'Пропагандист в эфире госТВ перечислил адреса объектов недвижимости, которой владеют некоторые из уехавших за границу беларусов' ['A propagandist on state TV listed addresses of real estate owned by some Belarusians who left the country'] *Zerkalo.io* (6 August 2025) https://news.zerkalo.io/economics/105600.html

[92] '«Происходит повсеместно». Приближенный к ГУБОПиК канал случайно опубликовал контакты известного врача - узнали, зачем им эти данные' ['"It happens everywhere." A channel close to GUBOPiK accidentally published a well-known doctor's contacts - we found out why they needed the data'] *Zerkalo.io* (5 July 2024) https://news.zerkalo.io/life/72551.html

[93] Vashy_Slivy (@vashy_slivy), 'Post #64764' [Telegram channel] (Telegram, 22 September 2025) https://t.me/vashy_slivy/64764; 'Post #63967' [Telegram channel] (Telegram, 4 September 2025) https://t.me/vashy_slivy/63967; 'Post #44064' [Telegram channel] (Telegram, 21 June 2024) https://t.me/vashy_slivy/44064

similar patterns: Iranian actors have used Twitter (now X) to post the personal addresses of relatives of activists abroad,[94] and Kremlin-linked outlets have exposed the information of individuals with alleged "pro-Western connections," labelling exiles as "foreign agents" by integrating hacked files into public shaming narratives.[95] In each case, private data is transformed into a public weapon to isolate the targets and intimidate their networks. Moreover, this process is increasingly automated. AI-driven doxxing streamlines what used to rely on slow, manual labour – scraping data and identifying targets – making deanonymisation faster. Belarusian "wanted lists" once depended on manual crowdsourcing,[96] but may become increasingly automated by facial recognition tools like those developed by Synesis, both facing European sanctions for helping to identify protesters.[97]

Intimidation intensifies around such visible political acts, turning mobilisation into a point of vulnerability. Syrian exiles, for example, recalled that after joining opposition rallies abroad, they were quickly bombarded with hostile calls and threatening online messages.[98] Such timing is not accidental: threats emerge as a direct response to participation, making any such activity feel like it carries immediate risk. Belarus has pursued a similar strategy, though through more systematised tools. As such, state-linked Telegram channels are known to be posting data of protesters abroad, coupling them with threats of criminal charges, home searches, or property seizures. Those who attended rallies in Warsaw, for example, were publicly targeted in this way,[99] and one campaign even listed 365 demonstrators by name, promising reprisals.[100] Timing again played a central role: these lists circulated in the wake of major protests, ensuring that political visibility abroad was immediately countered with intimidation. The same approach extends to individuals. Sprinter Krystsina Tsimanouskaya, who defected during the Tokyo Olympics,[101] described receiving digital threats in Warsaw, saying, "they would rip my stomach open if I went outside."[102] In general, women face an even more targeted dimension of this visibility-driven

[94] Reporters Without Borders, *"Watch Out Because We're Coming For You": Transnational Repression of Iranian Journalists in the UK* (RSF) https://rsf.org/sites/default/files/medias/file/2024/04/Rapport%20Iran%20V6%20Web_2.pdf

[95] Mariya Omelicheva, 'Russia's Doxing Campaign: An Expanding Trend in Extraterritorial Repression' *RussiaPost* (5 August 2024) https://russiapost.info/society/doxing_campaign

[96] 'Силовики в соцсетях активизировали поиски участников протестов 2020 года - их интересуют выходившие на марши в двух городах' ['On social media, the security forces have stepped up their search for participants in the 2020 protests - they are interested in marchers from two cities'] *Zerkalo.io* (15 July 2025) https://news.zerkalo.io/life/103966.html

[97] Markéta Gregorová, *Human rights sanctions against Russian company NtechLab* (Question for Written Answer E-003687/2021 to the Council, European Parliament, 21 July 2021) https://www.europarl.europa.eu/doceo/document/E-9-2021-003687_EN.html; Katya Pivcevic, 'Police facial recognition use in Belarus, Greece, Myanmar raises rights, data privacy concerns' *BiometricUpdate.com* (15 March 2021) https://www.biometricupdate.com/202103/police-facial-recognition-use-in-belarus-greece-myanmar-raises-rights-data-privacy-concerns

[98] Amnesty International, *Syria: The Long Reach of the Mukhabaraat: Violence and Harassment Against Syrians Abroad and Their Relatives Back Home* (Amnesty International October 2011) https://www.amnesty.org/en/documents/MDE24/057/2011/en/

[99] 'Силовики угрожают «уголовными делами, обысками и арестами имущества» также участникам акций в Варшаве 9-10 августа' ['Security forces threaten "criminal cases, searches and property arrests" also to participants of rallies in Warsaw, 9-10 August'] *Zerkalo.io* (5 August 2025) https://news.zerkalo.io/life/105544.html

[100] 'СК угрожает 365 участникам зарубежных акций, прошедших 26 января. Завели уголовное дело и будут искать имущество в Беларуси' ['The Investigative Committee threatens 365 participants of foreign rallies held on 26 January. A criminal case has been opened and they will search for property in Belarus'] *Zerkalo.io* (27 January 2025) https://news.zerkalo.io/life/89645.html?c

[101] In Tokyo, Belarus team officials tried to force Tsimanouskaya onto a flight home. She refused, sought police protection, and later received a Polish humanitarian visa; Gabrielle Tétrault-Farber, 'Belarusian Sprinter Refuses to Leave Tokyo' *Reuters* (2 August 2021) https://www.reuters.com/lifestyle/sports/exclusive-olympics-belarusian-athlete-says-she-was-taken-airport-go-home-after-2021-08-01/

[102] Yuras Karmanau, 'Belarusians Fleeing Repression at Home Say They Face New Threats and Intimidation Abroad' *Independent* (10 September 2024)

repression through AI-generated sexualised deepfakes, which now make up the vast majority of non-consensual synthetic content.[103] Indeed, actors exploit this imbalance to discredit female activists, weaponising stigma and undermining their credibility. Journalist Rana Ayyub was an early high-profile victim,[104] but the same pattern now appears in other political contexts across Europe: Ireland saw police investigations into explicit deepfakes of a female politician,[105] and Italy's Prime Minister Giorgia Meloni has also been targeted,[106] illustrating that the same AI tools used for phishing lures also enable intimidation.

Few states have turned online intimidation into such a routine tool of repression as Iran. In the UK, newsrooms at BBC Persian and Iran International have been bombarded with digital harassment against Iranian dissidents working there that mixed sexualised abuse, death threats, and the leaking of personal details.[107] A 2024 survey by Reporters Without Borders found that almost nine out of ten Iranian journalists working in exile in the UK had endured such online threats, with many admitting they had curtailed their reporting or changed daily habits as a response.[108] The threat environment grew so severe that MI5 publicly acknowledged credible plots against these journalists, and Iran International even suspended its London operations for a period.[109] Similar cases of abuse appear across the continent. In Germany, Iranian exiles told of being hit with a flood of online death threats, with sometimes thousands arriving within just a few days, alongside repeated hacking attempts on their personal devices; an Iranian activist in Spain recalled being hounded by hostile messages and digital stalking to the point that she began to feel watched.[110] In the UK, campaigners were told by police that there were "credible threats to life," with the intimidation traced back to Tehran's security services.[111] Iran has thus made cross-border digital harassment a part of its governing toolkit, seeing how this cheap and accessible tactic actually leads the targets to change their daily behaviours.

Online intimidation follows the same underlying logic across different political contexts, aiming to punish those who speak out for their voice and visibility. The cases of such attacks are nearly endless. In Germany, Azerbaijani reporters working with the platform Meydan TV have faced smear campaigns and coordinated harassment, efforts aimed at discrediting their reporting and warning

https://www.independent.co.uk/news/ap-alexander-lukashenko-sviatlana-tsikhanouskaya-georgia-belarus-b2609935.html

[103] Beatriz Kira, 'Deepfakes, the Weaponisation of AI Against Women and Possible Solutions' *Verfassungsblog* (3 June 2024) https://verfassungsblog.de/deepfakes-ncid-ai-regulation/

[104] Rana Ayyub, 'I Was the Victim of a Deepfake Porn Plot Intended to Silence Me' *HuffPost UK* (21 November 2018) https://www.huffingtonpost.co.uk/entry/deepfake-porn_uk_5bf2c126e4b0f32bd58ba316

[105] 'Deepfake: Garda Probe into Phoney Topless Images of Female Politician' *Irish Independent* (18 February 2025) https://www.independent.ie/podcasts/the-indo-daily/the-indo-daily-deepfake-garda-probe-into-phoney-topless-images-of-female-politician/a574996059.html

[106] Laura Gozzi, 'Giorgia Meloni: Italian PM seeks damages over deepfake porn videos' *BBC News* (20 March 2024) https://www.bbc.com/news/world-europe-68615474

[107] Reporters Without Borders, *"Watch Out Because We're Coming For You": Transnational Repression of Iranian Journalists in the UK* (RSF) https://rsf.org/sites/default/files/medias/file/2024/04/Rapport%20Iran%20V6%20Web_2.pdf

[108] Ibid.

[109] Mark Townsend and Geneva Abdul, 'Met Police and MI5 foil 15 plots by Iran against British or UK-based "enemies"' *The Guardian* (18 February 2023) https://www.theguardian.com/uk-news/2023/feb/18/met-police-mi5-foil-15-iranian-plots-against-british-or-uk-based-enemie

[110] Manisha Ganguly, 'Iranian Activists Across Europe Are Targets of Threats and Harassment' *The Guardian* (22 September 2023) https://www.theguardian.com/world/2023/sep/22/iranian-activists-across-europe-are-targets-of-threats-and-harassment

[111] Negar Mojtahedi, 'UK Parliamentary Report Classes Iran Among Greatest Foreign Threats' *Iran International* (30 July 2025) https://www.iranintl.com/en/202507291422

others in the diaspora against anti-government reporting.[112] Chinese and Hong Kong students across Europe describe how their photographs from protests reappear online, stripped of context and paired with hostile messages, ensuring that every public appearance carries future risks and threats.[113] Similarly, in Belgium, Rwandan exiles talk about meetings infiltrated by suspicious "participants" who later resurface online, alongside sudden floods of defamatory posts and whispered reminders that Kigali is paying attention.[114] Palestinians in Europe experience a whole different yet related form of intimidation: mass trolling, targeted harassment, and coordinated reporting that erases their online presence.[115] Indeed, many say they run into shadow bans and repeated takedowns that strip them of their ability to reach an audience, showing how intimidation has seeped into the very systems that govern online speech.[116] Here, the abuse does not primarily stem from their own state but from hostile networks exploiting digital platforms, showing how platform vulnerabilities can be weaponised in conflicts beyond the exile's state of origin. In each case, the result is the same: intimidation narrows civic space, silences voices, and exploits digital systems.

Online intimidation of exiles can be driven so far that it no longer resembles merely harassment, but begins to take on the shape of real terror. Chechnya offers a stark example: with minimal effort, its state-linked networks have used digital platforms to send extremely blunt threats to dissidents abroad. One of the chilling examples comes from a State Duma member from Chechnya, who used Instagram to threaten the exiled lawyer Abubakar Yangulbaev and his family with beheading.[117] The statement, shared widely online, served as a public warning that families of Chechen dissidents were vulnerable and watchable too. Other officials reinforced the tactics. In 2019, a speaker of Chechnya's parliament similarly released a video online declaring a "blood feud" against exiled blogger Tumso Abdurakhmanov, with senior officials later voicing support for the threat. The victim himself publicised these endorsements, underscoring how intimidation was not hidden but deliberately staged online to instil fear.[118] Even Ramzan Kadyrov has personally engaged in such digital theatrics, telling an underage critic during an Instagram livestream: "you won't sleep at night, I will destroy you."[119] Some of these examples also reveal how intimidation extends beyond the individuals themselves, as families are often drawn into the situation as leverage. As OC-Media documented in 2023, Chechen security deployed such tactics frequently, with one example being

[112] *Index on Censorship*, 'Azerbaijan: Harassment of Meydan TV Must Stop' *Index on Censorship* (20 April 2016) https://www.indexoncensorship.org/2016/04/azerbaijan-harassment-meydan-tv-must-stop/

[113] Jessie Lau, 'Threats, Fear and Surveillance: How Beijing Targets Students in the UK Who Criticise the Regime' *The Guardian* (25 March 2024) https://www.theguardian.com/global-development/2024/mar/25/china-students-uk-beijing-transnational-repression-surveilla

[114] Louis Colart and Joël Matriche, 'En Belgique, le Rwanda met au pas sa diaspora [In Belgium, Rwanda Brings Its Diaspora to Heel]' *Le Monde* (28 May 2024) https://www.lemonde.fr/international/article/2024/05/28/en-belgique-le-rwanda-met-au-pas-sa-diaspora_6236063_3210.html

[115] 7amleh – The Arab Center for the Advancement of Social Media, *Briefing on the Palestinian Digital Rights Situation Since October 7th, 2023* (7amleh 1 November 2023) https://7amleh.org/post/briefing-on-the-palestinian-digital-rights-situation-since-october-7th-2023

[116] 7amleh – The Arab Center for the Advancement of Social Media, *Position Paper: Safeguarding Palestinian Digital Rights in the EU Policy Framework* (7amleh and RNW Media 10 July 2025) https://7amleh.org/post/position-paper:-safeguarding-palestinian-digital-rights-in-the-eu-policy-framework

[117] Amnesty International, 'Russia: Politician threatens to decapitate family members of Chechen activist' *Amnesty International* (2 February 2022 https://www.amnesty.org/en/latest/news/2022/02/russia-politician-threatens-to-decapitate-family-members-of-chechen-activi

[118] Gabrielle Tétrault-Farber, 'Top Chechen Official Claims Blood Feud Against Blogger' *VOA News* (12 March 2019) https://www.voanews.com/a/top-chechen-official-claims-blood-feud-against-blogger/4825742.html

[119] *'"I Will Destroy You": Chechen Leader Threatens Kid on Instagram' Radio Free Europe/Radio Liberty* (20 May 2021) https://www.rferl.org/a/chechnya-kadyrov-instagram/31265313.html

them threatening to kill the families of administrators of opposition Telegram channels, unless those channels were deleted.[120]

These cases point to an even darker dimension of online intimidation: when threats spill over from dissidents themselves to their families. By targeting parents, siblings, and other relatives who remain at home, and are thus the most vulnerable, regimes send a strong reminder that leaving the country does not mean leaving the regime's grasp. Online threats directed at activists abroad gain force precisely because they are often paired with the knowledge that family members back home can be harassed, detained, or coerced. Often, these digital threats targeting exiles are paired with direct and even harsher threats to the family members at home. Syrian activists in Europe have long recounted how anonymous online harassment from regime-linked accounts was soon followed by warnings that their families would "pay the price," turning what began as low-level digital pressure into the very real prospect of retaliation in Damascus, at times even escalating to torture in real life.[121] BBC Persian staff in London have also faced coordinated online abuse in combination with their relatives in Iran being summoned, interrogated or pressured to cut off contact, with such concerns documented in high-level evidence.[122] In Belarus, authorities amplify pressure on families with digital means: relatives targeted through threats, searches, or arrests are not only punished but also have their arrests recorded and displayed on official Telegram channels, turning reprisals into public warnings for all.[123]

Another lesson from these cases is that online intimidation is never only about the hostile messages themselves, but also about the structures and platforms that allow them to spread and take hold. European-level evidence showcases consistent gaps in platform moderation: the Fundamental Rights Agency found that human content checkers miss online abuse and that algorithms can multiply errors and even promote harmful content.[124] The same research flagged that Telegram, a platform many exiles rely on, demonstrates particularly limited efforts to detect online hate.[125] Notably, the persistence of digital intimidation online is also reinforced by other systemic weaknesses: reporting tools can be manipulated, content moderation rules fail outside of English-speaking communities, and legal gaps leave victims with little opportunity for redress. Language inequality is particularly evident and relevant to exiles: analysis of the Digital Services Act transparency data by Oxford researchers suggests that millions of European users on X (formerly Twitter) lack moderation in their national language.[126] Taken together, these gaps let digital intimidation proliferate. In some cases, such as for Palestinian communities, these governance gaps have produced the opposite problem: over-removal of online speech. Human Rights Watch documented the suppression of protected expression on platforms like Instagram and Facebook, driven by flaws in Meta's policies, their inconsistent application, clear deference to

[120] Luiza Mchedlishvili, 'Chechen Security Forces 'Threaten to Kill' Families of Telegram Channel Admins' *OC.media* (5 January 2024) https://oc-media.org/chechen-security-forces-threaten-to-kill-families-of-telegram-channel-admins/

[121] Sam Jones, 'Syria Accused of Torturing Relatives of Overseas Activists' *The Guardian* (3 October 2011) https://www.theguardian.com/world/2011/oct/03/syria-accused-torturing-relatives-activists

[122] BBC World Service, *Written Evidence Submitted by BBC World Service* (UK Parliament, February 2025) https://committees.parliament.uk/writtenevidence/138345/pdf/

[123] Press MVD (@pressmvd), 'Post #7278' [Telegram channel] (Telegram, 14 March 2023) https://t.me/pressmvd/7278

[124] European Union Agency for Fundamental Rights, *Online Content Moderation: Current Challenges in Detecting Hate Speech* (FRA, Vienna 2023) https://fra.europa.eu/sites/default/files/fra_uploads/fra-2023-online-contet-moderation_en.pdf

[125] Ibid. 66

[126] Manuel Tonneau and others, 'Language Disparities in Moderation Workforce Allocation by Social Media Platforms' (SocArXiv Preprint, 27 August 2025) https://osf.io/preprints/socarxiv/amfws_v1

government requests, and heavy reliance on automated tools.[127] For exiled activists, this means that digital transnational repression is sustained not only by hostile actors but also by protection gaps on platforms. Ultimately, this enables the silencing of exiles, undermines participation, and allows digital repression to cross borders with impunity.

## DDoS Attacks

*"We were trying to spin up solutions… Everything to continue to write news."*[128]

- *lead software engineer of a Russian media outlet in exile on being targeted with DDoS attacks*

Aside from other technical breaches, transnational repression can also take the form of access disruption, when the websites or digital communication hubs of dissident networks are forced offline. Distributed denial-of-service (DDoS) campaigns are a tool used to target websites or platforms with artificial traffic until they become unavailable, cutting off online access for actual users. The denial of service for exile-run outlets and rights groups, even for a short period, can stall mobilisation and push communities into less secure networks where surveillance traps are easier to set. In April 2024, a Russian independent media outlet in exile, operating from Europe, was hit with a 48-hour DDoS attack that generated more than two billion requests, making the site completely inaccessible.[129] Between 2010 and 2015, Qurium also mitigated dozens of such attacks against Azerbaijani media, many of them exile-run, while observing overlaps with other forms of platform manipulation.[130] For example, in mid-2020, Berlin-based Azerbaijani outlet Meydan TV also suffered coordinated breaches of its Facebook and Instagram accounts, with years of content wiped and follower counts slashed.[131] In Belarus-linked cases, the volunteer help site motolko.help crashed in January 2025 following a traffic surge exceeding 1000 per cent of normal volume, just hours after BELPOL had also been knocked offline in a suspicious "hack."[132] The combined timing and selective targeting in such incidents suggest not random glitches, but deliberate efforts to paralyse activist information-sharing infrastructure at moments of high political activity.

Exile media are most likely to be targeted with such cyberattacks when their reporting is most urgent, making information access the key pressure point. In late 2024, another EU-based Russian

[127] Deborah Brown, *Meta's Broken Promises: Systemic Censorship of Palestine Content on Instagram and Facebook* (Human Rights Watch 21 December 2023) https://www.hrw.org/report/2023/12/21/metas-broken-promises/systemic-censorship-palestine-content-instagram-and

[128] Jonathan Rozen, 'Cyberattackers Use Easily Available Tools to Target Media Sites, Threaten Press Freedom' *CPJ* (30 July 2024) https://cpj.org/2024/07/cyberattackers-use-easily-available-tools-to-target-media-sites-threaten-press-freedom/

[129] 'Cyberattackers Target Meduza With Unprecedented DDoS Campaign in Effort to Disable Site' *Meduza* (23 April 2024) https://meduza.io/en/feature/2024/04/23/cyberattackers-target-meduza-with-unprecedented-ddos-campaign-in-effort-to-disable-site

[130] Qurium Media Foundation, *A Decade of Efforts to Keep Independent Azeri Media Online* (Qurium Media Foundation 10 July 2021) https://www.qurium.org/alerts/the-challenge-of-keeping-azeri-media-online/

[131] 'Hackers Delete Social Media Content of Independent Azerbaijani News Outlet Meydan TV' *CPJ* (14 July 2020) https://cpj.org/2020/07/hackers-delete-social-media-content-of-independent-azerbaijani-news-outlet-meydan-tv/

[132] 'Сайт motolko.help атакован - его пытаются взломать. Ранее подобное происходило с сайтом BELPOL' ['The motolko.help site was attacked - attempts to hack it. Previously something similar happened with the BELPOL site'] *Zerkalo.io* (27 January 2025) https://news.zerkalo.io/life/89631.html

newsroom endured days of DDoS while publishing sensitive work.[133] In mid-2025, a London-based Iranian outlet in exile reported coordinated account compromises and intimidation,[134] a reminder that the repression tactics often overlap and reinforce one another. At the same time, European monitoring shows repeated waves of denial-of-service attacks against media more broadly,[135] making availability attacks a routine pressure point, not a one-off technical error. Law enforcement has already acted on this issue. In July 2025, a cross-border EU operation disrupted systems used for politically motivated DDoS attacks,[136] showing that much of this cyber capacity sits within Europe's reach and can, in fact, be policed. Yet, attribution remains the most challenging part of this process. Independent reporting particularly shows that many denial-of-service campaigns are routed through commercial proxy and data centre services, effectively masking operators, with some providers stalling the efforts to identify such malicious clients.[137] In practice, this leaves both the victims and law enforcement with only circumstantial evidence, even when the timing and the nature of the targeting itself may appear consistent with state-sponsored repression. Similarly, ENISA finds that most denial-of-service incidents leave few reliable traces, and even basic indicators (such as IP addresses) are usually not trustworthy, with 59 per cent of recorded cases not clearly attributable to any group.[138] As a result, such cyber disruptions function as another tool of censorship, a brief yet strategic silencing of dissent.

# Part 2. Hybrid Means

## Legal-Tech Hybrids

*"Lukashenko is showing that he can hang the fate of any citizen by a thread. This means that a Belarusian anywhere in the world needs to be prepared for unpleasant surprises."*[139]

- *Belarusian dissident on being detained at the Armenia border over an arrest warrant*

Digital repression no longer manifests only as hacking or harassment. Instead, it is increasingly channelled through the official systems that govern people's legal status, mobility, and rights. Tools built to ensure mobility and protect people, such as passports, consular services, cross-border databases, and "extremism" lists, are now being repurposed into modern levers of transnational

[133] 'Novaya Gazeta Europe Website Hit by Multiple Cyberattacks' *Novaya Gazeta Europe* (16 October 2024) https://novayagazeta.eu/articles/2024/10/16/novaya-gazeta-europe-website-hit-by-multiple-cyberattacks-en-news

[134] 'Iranian-Linked Hacker Group Targets Iran International Journalists in Cyberattack' *CPJ* (9 July 2025) https://cpj.org/2025/07/iranian-linked-hacker-group-targets-iran-international-journalists-in-cyberattack/

[135] 'New Surge of DDoS Attacks Threatens Media Freedom in Europe' *International Press Institute (IPI)* (19 February 2024) https://ipi.media/new-surge-of-ddos-attacks-threatens-media-freedom-in-europe/

[136] 'Global Operation Targets NoName057(16) Pro-Russian Cybercrime Network' *Europol Newsroom* (16 July 2025) https://www.europol.europa.eu/media-press/newsroom/news/global-operation-targets-noname05716-pro-russian-cybercrime-network

[137] Jonathan Rozen, 'Cyberattackers Use Easily Available Tools to Target Media Sites, Threaten Press Freedom' *CPJ* (30 July 2024) https://cpj.org/2024/07/cyberattackers-use-easily-available-tools-to-target-media-sites-threaten-press-freedom/

[138] European Union Agency for Cybersecurity, *Threat Landscape for DoS Attacks - January 2022 to August 2023* (ENISA, November 2023) https://www.enisa.europa.eu/sites/default/files/publications/DoS%20report.pdf

[139] Yuras Karmanau, 'Belarusians Fleeing Repression at Home Say They Face New Threats and Intimidation Abroad' *Independent* (10 September 2024) https://www.independent.co.uk/news/ap-alexander-lukashenko-sviatlana-tsikhanouskaya-georgia-belarus-b2609935.html

repression. Once entrenched in such infrastructures, what begins as informal digital pressure is easily converted into official procedures that carry the force (and appearance) of law. These may include: a designation criminalising online activity; cancelled documents that lead to statelessness and loss of mobility; or a compliance freeze that shuts down digital fundraising. As legal infrastructures become digitised and interlinked across borders, these points of abuse can travel quickly and trigger effects in other systems. Exiled communities who already face digital threats must also now navigate the risk that basic legal mechanisms, designed to safeguard identity, may be turned against them. The result is a hybrid model of repression that moves fluidly between online spaces and formal mechanisms, multiplying points of vulnerability for people in exile and exporting risk into European bureaucracies. In this sense, transnational digital repression becomes intertwined with traditional mechanisms of state power, giving rise to what this paper terms legal-tech hybrids.

## Pushing Dissidents Into Statelessness

A central element of these legal-tech hybrid tactics is the use of passports and consular services as leverage. In 2023, Belarus changed the law on passport renewals and document processing, cutting off the ability to obtain key legal documents through consulates.[140] By turning an ordinary consular service into a point of additional pressure and control, the authorities have repurposed the need for access to legal identity into a weapon against those living abroad. For the several hundred thousand Belarusians outside of the country, the change created a profound insecurity: without valid documents, it becomes nearly impossible to live, work, or travel legally, while returning home to renew them carries a real risk of detention. The UN Special Rapporteur on Belarus warned that the measure could leave many exiles without valid documents and even create the risk of statelessness for children born abroad whose parents could not safely travel home to register them.[141] Testimonies confirm this pressure in practice: Belarusians abroad have received emails declaring their passports invalid and ordering them to report in person to Belarus to replace them, a move described by opposition figures as political blackmail.[142] Rather than providing needed protection and essential legal services, Belarusian embassies and consulates abroad have therefore quietly become instruments of repression, forcing dissidents to choose between navigating uncertain legalisation processes or risking the loss of legal identity, or even arrest. In 2023 only, rights observers counted 207 people detained at Belarusian border checkpoints, which confirms this as a real consequence.[143]

Belarus is not the only state deploying such tactics. Egypt, for instance, has long been documented denying ID cards or passports to dozens of dissidents, journalists, and human rights activists

[140] Human Rights Watch, 'Belarus: Decree Puts Exiled Citizens at Risk' *News Release* (8 September 2023) https://www.hrw.org/news/2023/09/08/belarus-decree-puts-exiled-citizens-risk

[141] Anaïs Marin, *Situation of Human Rights in Belarus: Report of the Special Rapporteur on the Situation of Human Rights in Belarus* (UNHRC 56th Session, UN Doc A/HRC/56/65, 9 May 2024) https://docs.un.org/en/A/HRC/56/65

[142] Leanid Marozau, 'Belarusians Abroad are Being Blackmailed with Expired Passports' [LinkedIn post] (LinkedIn, August 2025) https://www.linkedin.com/feed/update/urn:li:activity:7363261127239098369/

[143] 'At least 207 detained upon return to Belarus: Current statistics from Viasna for 2023' *Spring 96* (11 January 2024) https://spring96.org/en/news/113911

abroad.[144] Similar forms of consular leverage have appeared elsewhere. In the case of Rwanda, some exiles in Europe reported that officials at the embassy would only renew passports or process land transfers if they joined the ruling party's organisation; otherwise, services were denied.[145] In August 2025, Hong Kong applied the same tactic, cancelling passports of exiled activists and banning others from providing them financial support.[146] These tendencies of authoritarian states pose multiple legal challenges for Europe itself. In the case of Belarus, for example, several countries across Europe have stepped in to issue substitute "foreigner" travel documents to those in exile,[147] but these remain specific national measures rather than a coordinated Europe-wide approach. The Council of Europe has urged member states to recognise expired passports, provide substitute travel documents, and grant long-term visas, stressing that no one should be forced back to the very regime they fled.[148] This shows why passport control is such an effective lever of transnational repression: it extends authoritarian reach into the bureaucratic machinery of host states, leaving European democracies in the uneasy position of dealing with the consequences. In practice, consular pressure exports repression into European systems, forcing states to choose between patchwork fixes or more durable but resource-demanding safeguards for those targeted. In parallel, Belarus has tied documents to "extremism": amendments to its Citizenship Law enable citizenship revocation for "extremist crimes,"[149] linking identity documents directly to political labelling.

## *"Extremist," "Terrorist," "Foreign Agent"* Designations

Another hybrid form of repression that links the digital sphere with real-world consequences is the use of "extremism" designations, combined with criminal liability for even minor acts of online association. Belarus illustrates this tactic most clearly. Under its expanding anti-extremism laws, even passive digital activity, such as subscribing to, reposting from, or even saving content from an opposition channel, can be treated as participation in an "extremist formation," carrying prison terms of up to seven or more years.[150] Ordinary online behaviour thus now leaves behind a criminal trail that not only fuels prosecutions at home,[151] but can also follow dissidents abroad, resurfacing at border crossings, consular offices, or in absentia court proceedings. The legal machinery behind

[144] Human Rights Watch, 'Egypt: Dissidents Abroad Denied Identity Documents - Undermines Victims' Access to Basic Rights' *News Release* (13 March 2023) https://www.hrw.org/news/2023/03/13/egypt-dissidents-abroad-denied-identity-documents

[145] Deborah Brown, *"Join Us or Die": Rwanda's Extraterritorial Repression* (Human Rights Watch, 10 October 2023) https://www.hrw.org/report/2023/10/10/join-us-or-die/rwandas-extraterritorial-repression

[146] John Power, 'Hong Kong Cancels Passports, Bans Financial Support for Wanted Activists' *Al Jazeera* (5 August 2025) https://www.aljazeera.com/news/2025/8/5/hong-kong-cancels-passports-bans-financial-support-for-wanted-activists

[147] Oleg Matskevich, 'Заграничные паспорта для белорусов в изгнании: главное' ['Foreign passports for Belarusians in exile: key points'] *BAJ – Белорусская Ассоциация Журналистов* (3 February 2025) https://baj.media/ru/karysnae/zagranichnye-pasporta-dlja-belorusov-v-izgnanii/

[148] Paul Galles, *Addressing the Specific Challenges Faced by the Belarusians in Exile* (Parliamentary Assembly of the Council of Europe, Doc 15783, 5 June 2023) https://rm.coe.int/report-addressing-the-specific-challenges-faced-by-the-belarusians-in-/1680ab3442

[149] Tatsiana Ziniakova, *Quashing Online Dissent: Anti-Extremism Laws Put Digital Rights at Risk in Belarus* (ARTICLE 19 and Human Constanta 2025) https://www.article19.org/wp-content/uploads/2025/08/Belarus-anti-extremism-laws-analysis-final.pdf

[150] 'Belarus Classifies Social Media Channels as 'Extremist'' *Al Jazeera* (29 October 2021) https://www.aljazeera.com/news/2021/10/29/belarus-classifies-social-media-channels-as-extremist

[151] 'В Беларуси уменьшилось количество «преступлений экстремистской направленности» - Следственный комитет' ['In Belarus, the number of "crimes of extremist character" has decreased - Investigative Committee'] *Nasha Niva* (25 November 2024) https://nashaniva.com/ru/356075

such repression is left broad, with “extremism” designations being arbitrarily assigned and even applied retroactively, and there being no meaningful avenue for redress. In this way, legislation is created to ensure that almost any online activity can be reinterpreted as criminal evidence. By creating an intricate web of such legal provisions and designations, the Belarusian state exercises fully unchecked discretion to attach the labels of “terrorism” and “extremism” to punish any dissent, whether it manifests in a like, comment, post, subscription, or a donation.[152] As a result, such a system does not just impose targeted punishments on individuals. It also cultivates a permanent sense of uncertainty, leaving people to navigate online spaces without knowing which activities may put them at risk.

This tactic is not unique to Belarus. Across contexts, governments have discovered that ordinary traces of digital life can be reframed as “evidence” of criminal intent, turning online speech into liabilities. In Hong Kong, authorities have recently extended this logic to its fullest, issuing arrest warrants and even offering substantial bounties for overseas activists, accusing them of “subversion” based on their digital advocacy.[153] These measures are not symbolic. They are reinforced with asset freezes, cancelled passports, and a lifelong stigma. Saudi Arabia applies a similar strategy through its cybercrime and counter-terrorism laws. The case of Salma al-Shehab, a UK-based doctoral student sentenced to decades in prison upon her return, illustrates how the simple act of retweeting dissident accounts can be reclassified as “terrorism.”[154] Russia’s legal framework has, too, evolved along the same lines. Its “foreign agent” and “undesirable organisation” designations blur the line between expression and association, allowing authorities to treat subscriptions, reposts, or donations as participation in illegal activity, as consequences follow both those at home and in exile.[155] Exiles from Russia have faced this frequently, with independent media in particular offering some of the clearest illustrations, showing how such labels migrate into more “neutral” infrastructures. When Russia labelled the exiled newsroom Meduza a “foreign agent” in 2021, the designation quickly spilled into financial infrastructures abroad.[156] Soon after, a wave of fraudulent transactions was directed against its crowdfunding system, prompting payment processors such as Stripe and PayPal to suspend all money transfers to the outlet.[157] In effect, a political label applied in Moscow cut the newsroom off from donations in Europe, not through law enforcement but through compliance routines.

The common pattern across these cases is not the specific charge, be it “extremism” or a “foreign agent” designation, but the fact that states use any available digital traces to drive repression and give such a crackdown the appearance of law. By collapsing speech into evidence, regimes therefore ensure that exile is never fully safe, as digital acts can always be used against dissidents

[152] Tatsiana Ziniakova, *Quashing Online Dissent: Anti-Extremism Laws Put Digital Rights at Risk in Belarus* (ARTICLE 19 and Human Constanta 2025) https://www.article19.org/wp-content/uploads/2025/08/Belarus-anti-extremism-laws-analysis-final.pdf

[153] Jessie Pang, ‘Hong Kong Issues Arrest Warrants for 19 Overseas Activists Accused of Subversion’ *Reuters* (26 July 2025) https://www.reuters.com/world/china/hong-kong-issues-arrest-warrants-19-overseas-activists-accused-subversion-2025-07-25/

[154] Stephanie Kirchgaessner, ‘Saudi Woman Given 34-Year Prison Sentence for Using Twitter’ *The Guardian* (16 August 2022) https://www.theguardian.com/world/2022/aug/16/saudi-woman-given-34-year-prison-sentence-for-using-twitter

[155] Maria Kiseleva, *Still Listening: Audience Strategies of Russia-Focused Media in Exile* (Reuters Institute for the Study of Journalism, March 2025) https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2025-07/RISJ%20Fellows%20Project_Masha_HT25_Final%201_1.pdf

[156] ‘Russia Labels Meduza Media Outlet as “Foreign Agent”’ *Radio Free Europe/Radio Liberty* (23 April 2021) https://www.rferl.org/a/russia-meduza-labeled-foreign-agent-press-freedom/31219272.html

[157] ‘Using Stolen Debit Cards, Hackers Try to Discredit and Derail Meduza’s Crowdfunding Campaign’ *Meduza* (5 May 2021) https://meduza.io/en/news/2021/05/05/using-stolen-debit-cards-hackers-try-to-discredit-and-derail-meduza

when convenient, routed through compliance systems which exiles depend on in their daily lives. Growing regional coordination may yet amplify this dynamic further. For example, the Shanghai Cooperation Organisation's counter-extremism framework (currently shared by ten member states) encourages its members to harmonise legal definitions and cooperate on criminal cases,[158] making it easier in practice for one country to use another's "extremism" designation to seek assistance in legal prosecution or even extradition. That logic now risks scaling globally: with the UN Cybercrime Convention opening for signature in October 2025, states would gain broader channels for cross-border data and evidence requests,[159] potentially easing cooperation on abusive "extremism" cases too. In short, the architecture is shifting from isolated prosecutions to interoperable systems: labels created domestically, validated through regional or global cooperation, and enforced through private compliance. The result is a quieter but wider form of pressure that narrows civic space and keeps exile precarious long after people have crossed a border.

## Interpol Abuse and Law Enforcement Spillovers

If "extremism" lists turn ordinary online activity into yet another potential point of exposure, Interpol Red Notices (wanted person alerts) make those risks concrete. Authoritarian governments learned to weaponise this Interpol system, transforming digital traces into grounds for arrests abroad. Indeed, charges based on digital activity or prosecutions in absentia do not always remain confined to domestic court files; they can reappear as Interpol alerts, triggering detention at a border thousands of kilometres away. Despite recent reforms, such as new review processes, watchdogs show that politically motivated Red Notices and diffusions (which countries can use to seek a person's extradition) still slip through Interpol's gates, creating loopholes for authoritarian abuse.[160] The Belarusian case of filmmaker and activist Andrei Hniot illustrates the tactic. In October 2023, he was detained at Belgrade airport on the basis of a Red Notice requested by Minsk for alleged tax offences; European officials and rights groups immediately denounced the case as political.[161] Even after the Interpol alert was withdrawn and Serbia's appeals court blocked extradition, Hniot had already spent months under house arrest, confined with an ankle monitor and limited movement.[162] This case shows that even when politically driven alerts are later overturned, the harm is already done: months of lost freedom, restrictions on movement, and the sobering proof that a charge opened in the home jurisdiction can still translate into an arrest on European soil.

[158] *Concept of Cooperation of State Members of the Shanghai Cooperation Organization in the Fight Against Terrorism, Separatism and Extremism* (Decision of the Heads of State of the SCO, 5 July 2005) https://cis-legislation.com/document.fwx?rgn=8218&

[159] Sara Benítez-Mongelós, 'The UN Cybercrime Convention: Why It Endangers Human Rights Defenders and Journalists' *Global Campus of Human Rights - Human Rights Preparedness Blog* (13 March 2025) https://www.gchumanrights.org/preparedness/the-un-cybercrime-convention-why-it-endangers-human-rights-defenders-and-journalists/

[160] Red Notice Monitor, 'European Parliament Study on Transnational Repression Highlights Interpol Red Notice Abuse' *Red Notice Monitor* (9 October 2025) https://rednoticemonitor.com/european-parliament-study-on-transnational-repression-highlights-interpol-red-notice-abuse/

[161] Sarah Rainsford, 'Belarus Filmmaker Pleads With Serbia Not to Send Him Back' *BBC News* (27 August 2024) https://www.bbc.com/news/articles/c3rd1l7pdyyo

[162] Ibid.

Turkey demonstrates another route through the same system. Beyond Red Notices, it has been documented misusing Interpol's Stolen and Lost Travel Documents (SLTD) database, flagging dissidents' passports as "revoked" or "stolen."[163] Such entries bypass the scrutiny attached to Red Notices yet still trigger detentions at foreign borders. Since the mass unrest of 2016, Turkey has, in this way, cancelled tens of thousands of passports, often without judicial review, turning a technical data feed into a mechanism of transnational repression.[164] One of the most visible cases was that of an NBA player who had publicly expressed criticism of the Turkish government, and whose passport was cancelled while travelling in Europe. He was briefly detained in Romania in 2017 on the basis of an Interpol alert before being released, effectively rendered stateless until he obtained alternative documentation.[165] Russia similarly follows and elevates Interpol abuse in its diverse forms. For instance, it is responsible for 38 per cent of all public Interpol Red Notices worldwide, as such notices are issued to detain activists, critics, and even asylum seekers.[166] This is legal-tech hybridity in its purest form: a neutral technical database repurposed to reproduce political control and repression abroad. What was designed as an administrative tool for border security becomes, in practice, an extension of regimes' blacklists, where a cancelled passport or a flagged document can instantly translate into detention or forced immobility.

Even without an Interpol notice, police and judicial signals can travel through other infrastructures – for example, by triggering private compliance freezes abroad through AML/KYC channels. Hong Kong showcases this dynamic: its National Security Law has extended beyond borders, operating like a financial cordon that restricts activists' access to their savings and services abroad. One striking example involved a pastor now based in the UK, who learned that his, his wife's, and his church's bank accounts had been frozen amid a police investigation related to alleged crowdfunding for protests, in charges he described as "political retaliation."[167] Some exiles, such as former lawmaker Ted Hui, have reported that their pension savings under the city's Mandatory Provident Fund were frozen by institutions such as HSBC, with "national security" cited as a reason to block withdrawals.[168] Instead of stopping at borders, these financial restrictions show how the national legislation can reach into the ordinary routines of people's lives abroad. When exiles are cut off from bank accounts or pension savings, the effect goes far beyond paperwork. Losing access to banking or pension systems deprives dissidents of the basics they need to settle into new lives, provide for their families, and continue their activism securely. As banks and online platforms move further toward automated compliance and AI-based risk screening, the chances of being cut off from these services are likely to grow rather than diminish. What is now a frozen pension or a blocked transfer could, in the future, be left to automated systems built on politicised data.

[163] Ali Yıldız and Ben Keith, 'After Spotlight on Red Notices, Turkey is Abusing Another Interpol Mechanism' *Just Security* (13 July 2023) https://www.justsecurity.org/87260/after-spotlight-on-red-notices-turkey-is-abusing-another-interpol-mechanism/

[164] Platform for Peace & Justice, *Cancellation of Turkish Passports and Related Violations* (Platform for Peace & Justice 2018) https://platformpj.org/wp-content/uploads/Cancellation-of-Turkish-Passports.pdf

[165] Benjamin Hoffman, 'N.B.A. Player Enes Kanter Released After Being Held in Romania' *The New York Times* (20 May 2017) https://www.nytimes.com/2017/05/20/sports/enes-kanter-detained-romania-erdogan-turkey.html

[166] 'Интерпол в ЕС стал инструментом российских репрессий – доклад' ['Interpol in the EU has become a tool of Russian repression – report'] *AREM / LSM.LV* (1 May 2020) https://arem.lv/interpol-v-es-stal-instrumentom-rossijskih-repressij-doklad/

[167] David Pierson, 'A Hong Kong Pastor Tried to Protect Democracy Activists. Now His Bank Account Is Frozen' *Los Angeles Times* (16 December 2020) https://www.latimes.com/world-nation/story/2020-12-16/hong-kong-bank-accounts-frozen

[168] Amy Hawkins, 'Exiled Pro-Democracy Hong Kong Activists Blocked from Accessing Pensions' *The Guardian* (22 July 2024) https://www.theguardian.com/world/article/2024/jul/22/exiled-pro-democracy-hong-kong-activists-blocked-from-accessing

# Key Features of Modern Digital Transnational Repression

## Layered Architecture

The section above mapped individual tools of digital transnational repression. However, it would be wrong to treat them merely as a patchwork catalogue of separate abuses. Read together, the cases show a different picture: the tools of transnational digital repression operate as a reproducible system. Authoritarian actors do not simply experiment and improvise; they borrow techniques from one another, rely on the same private suppliers, and combine legal and social coercion in ways intended to strongly reinforce each other. This cumulative logic is what gives repression its transnational character: a spyware infection in Belgium, a phishing attack in Germany, or a bounty posted in Hong Kong may seem random, but all these cases appear as components of a larger system. Human Rights Watch has described this as the "system logic" of transnational repression: practices deliberately layered so that the whole is greater than the sum of its parts.[169] Indeed, data stolen through a phishing attack may lead to personal and network exposure, enabling smear campaigns and domestic labelling, which in turn legitimises further hybrid restrictions, such as denial of online services. All of these elements are modular and can be layered, repeated, or interchanged, thereby enabling the whole system of repression to exert a greater real-world impact. For exiles in Europe, this system is a decisive factor: it explains why repression does not come as isolated harassment or phishing campaigns, but instead appears in people's lives as a constant pressure that reaches into daily activities, broader networks, and families at home.

## Surveillance Market

A second pattern emerges from the increased commodification of digital surveillance, where private suppliers now commonly turn authoritarian tactics into services that can be bought and used across borders. The fact that the same spyware products turn up in such different contexts shows the scale of this shift: repression has become something states can purchase relatively easily off the shelf. Governments no longer need to build their own capabilities; they can contract firms like NSO Group or Intellexa and deploy pre-packaged surveillance systems against exiles abroad. Rwanda's use of Pegasus against the daughter of Paul Rusesabagina in Belgium made the logic visible: her device was compromised not because Rwanda possessed unique technical expertise, but because it had access to a global marketplace of surveillance tools.[170] The European Parliament's inquiry showed how Predator, marketed through the Intellexa consortium, was brokered via shell companies, creating channels through which clients could acquire the technology even from within European jurisdictions.[171] The market now crucially reaches beyond

[169] Human Rights Watch, *We Will Find You: A Global Look at How Governments Repress Nationals Abroad* (Human Rights Watch 2024) https://www.hrw.org/report/2024/02/22/we-will-find-you/global-look-how-governments-repress-nationals-abroad

[170] Stephanie Kirchgaessner, 'Hotel Rwanda Activist's Daughter Placed Under Pegasus Surveillance' *The Guardian* (19 July 2021) https://www.theguardian.com/news/2021/jul/19/hotel-rwanda-activist-daughter-pegasus-surveillance

[171] Sophie in 't Veld, *Committee of Inquiry to Investigate the Use of Pegasus and Equivalent Surveillance Spyware: Draft Compromise Report* (European Parliament PEGA Committee, 8 May 2023) https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/PEGA/DV/2023/05-08/REPORTcompromises_EN.pdf

the device: firms also sell phone-network tracking as a service, packaging SS7-style access into buyable tools, similarly linked to Europe.[172] Such surveillance is not used by autocracies alone: democracies from Spain to India have also relied on spyware and similar systems to monitor journalists, lawyers, and opposition figures, lowering the incentives to regulate the market.[173] This overall commercialisation of digital repression carries two consequences. First, it lowers the barrier to entry, allowing governments with little technical expertise to benefit from advanced spyware. Second, it blurs accountability: once a company sells its product, the same tool can reappear in different contexts, hidden behind murky corporate chains that make attribution difficult and remedies nearly impossible. The result is a novel model of repression which can be "hired," leaving dissidents exposed because more actors gain access to such markets.

## Domino Effect

Another pattern is that digital transnational repression is no longer directed solely at silencing individuals; its real aim is to undermine the wider networks that sustain dissidents in exile. Tools such as spyware, phishing, or legal designations may appear to target one person at a time, but in practice, they disrupt entire community structures. When a device is compromised by spyware, the impact spreads: contact lists, shared drives, and group chats are exposed, putting entire activist circles at risk. After the "Belarusian Hajun" bot was compromised, users lost their ability to anonymously share sightings of military movements and equipment, chilling what were otherwise active independent OSINT channels and seeding distrust. Legal branding works in the same way. When Belarus designates a civic organisation as "extremist," it is not only its team who are silenced. The label discourages donors, deters volunteers, and makes even casual engagement, such as following their page online, risky. The result is the erosion of structures that support activism. Timed availability attacks worsen the damage. One DDoS or mass reporting campaign not only affects the outlet or silences the selected users; it pushes whole audiences into other, often less secure channels, interrupts access to crucial information and advocacy, and stalls wider network engagement. When communities rely on access to information, shared resources, and a sense of solidarity, as is true for most exiles, such pressures become especially dangerous. Trust becomes harder to sustain, cooperation pauses, and initiatives lose momentum under the combined weight of legal and digital pressure. This is why the same pattern recurs across contexts as diverse as Syria, Rwanda, China, and Belarus: it offers regimes a transferable way to weaken movements even when they can reach them only from afar.

## AI as a Force Multiplier

AI has been rapidly changing global politics and reshaping the dynamics of digital repression, giving authoritarian actors new tools of unprecedented scale and precision. The cases discussed above demonstrate that the use of AI for political aims, including repression, is no longer rare but increasingly routine. It is used to streamline the creation of malicious content such as deepfakes,

[172] Gabriel Geiger and others, 'Surveillance Secrets' *Lighthouse Reports* (14 October 2025) https://www.lighthousereports.com/investigation/surveillance-secrets/

[173] Ronan Farrow, 'How Democracies Spy on Their Citizens' *The New Yorker* (18 April 2022) https://www.newyorker.com/magazine/2022/04/25/howwere-democracies-spy-on-their-citizens

to allow intimidation campaigns to scale, and to reduce the cost of silencing dissent online altogether. This is a significant novel pattern because it changes the very nature of transnational digital repression. What once took significant human attention and time – scraping personal data, creating digital lures – can now be automated and put on repeat. AI-enabled doxxing operates behind the scenes, deepfakes are more difficult to disprove, and personalised phishing, as well as honeypots, are more convincing than ever. At the same time, AI lowers entry costs and expands the reach of repression: it makes digital surveillance more intrusive and enables platform-scale censorship that outpaces human oversight, while AI-based ranking and recommendation algorithms remain largely unaccountable to researchers and civil society.[174] These dynamics deepen distrust and place increased burdens on those targeted, as navigating modern digital spaces safely takes more and more effort. At a system level, AI-driven repression also complicates the questions of attribution and accountability. For example, it is becoming increasingly difficult to trace the true origins of automated content as it spreads online, overwhelming and exploiting platform moderation rules. For exiles in Europe, this means that cross-border digital repression becomes more adaptive, scalable, and persevering. Seeing AI as an already established amplifier of repression is, therefore, key to fully understanding the modern political environment.

## Platforms as Battlegrounds

Much of transnational digital repression now plays out on the same platforms people use and depend on for their daily communication – social networks, messengers, and cloud services. In fact, the tools of modern repression are now almost inseparable from the platforms themselves, which create spaces where trust can be built, yet just as easily exploited. As a result, the very digital environments where exiles gather are now turned against them, making repression harder to distinguish from ordinary online interaction. Platforms are turned into points of exposure through the infiltration of private groups, impersonation via look-alike accounts and honeypot attacks, and other trust-based manipulations. Even the smallest traces of digital activity, such as a like or a comment, can be reframed as evidence, reinforcing the totalitarian logic in which legal systems are so tight that everyone can be found guilty of something. Online platforms magnify this dynamic, producing a chilling effect across entire communities and deterring people from engaging via digital infrastructures. Moreover, the platforms themselves become de facto controllers of how this all plays out: whether phishing campaigns spread or defamatory content is removed is often determined by a company's own rules and enforcement capacity. Recent governance shifts highlight this: Meta announced that it would phase out its third-party fact-checking in favour of the community notes model,[175] and X (formerly Twitter) already quit the voluntary Code of Practice on Disinformation,[176] both tilting towards moderation models which are easier for political actors to exploit. This raises questions about transparency and accountability, especially for large international actors. Therefore, recognising platforms as a structural vector of repression is crucial, as it is their policies, responses, or lack thereof, that determine whether repression succeeds.

[174] International IDEA, *The Global State of Democracy 2024: Strengthening the Legitimacy of Elections in a Time of Radical Uncertainty* (International IDEA 2024) 31 https://www.idea.int/democracytracker/sites/default/files/2024-09/the-global-state-of-democracy-2024-strengthening-legitimacy-elections.pdf

[175] Chris Vallance, 'Meta Is Ditching Fact Checkers for X-style Community Notes. Will They Work?' *BBC News* (26 January 2025) https://www.bbc.com/news/articles/c4g93nvrdz7o

[176] Cynthia Kroet, 'Online Platforms Disinformation Code Going Formal, but X Is Out' *Euronews* (13 February 2025) https://www.euronews.com/next/2025/02/13/online-platforms-disinformation-code-going-formal-but-x-is-out

# Recommendations

This study has sought to provide a detailed and nuanced picture of how transnational digital repression operates today. It has mapped the expanding toolkit of repressive measures – ranging from technical intrusions and surveillance to the hybrid use of legal and regulatory instruments used to silence dissent. The analysis has shown that these mechanisms do not exist in isolation but rather form an interconnected ecosystem, where multiple tools overlap and reinforce one another to sustain a durable architecture of control. While the landscape remains deeply troubling amid the broader global decline of democratic norms, understanding the complexity and interdependence of these repressive practices is a necessary step toward countering them effectively.

Concrete and practical defences are starting to take shape. Some European host states are taking legal measures first, with Sweden's "refugee espionage" law already producing convictions for infiltrating and mapping exiled communities,[177] showcasing that cross-border intimidation can be prosecuted. Democratic oversight also matters: Pegasus inquiries in Poland,[178] together with related applications before the European Court of Human Rights,[179] show how scrutiny can trigger judicial and parliamentary reviews and set standards. Coordination between states has been improving as well. In 2023, CISA and several European partners launched a Strategic Dialogue on Cybersecurity of Civil Society Under Threat of Transnational Repression, aiming to implement joint practical protections for vulnerable groups.[180] Their High-Risk Community Protection and the Joint Cyber Defence Collaborative similarly began bringing tech firms and civil society into that effort.[181] Indeed, the tech sector can play a big role in mitigating harassment of vulnerable users and takedowns, as was seen in the case of Facebook disrupting a China-linked operation against Uyghur exiles.[182] The novel DSA act on the EU level will also ensure further accountability and risk assessment.[183] Finally, civil society has been scaling practical support: CyberPeace Institute's CyberPeace Builders pairs NGOs with volunteer experts for long-term support;[184] Access Now's Helpline and CiviCERT provide rapid response;[185] and grassroots efforts like Cyber Beaver adapt guidance for local audiences.[186] Greater focus has been put on skills, as the DRFLab's Digital Sherlock training, for example, has equipped large numbers of people with incident-response techniques, aiming to enhance community resilience.[187] Together, these diverse angles offer a real

[177] Freedom House, *Sweden: Transnational Repression – Host Country Case Study* (Freedom House, 2022) https://freedomhouse.org/report/transnational-repression/sweden

[178] Shaun Walker, 'Poland Launches Inquiry into Previous Government's Spyware Use' *The Guardian* (1 April 2024) https://www.theguardian.com/world/2024/apr/01/poland-launches-inquiry-into-previous-governments-spyware-use

[179] *Javadov and Others v Azerbaijan* App no 30573/22 (communicated on 24 September 2025); *Ganbarova v Azerbaijan* App no 45877/22 (communicated on 24 September 2025)

[180] Cybersecurity and Infrastructure Security Agency, 'Joint Statement on the Strategic Dialogue on Cybersecurity of Civil Society Under Threat of Transnational Repression' *Press Release* (30 March 2023) https://www.cisa.gov/news-events/news/joint-statement-strategic-dialogue-cybersecurity-civil-society-under-threat-transnational-repression

[181] Cybersecurity and Infrastructure Security Agency, 'High-Risk Communities' (CISA) https://www.cisa.gov/audiences/high-risk-communities

[182] Cody Godwin, 'Facebook Removes Accounts of "China-Based Hackers" Targeting Uighurs' *BBC News* (24 March 2021) https://www.bbc.com/news/technology-56518467

[183] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC [2022] OJ L 277/1 (Digital Services Act)

[184] CyberPeace Institute, 'CyberPeace Builders' https://cpb.ngo/

[185] Access Now, 'Digital Security Helpline' https://www.accessnow.org/help/

[186] Cyber Beaver (Кібер Бабёр), 'Get Help' https://cyberbeaver.help/get-help/

[187] Digital Forensic Research Lab, 'Digital Sherlocks' https://dfrlab.org/digital-sherlocks/

path towards mitigating the harms of transnational digital repression and keeping exile spaces safer.

The following section outlines key recommendations for states, platforms, and civil society actors to strengthen resilience, accountability, and protection in the face of these evolving threats.

## To States:

- Cease the use of digital, legal, and hybrid instruments to exert pressure on activists, journalists, and human rights defenders, whether such actions take place within the state's own territory or target individuals abroad.
- Guarantee effective protection from transnational repression by ensuring that relevant legal safeguards are not only recognised in principle but also implemented and accessible in practice to exiled activists residing within the state's jurisdiction. This effort must be proactive: exiled activists often find themselves in vulnerable positions, unfamiliar with local procedures, legal systems, or even the language of the host country. States should therefore ensure that information on protection mechanisms is easily accessible and communicated in a way that is understandable to exiled communities. Public authorities should not wait for victims to request support; they should actively engage with civil society and diaspora networks to reach those at risk.
- Ensure the lawfulness, transparency, and predictability of all measures that may interfere with the right to privacy and freedom of expression. Any surveillance, data access, or content-related interventions should be prescribed by law, necessary, proportionate, and subject to independent oversight.

## To Platforms:

- Continuously monitor and assess how their services are exploited by authoritarian regimes to surveil, harass, or silence activists and independent voices, including those in exile. Platforms should establish structured internal processes to identify patterns of state-linked abuse and adopt clear policies addressing the misuse of their infrastructure for repressive purposes. This may include threat intelligence partnerships, transparency reporting, and collaboration with trusted civil society experts to strengthen detection mechanisms.
- Adopt comprehensive, security-oriented operational strategies for engagement in high-risk or authoritarian markets. These strategies should go beyond basic risk assessments to include thorough human rights due diligence, mapping the potential for misuse of their services and developing mitigation plans in line with the UN Guiding Principles on Business and Human Rights.
- Respond promptly and transparently to cases of platform abuse, ensuring users can access effective protection tools such as rapid reporting channels, options to promptly delete personal data, mechanisms to block attackers' accounts, and access to digital evidence for possible legal or advocacy actions.

### To Civil Society:

- Strengthen cybersecurity expertise across the human rights community by developing localised knowledge hubs, training programmes, and capacity-building initiatives that enable activists to recognise, prevent, and respond to digital threats.
- Monitor and document threats faced by exiled activists, including incidents of transnational digital repression, and provide multi-layered support to victims, covering advocacy, strategic litigation, digital forensics, data protection assistance, and psychological or community-based resilience support.
- Form and reinforce transnational advocacy networks that facilitate coordination, information exchange, and solidarity across borders. As authoritarian regimes increasingly cooperate and share repressive tactics, civil society actors must equally enhance their cross-border collaboration, sharing knowledge, resilience strategies, and early-warning information to strengthen collective resistance to transnational repression.

A quarter of the 21st century in, a sober realisation that cyberspace is not, in fact, "naturally independent of the tyrannies"[188] has settled in, leaving the "rhapsodising about the many ways in which the internet will spread democracy"[189] behind. While digital tools enable exiled activists to preserve their voices, audiences, and platforms, the methods of silencing are evolving just as quickly. Whether or not one shares the alarmism of the internet being in a state of "imminent demise,"[190] online transnational repression is real and rampant. By hitting the less visible category of exiles the hardest, they are testing the responses of host states, their willingness to extend protection to non-citizens, and ultimately their vigilance in protecting democracy online and offline. The inertia of state and non-state actors benefits the attackers and paralyses responses to what is ultimately an attempt to radically redefine free expression online.

Human constanta

[188] John Perry Barlow, *A Declaration of the Independence of Cyberspace* (Electronic Frontier Foundation 1996) https://www.eff.org/cyberspace-independence
[189] Anne Applebaum, *Autocracy Inc* (Penguin Books 2024) 66
[190] 'Pavel Durov Warns of the "Imminent Demise" of the Free Internet' *ForkLog* (10 October 2025) https://forklog.com/en/pavel-durov-warns-of-the-imminent-demise-of-the-free-internet/