

November **2026**

Kevin Limonier
Professor at the French Institute of Geopolitics (Institut Français de Géopolitique), Université Paris 8

Maxime Audinet
Assistant Professor and holder of the chair "Influence and Counter-Influence Strategies in the Digital Context" at the Institut national des langues et des civilisations orientales (Inalco)

INSTITUT DE RECHERCHE STRATÉGIQUE DE L'ÉCOLE MILITAIRE
irsem

The Last Mile of Russian Interference

An Ethnographic and Digital Investigation in Southern Moldova

Étude n°140

Dépôt légal
ISSN: 2268-3194 | ISBN: 978-2-11-186024-7

To quote this study

Kevin Limonier and Maxime Audinet, "The Last Mile of Russian Interference: An Ethnographic and Digital Investigation in Southern Moldova," Étude 140, IRSEM, November 2026.

This study was made possible by the technical support of Cassini (www.cassini.group) and GEODE (www.geode.science).

Maxime Audinet's research chair "Influence and Counter-Influence Strategies in the Digital Context" at Inalco is funded by the French National Research Agency (ANR) and the French Ministry of Higher Education and Research.

Funded by the European Union [ERC DATAROUTES No. 101098032]. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Research Council. Neither the European Union nor the granting authority can be held responsible for them.

DISCLAIMER: IRSEM's mission is to contribute to public debate on defence and security issues. The views expressed in its publications are solely those of their authors and in no way represent an official position of the Ministry of the Armed Forces. The English version of this brief has been translated from the French version with the assistance of AI and edited by IRSEM.

Cover illustration: © Elsa Bordes Graphiste – Magnific.com.

© 2026 Institute for Strategic Research (IRSEM).

The Last Mile of Russian Interference

An Ethnographic and Digital Investigation in Southern Moldova

Kevin Limonier
Professor at the French Institute of Geopolitics (Institut Français de Géopolitique), Université Paris 8

Maxime Audinet
Assistant Professor and holder of the chair "Influence and Counter-Influence Strategies in the Digital Context" at the Institut national des langues et des civilisations orientales (Inalco)

I Publication Director
Martial FOUCAULT

I Editor
Chantal DUKERS

I Graphic design
Elsa Bordes Graphiste

Recently published

139 | The Politicisation of Central European States' Policies Towards Ukraine
David CADIER

138 | Sahel, au centre du djihadisme mondial
Alexandre LAURET et Mathieu MÉRINO (dir.)

137 | Santé mentale et guerre de haute intensité : un déterminant stratégique à ne plus négliger
Marion TROUSSELARD

136 | Les interventions HADR face aux aléas environnementaux : Enjeux scientifiques, politiques et opérationnels
Marine de GUGLIELMO WEBER, Florian OPILLARD et Carine PINA

135 | How do wars end? 'Securitisation' and the problem of victory and defeat
Hew STRACHAN

134 | Penser la durabilité à l'ère de la préparation de la guerre – La Finlande, la Suède et la Norvège au prisme de la défense durable
Marine de GUGLIELMO WEBER et Sophia MALLER

133 | Stratégies chinoises et équilibres de puissance en Océanie insulaire
Carine PINA

132 | L'écriture des constitutions en période de conflit armé – Étude interdisciplinaire
Anne-Hélène BERTANA et Yaodia SÉNOU DUMARTIN (dir.)

131 | Dissuader la Chine ? Taïwan et les États-Unis face à leurs dilemmes défensifs
Hugo TIERNY

130 | Des institutions en (r)évolution : Armée et police en Tunisie après 2011
Audrey PLUTA

About IRSEM

Created in 2009, IRSEM is the strategic research institute of the French Ministry of Armed Forces and operates under the supervision of the Directorate General for International Relations and Strategy (Direction générale des relations internationales et de la stratégie, or DGRIS). It is made up of about forty civilian and military staff, most of whom hold a doctorate. It is the main research centre on War Studies in the French speaking world, and its objective is to strengthen French research on defence and security.

The research team is divided into six departments:

• The Euro-Atlantic Region – Russia department analyzes strategic and geopolitical developments in North America, Europe, Russia and the Eurasian space, which includes Eastern Europe (Moldova, Ukraine, Belarus), the Southern Caucasus (Armenia, Georgia, Azerbaijan) and the five Central Asian countries. It focuses on power competition in this area, the changing role of NATO, maritime security and influence strategies.

• The Africa – Asia – Middle East department analyzes strategic and geopolitical developments in Africa, Asia, and the Middle East, concentrating on the following cross-cutting themes: political authoritarianism and economic liberalization in emerging countries; the role of armies and security institutions in the functioning of states and societies; strategic and regional security issues; and ideologies, nationalism, and the recomposition of regional inter-state balances.

• The Armament and Defense Economics department deals with economic issues related to defense and, more broadly, with strategic issues resulting from technological developments, problems of access to natural resources and those related to environmental issues. This research work is based on both a qualitative and quantitative multidisciplinary approach, which draws on various scientific fields: economics, history of technologies, and geography.

• The Defense and Society department is at the junction of issues specific to the military and the societal developments it faces. The following aspects are studied: the link between civil society and the armed forces; the sociology of military personnel; the integration of women in armed conflict; relations between political power and military institutions; the notion of commitment and its evolution; how youth is socialised and integrated into society; and the rise of radicalism. In addition to its research activities, the "Defense and Society Team" also intends to promote defense issues within civil society, including in academia.

• The Strategies, Norms, and Doctrines department studies contemporary armed conflict, in particular its political, military, legal and philosophical aspects. Research focuses on both its productions and its events and deals with international law, particularly technological issues (cyber, artificial intelligence, robotics); doctrines of dissuasion; arms control and the fight against proliferation; and nuclear disarmament. The transformation of international relations, the related power and security issues, as well as the philosophy of war and peace, are also part of this area of study.

• The Intelligence, Strategy foresight and Influence department conducts research on the strategic function of "knowledge and anticipation" that has been highlighted by the French White Paper on Defense since 2008. The primary ambition of this program is thus to contribute to a more detailed understanding of intelligence in its broadest sense (i.e., as information, process, activity and organization); the second is to contribute to the consolidation of analytical approaches, particularly in terms of anticipation; the third is to work on the different aspects of so-called "hybrid" warfare, in particular influence and the manipulation of information. This field underscores the hybrid character of IRSEM by circulating papers and reports that are at the intersection of academic research and open source intelligence analysis.

Biographies



Kevin LIMONIER

kevin.limonier@protonmail.com

Kevin Limonier is Full Professor of Geography at the French Institute of Geopolitics (Université Paris 8). He is a junior member of the Institut Universitaire de France and deputy director of the GEODE research centre. He also serves as scientific director of the Russian-Language Infosphere Observatory, conducted on behalf of the French Ministry of the Armed Forces, and is a member of the Russia Program at George Washington University and a founding partner of the mapping firm Cassini. He also sits on the French Defence Ethics Committee. His research focuses on developing new methods for mapping cyberspace and for digital investigation (OSINT) in the post-Soviet context (*Cartographier le pouvoir à l'ère numérique : enquêtes et explorations dans le cyberespace russe* [Mapping Power in the Digital Age: Investigations and Explorations in Russian Cyberspace], forthcoming from CNRS Éditions in 2026). More broadly, he specialises in the Russian-language internet and in territorial innovation policies in the USSR and contemporary Russia.



Maxime AUDINET

maxime.audinet@inalco.fr

Maxime Audinet is Assistant Professor and holder of the chair "Influence and Counter-Influence Strategies in the Digital Context" at the National Institute for Oriental Languages and Civilisations (Inalco). A specialist in Russian foreign policy, he holds a PhD in Slavic studies and political science from Université Paris Nanterre. He is a full member of Inalco's Europe-Eurasia Research Centre (CREE) and an associate researcher at the GEODE centre at Université Paris 8. From 2020 to 2025, he was Research Fellow on influence strategies at the Institute for Strategic Research (IRSEM).

Contents

7 **Abstract**

9 **Introduction**

A study made possible by chance discoveries in the field 11
A combined approach to the conditions of reception and circulation of Russian strategic narratives 12

18 **I. Moldova, a contested information space**

A country undergoing "de-post-Sovietization" 19
Moldova, the European Union's new frontier (and vulnerable interface) 21
The growing clandestinization of Russian influence in Moldova 22

25 **II. Porosity to Russian and pro-Russian narratives in Gagauzia, or the weaponization of marginality**

"Europe means war, Russia means peace": narrative convergence and adherence to Russian positions 25
The feeling of marginalization, fertile ground for Russian and pro-Russian strategic narratives 31

34 **III. Making narratives circulate in a hostile space**

Rudimentary techniques of information clandestinization: the case of *Komsomolskaya Pravda* (KP) 35
Growing recourse to cybercrime: the case of bulletproof hosters (BPH) and IPTV 39

48 **IV. Moldovan BPHs and IPTV: a threat to Europe?**

54 **Conclusion**

Abstract

How do Russian narratives reach their audiences in an information space that is, in theory, closed to them, and why are they received favorably there? This study addresses this twofold question on the basis of fieldwork conducted in southern Moldova in August 2025, by examining together the conditions under which Russian and pro-Russian narratives circulate and the conditions under which they are received. Through the Moldovan case, it sheds light on how Russia's interference practices are evolving, in particular their growing "clandestinization." Identified by Moscow as a vulnerability through which Europe can be reached, Moldova serves as a laboratory where various techniques are tested before being deployed in other countries. The investigation focused on Gagauzia, a southern region of Moldova that Russia regards as a breach in the EU's eastern flank, on the country's capital, Chișinău, and, to a lesser extent, on certain cyber actors in Transnistria. It combines, on the one hand, ethnographic fieldwork and interviews with national and local decision-makers and politicians, activists, journalists and ordinary citizens and, on the other hand, a digital investigation using cyber and OSINT methods.

The adherence of a considerable part of the Gagauz population to Russian strategic narratives is explained first of all by a widespread feeling of marginalization with respect to Chișinău and to Europe, rooted in a specific local history. The link between marginalization and receptiveness to Russian narratives is not peculiar to Moldova: it can be found throughout Europe, including in France. These narratives also manage to circulate in a space that is nonetheless controlled by the pro-European authorities in Chișinău, notably with the support of cybercriminal circles.

Finally, the study presents the technical autopsy of three interference operations. The first concerns Hai TV, an application designed to circumvent the blocking of Russian channels and linked to the cybercriminal group AEZA, which is itself involved in the Doppelgänger

operation[1] run by the Social Design Agency, a digital marketing company contracted by the Kremlin to conduct information interference in Europe. The second concerns equipment sold clandestinely in Moldovan markets to watch Russian channels on a television set: a reverse-engineering analysis carried out with cybersecurity students from Polytech Chambéry and researchers from the GEODE research center revealed a cybercriminal galaxy involving Russian, Chinese and possibly Iranian actors. The third operation, discovered by chance, allowed us to trace an interference operation that is still active and targets Germany and, to a lesser extent, France: it involves an operator based in Transnistria that has set up a Netflix-type service in Germany, Kartina.tv, aimed at Russian-speaking populations in Western Europe.

1. https://vsquare.org/sanctions-west-prosecuted-in-russia-aeza-still-working-in-the-eu-doppelganger/

Introduction

In November 2025, the Moldovan Prosecutor's Office for Combating Organized Crime and Special Cases (PCCOCS) charged Anatoli Prizenko with organizing "mass disorder."[1] The accusations against him are numerous: he allegedly helped organize training camps supervised by Russian military intelligence (GRU) in Bosnia and Herzegovina, in order to prepare groups meant to carry out destabilization operations in Europe. Above all, he was the man behind the well-known operation in which Stars of David were spray-painted on walls in Paris and its suburbs in late October 2023, a few days after the Hamas terrorist attacks of 7 October. In this case, Prizenko allegedly acted as an intermediary between the Russian sponsors of the operation and those who carried it out – Moldovan citizens holding Romanian passports and therefore free to travel without restriction throughout the European Union.

Beyond what it reveals about the organization of Russian clandestine operations, the Prizenko case points to the territories that Russia has identified as suitable for setting up rear bases from which to reach Europe. Besides Bosnia, the Sahel and Armenia, several document leaks suggest that Russia regards Moldova as a "vulnerable territory" from which the member states of the European Union, including France, can be reached. This is the case of the documents contained in the "SDA Leaks", analyzed in a previous study, through which the internal documentation of a Russian company specializing in organizing interference in Europe was leaked.[2] In one of these documents,

1. "Ingérences étrangères : en Moldavie, l'enquête pénale qui rencontre les affaires françaises," *Libération*, November 29, 2025, https://www.liberation.fr/checknews/ingerences-etrangeres-en-moldavie-lenquete-penale-qui-rencontre-les-affaires-francaises-20251129_O4DLE7HWKFCPNOFDELJS6KBDJQ/
2. Kevin Limonier, "La guerre numérique de Vladimir Poutine : enquête sur les hackers d'État en Russie," *Le Grand Continent*, June 17, 2025, https://legrandcontinent.eu/fr/2025/06/17/enquete-ingerence-russe-europe/

these four territories are clearly identified as bridgeheads for actions against France and its interests.

These four territories contain zones of contact between, on the one hand, networks, political orders or territories controlled – directly or indirectly – by Russia and, on the other hand, populations that can move freely within the Schengen area. In the Moldovan case, the vulnerability lies above all in the existence of Russian-speaking areas where the Kremlin's narratives are widely embraced, but also in the existence of a self-proclaimed entity, Transnistria, where nearly 5,000 Russian soldiers are stationed. It was precisely this territory that Prizenko used as a springboard, in a country where a citizen can both have direct access to Transnistria and travel freely within the Schengen area if, like about one third of the Moldovan population, he or she holds a Romanian passport. In other words, through its growing integration into the European economic and political space, Moldova is an interface that Russia now exploits to conduct operations throughout Europe. Moldova is therefore an ideal and easily accessible ground for observing, understanding and analyzing as closely as possible the changes in Russia's interference strategy in Europe, with the aim of anticipating them and thus countering them effectively.

The present study reports on two weeks of fieldwork carried out in Moldova in August 2025. This was a critical period for the country: we were a few weeks away from the September 2025 parliamentary elections, in which the pro-European coalition won a narrow majority against the political parties favoring closer ties with Russia. Interference was then at its peak, and a palpable nervousness reigned in the country.

A study made possible by chance discoveries in the field

The investigation originally had a twofold objective. On the one hand, it sought to better understand how the strategic narratives deployed by Russia are received among the Russian-speaking populations of Moldova. On the other hand, a more technical part of the fieldwork was to consist in taking telemetry measurements of the Moldovan Internet as part of the ERC project DATAROUTE,[1] in order to understand how connectivity in the region has evolved since the start of the full-scale invasion of Ukraine. These two objectives, seemingly far apart, quickly converged: the mechanisms through which these narratives were received depended largely on the ways in which they circulated, particularly in digital form, in an information space that is "constrained" for Russian actors. For example, some conversations with residents of southern Moldova revealed ways of consuming information from Russia that rely mainly on circumventing the restrictions imposed by the Moldovan authorities. One case was that of Sergei G., a young Gagauz man living in Chișinău, who explained to us that his grandparents watched Russian news channels (blocked in Moldova) through digital boxes sold illegally in the markets of Russian-speaking regions or neighborhoods. It turned out that these boxes, operated by cyber-mafias that will be discussed at length below, are a central digital infrastructure: they allow a whole aging, Russian-speaking and

1. The ERC Advanced Grant DATAROUTE, led by Frédérick Douzet at the GEODE research center (Université Paris 8), is a research project funded by the European Research Council since 2023. It studies the logical routes of the Internet, that is, the paths actually taken by digital data through networks, at the global scale. By combining mapping based on BGP routing data, the development of dedicated tools (a BGP observatory, a participatory measurement application) and field telemetry campaigns in several regions of the world, the project seeks to understand how the control strategies of state and private actors shape the architecture of cyberspace. It draws from this analyses of the resulting dependency dynamics and bottlenecks, and of the security and public policy issues they raise for the European Union. https://cordis.europa.eu/project/id/101098032

pro-Russian part of the population to bypass the controls imposed by the Moldovan state and to access Russian state media and their talking points. The same is true of certain VPNs (Virtual Private Networks), which make it possible to get around the DNS blocking put in place by Moldovan operators. The reception of Russian strategic narratives, and the support they generate among the populations we met, therefore depend to a large extent on infrastructures and practices that digitally circumvent information borders and Moldovan law.

These discoveries led us to refocus the investigation on the conditions under which Russian strategic narratives are received and circulate in an information space that is hostile to their dissemination. The question then becomes the following: through what mechanisms and under what conditions do Russian narratives circulate and find a favorable reception in a contested information space such as Moldova? Answering it requires combining two angles that are rarely brought together. The first is the local dimension – that is, the observation, at a small scale, of the geographical, sociological, economic and memory-related conditions in which the populations that respond positively to Russian narratives live. The second is the digital and cyber dimension – that is, the networks and infrastructures through which these narratives circulate.

A combined approach to the conditions of reception and circulation of Russian strategic narratives

As regards the local dimension, the interference we witnessed depends largely on the socio-economic conditions of the targeted population group. This is why we focused on a specific territory: Gagauzia. With a population of 135,000, this autonomous region in the south of Moldova is an ideal observation post for several reasons. First, because it has an ethnolinguistic and political context that is unique in the country, with a population that is 83% Gagauz and known for its pro-Russian orientation, its opposition to Moldova's integration into the European Union and its hostility toward the central government

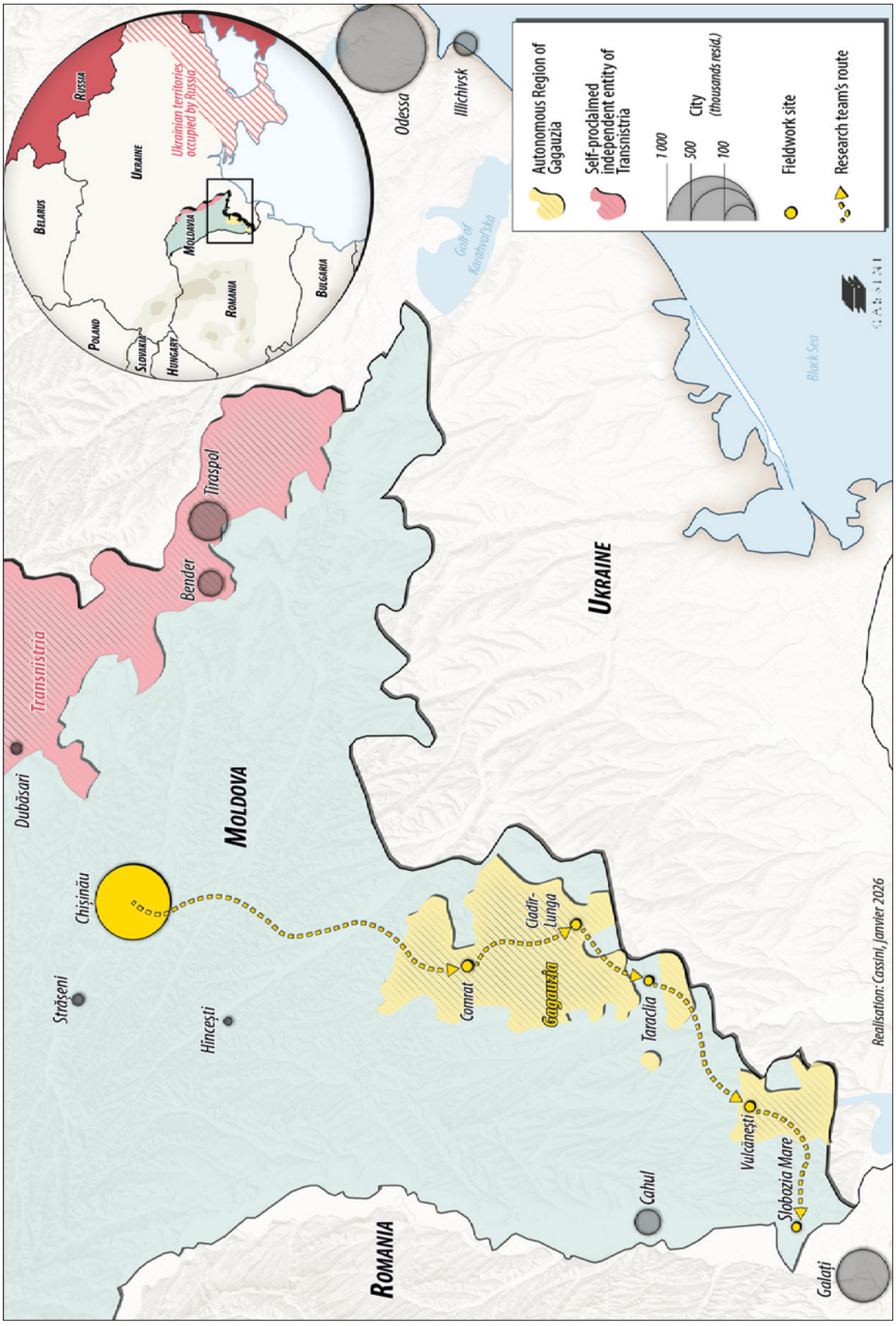
in Chișinău. Second, because, unlike the pro-Russian separatist region of Transnistria, Gagauzia is easy to access from the rest of Moldova and has received much less attention in the specialist literature.[1]

Our fieldwork therefore combined an ethnographic investigation and a digital investigation. It proceeded as follows. We spent the first three days and the last three days in the capital, Chișinău, where we met officials from several public and government agencies, heads of NGOs, journalists, Moldovan experts working in particular on foreign interference, and members of the French Embassy in Moldova. In between, we spent eight days in several towns and villages of Gagauzia and other districts of southern Moldova (Comrat, the regional capital, Ceadîr-Lunga, Congaz, Taraclia, Vulcănești and Slobozia Mare). There we observed several cultural events and venues (festivals, concerts, museums, an amusement park, etc.) and conducted interviews with local officials (town halls, houses of culture), activists and ordinary residents we met in cafés and restaurants, at markets or in front of places of worship. In total, we conducted twenty-one semi-structured or spontaneous interviews, in Russian with Russian speakers and in English with Romanian speakers. Some of these interviews are transcribed in this study. All the names of our interviewees have been anonymized.

1. This lack of research on Gagauzia is noted by Tudoroiu in his article on "failed frozen conflicts": Theodor Tudoroiu, "Unfreezing Failed Frozen Conflicts: A Post-Soviet Case Study," *Journal of Contemporary European Studies* 24, no. 3 (2016): 375–96. See also, on the way Gagauz elites use the notion of the "Russian World" (*Russkiy Mir*) for legitimation purposes: Marcin Kosienkowski, "The Russian World as a Legitimation Strategy Outside Russia: The Case of Gagauzia," *Eurasian Geography and Economics* 62, no. 3 (2021): 319–46.

I MAP 1

The poorest region in Europe's poorest country: an ethnographic study in Gagauzia



As for the cyber dimension, that is, the physical and logical infrastructures that make the Internet work, the fieldwork took place in two stages. The first, before the physical fieldwork, consisted in analyzing the general structure of the Moldovan Internet and the dependency dynamics that characterize it. This analysis relied on the tools developed by the GEODE research center as part of the ERC project DATAROUTE and deployed on the CRYSTAL platform,[1] in order to map the connections between the subsystems that make up the Moldovan Internet, as well as its connections with Moldova's neighbors. The initial objective was to identify the strategic bottlenecks of the regional Internet and the dependency dynamics that result from them. In the end, the analysis identified some highly unusual network nodes, particularly in Transnistria (see the last part of this study). The remote exploration of the regional network thus made it possible to conduct a first mapping campaign, which quickly brought out many points of interest to be examined in more depth on site.

The second part of the digital fieldwork took place in Moldova, in parallel with the ethnographic investigation. Here again, the aim was to take telemetry measurements in the field using the tools of the CRYSTAL platform developed by GEODE. Maps produced remotely from Paris lack granularity. To obtain a finer view and analysis, and to meet the scientific objectives of the ERC project DATAROUTE, fieldwork is conducted in several regions of the world, including Moldova. In practice, pings[2] and traceroutes[3] were sent from the equipment we carried with us across the country to targets located all over the

1. Kevin Limonier, Maxime Audinet, "From Restricted to Digital Fieldwork: A Renewed Methodological Framework for Russian Studies After the Full-Scale Invasion of Ukraine," *Communist and Post-Communist Studies* (2025), DOI: https://doi.org/10.1525/cpcs.2025.2474792
2. Ping is the response time taken by a data packet to make the round trip between a computer and a remote server. It is used to measure latency between two points of the network, usually expressed in milliseconds.
3. Traceroute is a network diagnostic tool that follows the exact path taken by a data packet between a computer and a remote server. It lists all the intermediate routers the packet passes through, and thus makes it possible to reconstruct the geographical path taken by a data packet between two points of the network.

world. Once collected, these data were processed by the engineers of the DATAROUTE project in order to refine the granularity of the initial maps. Alongside these measurements, a more qualitative aspect of this phase of the investigation sought to better understand how local populations access the network, as well as the strategies and representations of the Moldovan authorities and of local telecom actors regarding connectivity. The proximity of Ukraine, as well as that of Transnistria, made this dimension of the investigation necessary. It allowed us to better grasp the circumvention strategies used by Russian actors to reach Moldovan cyberspace, at a time when local cybersecurity agencies scrutinize any attempt to intrude into or manipulate national infrastructures for destabilization purposes. Several interviews with these agencies and their heads allowed us to add the representations of local cybersecurity actors to our map of the Moldovan network, and to observe how widespread the "clandestinization" of Russian interference operations had become in the country during the election period. Clandestinization here refers to the process by which the actors of influence strategies adapt to and circumvent new forms of control and surveillance of the digital and information space in order to keep operating in the environment of the targeted country, while exploiting human, cyber and infrastructural weaknesses.[1] Combining the digital and ethnographic dimensions of the fieldwork provided many illustrations of this process.

In all, this study contains the autopsy of three clandestine interference operations that show significant porosity with several Russian, Chinese and possibly Iranian cybercriminal groups, as well as ramifications in Western Europe.

The first concerns Hai TV, an application designed to circumvent the blocking of Russian television channels and linked to the cybercriminal group AEZA, which is also involved in the Doppelgänger operation.

1. Maxime Audinet and Colin Gérard, "Under the radar: Crisis, restructuring, and clandestinization of Russia's ecosystem of information influence after the invasion of Ukraine," *Réseaux* 3, no. 245 (2024): 113–152.

The second operation concerns equipment sold clandestinely in Moldovan markets to watch Russian channels on a television set. We obtained this equipment and carried out a reverse-engineering study on it with cybersecurity students linked to the GEODE research center. We uncovered a cybercriminal galaxy connecting Russian, Chinese and possibly Iranian actors.

Finally, the third operation, discovered by chance, allowed us to trace an interference operation still under way that targets Germany and, to a lesser extent, France. It involves an operator based in the separatist region of Transnistria that has set up a Netflix-type service in Germany called Kartina.tv. Aimed at the Russian-speaking populations living in Western Europe, this service notably gave voting instructions to its subscribers through advertisements in favor of the German far-right party AfD.

Ultimately, the complementarity of *in situ* ethnographic approaches and cyber approaches allowed us to confirm one of the main arguments of the geopolitics of the "datasphere"[1]: conflicts and territorial strategies can no longer be observed only through the lens of the physical world, or even of the digital world, but through the observation of the *continuum* formed by these two dimensions.

1. Frédérick Douzet, "Du cyberespace à la datasphère. Enjeux stratégiques de la révolution numérique," *Hérodote*, 177–178, no. 2 (2020): 3–15, https://doi.org/10.3917/her.177.0003

I. Moldova, a contested information space

Before presenting our investigations *stricto sensu*, it is important to return to the context in which they were conducted, as well as to the particular, interstitial position that Moldova now occupies in Europe, between decoupling from the post-Soviet world and gradual integration into the European space. It is in this particular position, between the persistence of post-Sovietism and European integration, that the country's main vulnerability lies – and it is also its great strength. This position partly explains the great virulence of Russian interference operations in the country, as well as their clandestinization, and it also provides us with an unprecedented vantage point for analyzing and anticipating the threats that may target the western part of Europe.

As mentioned above, our fieldwork took place in particular circumstances, given the imminence of the September 2025 parliamentary elections. The interference campaigns we witnessed, some of which have been widely documented, were then reaching peak intensity.[1] The stakes were indeed high for this small country of 2.3 million inhabitants. Wedged between the EU's eastern flank and Ukraine's western border, Moldova occupies a highly strategic position, especially since Russia launched its full-scale invasion of its neighbor. The first Moldovan border posts, for example, are only 150 kilometers from the major Ukrainian port of Odesa – one of Russia's main strategic targets in this war – so that the coming to power of a pro-Russian government could have had disastrous consequences for Kyiv.

1. See: Valentin Châtelet, Victoria Olari, "Paid to post: Russia-linked 'digital army' seeks to undermine Moldovan election," DFRLab, September 2025, https://dfrlab.org/2025/09/24/paid-to-post-russia-linked-digital-army-seeks-to-undermine-moldovan-election/

A country undergoing "de-post-Sovietization"

The strategic position that the war in Ukraine gives Moldova is not, however, enough to explain the violence and intensity of the interference that targeted the summer 2025 campaign. It is also due to the depth of the changes initiated by President Maia Sandu's majority since she came to power in December 2020. In both camps, the election was presented as a "historic choice" between two paths seen as irreconcilable: European integration on the one hand, and a "return" to the "Russian World" (*Russkiy Mir*) on the other.

This duality in Moldovan political life is partly the result of the success of the policies implemented by the presidential party, PAS. Since 2020, the ruling coalition has actively sought to deepen a form of strategic decoupling from Russia and, more broadly, from "post-Sovietism" – that is, the power structures, together with the practices and narratives that accompany them, sustained by the persistence of the networks that once formed the backbone of the Soviet Union. These networks, whether physical, economic, social, media-related or even family-based, share the characteristic of converging on (or passing through) Moscow, which has made them its main lever of influence in its former imperial space. Often described as post-Soviet, this space is, in the words of the geographer Jean Radvanyi, a "force field" organized around Moscow and the Kremlin.[1] It works through the convergence of a multitude of physical and immaterial networks toward the center of the former empire, where the most important decisions are made and where the political and economic allegiances that bind the peripheries to the capital are built.

Moldova was, and in some respects remains, one of these peripheries. Considered a training ground for Soviet senior officials, who gained experience there during their first postings before being sent

1. Jean Radvanyi, *"L'espace postsoviétique comme champ de forces,"* in *Les États postsoviétiques : Identités en construction, transformations politiques, trajectoires économiques* (Armand Colin, 2011): Introduction, 5–12.

to more complex theaters,[1] the country long lived in almost total economic and political dependence on Russia: an economy and political elites dependent on Moscow, structural corruption inherited from the practices of the Soviet bureaucracy, media dominated by Russian-language groups aligned with the line of the major Russian dailies, and so on.

In Moldova, as elsewhere, the persistence of post-Sovietism allows certain actors who occupy a strategic position in the networks converging on Moscow to enjoy an economic and/or political rent that has long protected them. The figure of Ilan Shor, a Moldovan oligarch now in exile in Russia, is emblematic here: he made his ties to the post-Soviet economy one of his main political assets. One may also think of the situation that long prevailed in Transnistria, a Russian-backed separatist entity, predominantly Russian-speaking and protected by some 5,000 Russian soldiers stationed there since 1992. For thirty years, and apart from the troops, Transnistria was able to survive as a viable territorial entity independent of Chișinău because it was the entry point for most of the electricity, gas and telecommunications networks that Moldova needed. These flows came mostly from Russia, through an infrastructure system designed under Soviet planning, which had made Tiraspol (the capital of Transnistria) a strategic hub for supplying the Moldavian Soviet Socialist Republic, located on the edge of the Soviet Union. As we will see later in this study, this situation allowed a whole generation of entrepreneurs and oligarchs to grow their capital by taking advantage of this strategic position, particularly in the cyber domain.

The full-scale invasion of Ukraine in February 2022 was the event that allowed Moldova to accelerate its emancipation from post-Sovietism. Here again, developments in Transnistria clearly illustrate this acceleration of history: whereas until 2023 Tiraspol supplied gas and electricity to Chișinău, and many imported goods transited through Transnistria from Odesa, the situation was abruptly reversed when Ukraine closed its border with the separatist entity and the gas

1. Mikhail Voslensky, *La Nomenklatura : Les Privilégiés en U.R.S.S* (Pierre Belfond, 1980).

pipelines were cut off. Some of the flows that structured post-Sovietism were thus suddenly interrupted, giving Chișinău a historic opportunity for lasting decoupling by betting on European integration. In the specific case of energy, it was the European Union that took over in supplying Moldova with the energy its economy needs: several high-voltage lines connecting the country to Romania made it possible not only to do without Transnistria, but above all to reverse the balance of power, so that today it is Chișinău that provides Tiraspol with the means of its subsistence, and no longer the other way round.

Moldova, the European Union's new frontier (and vulnerable interface)

This abrupt reversal of the balance of power can be found at every scale and in every domain where connection to flows of information and wealth had allowed entrepreneurs to prosper and to contribute to maintaining the "force field" of post-Sovietism. It has been strongly encouraged by a vigorous policy on the part of the ruling coalition, itself supported by the European Union and, until 2024, by the United States. In the information domain, for example, several government agencies backed by Moldova's Western allies can now block certain content and newspapers coming from Russia with a precision and resources far greater than what the Moldovan state could have on its own.

At the European level, Moldova has thus benefited from assistance and expertise that are part of a broader dynamic of gradual sealing of the EU–Russia border. Since 2022 and, to a lesser extent, since 2014, the multiplication of sanctions, the closure of physical borders, the reduction of energy and logistics corridors and the blocking of information flows coming from Moscow have formed an underlying trend followed by almost all European countries, with the exception of Slovakia and, for a long time, Hungary. In Moldova, the strategy of decoupling from post-Sovietism thus has the effect of gradually anchoring the country in this wider dynamic of decoupling.

In other words, Moldova is now a border in the sense given to the term by the geographer Jean Gottmann in the 1950s, that is, an interface between two worlds, materialized by a line – or dyad – along which control is exercised in order to limit the movement of goods, people and ideas.[1] Yet, as Gottmann points out, a border is characterized not only by the flows it restricts, but also by those it cannot stop – and there are always some.[2] We are thinking here in particular of clandestine flows, which have been inherent in the phenomenon of borders ever since the territorial state became the dominant model of power.

The growing clandestinization of Russian influence in Moldova

In our case, the "hardening" of the border between the EU and Russia, materialized by various sanctions and blocking measures that limit the movement of the goods, people and ideas that structure post-Sovietism, has pushed part of these flows underground – that is, from the legal to the illegal exploitation of certain digital, political or economic networks. At another scale, the same logic can be seen in the shadow fleet that allows Russia to export its hydrocarbons despite sanctions, or in the cyber tactics – fragmentation of their digital ecosystems, creation of dozens of mirror sites – used by Russian media outlets such as RT and Sputnik to keep disseminating their content in the EU despite the ban. As a territory at the interface with the post-Soviet world, Moldova is necessarily a privileged place for organizing or channeling such clandestine flows, particularly in the information and digital fields.

Moldova's position as an interface therefore makes it particularly permeable to all kinds of strategies and tactics for circumventing the

1. Jean Gottmann, *La politique des États et leur géographie* (Éd. du CTHS, 2007).
2. Lucas Muscara, "Les mots justes de Jean Gottmann," *Cybergeo: European Journal of Geography*, CNRS-UMR Géographie-cités 8504, March 26 , 1998, DOI: 10.4000/cybergeo.5308, accessed 27 April 2021.

limits placed on the flows that still bind it to the post-Soviet "force field." These strategies and tactics are part of this process of clandestinization, particularly in the information domain. Here, clandestinization consists in a transformation of influence practices under the constraint of the restrictions imposed by the targeted states.[1] This is what has been happening across Europe since the start of the full-scale invasion of Ukraine in February 2022. The blocking of the Russian state media RT and Sputnik in most European countries, together with the emergence of proactive policies against foreign digital interference, has led Russia to turn to new actors whose specialty is precisely to cover their tracks and to exploit systems, infrastructures or networks that lie at the margins of the field of vision of the authorities and of counter-interference services.

Ultimately, clandestinization is a territorial process: it consists in circumventing the "hardening" of the continent's information borders since 2022, and thus in penetrating European space by exploiting loopholes in control mechanisms. More generally, it is a matter of slipping into the interstices of the territorial control exercised by a state, and thus of playing with the way power meshes space, to borrow the approach developed in the 1980s by the Swiss geographer Claude Raffestin.[2] In the digital age, the strength of such a strategy lies in the attacker's simultaneous exploitation of the countless networks that constitute as many topological dimensions of the space that a state must monitor to ensure its security and sovereignty. In other words, the digital revolution has abolished neither borders nor territory: on the contrary, it has projected them into an infinite number of new digital dimensions, where circumvention strategies are now played out.

In Moldova, the clandestinization of Russian influence takes place not only in physical space, but also in the cyber and ideational dimensions. It generally involves exploiting margins to reach the center: socio-economic and territorial margins in the case of Gagauzia; political and ideational margins in the case of the narratives being

1. M. Audinet and C. Gérard, "Under the radar."
2. Claude Raffestin, *Pour une géographie du pouvoir* (Librairies techniques, 1980).

promoted, which, besides being often conspiratorial, run counter to those on which the legitimacy of Moldova's European integration policy rests. There are also cyber margins, with the use of cyber-criminal groups that de facto become disseminators of narratives manufactured by Russia, and, finally, infrastructural margins, with the exploitation of devices such as IPTV boxes (which allow digital television to be received at home). These margins fall outside the ideal type of an information war that is too often viewed only through the lens of social media.

II. Porosity to Russian and pro-Russian narratives in Gagauzia, or the weaponization of marginality

The study of these clandestine flows must be linked to that of the adherence of certain populations to the political project offered by Russia. While other levers are generally used (corruption, coercion, compromising material, etc.), the structural nature of pro-Russian sympathies within part of the Moldovan population calls for an explanation. It requires looking at the porosity to Russian narratives of a significant part of Moldovan public opinion, particularly the part that does not identify with Maia Sandu's political choices. More generally, the aim here is to consider the competition between political ideas and antagonistic narratives in Moldova, an interface zone where radically different worldviews clash. The autonomous region of Gagauzia offers a privileged field for bringing to light this porosity, the conditions under which these narratives are received, and the vulnerabilities associated with them. This is why the ethnographic part of the investigation and the interviews were conducted in this region of southern Moldova, which borders Ukraine's Odesa oblast and has 135,000 inhabitants, of whom 83% are Gagauz, 5% Bulgarians, 5% Moldovans and 3% ethnic Russians (2014 census).

"Europe means war, Russia means peace": narrative convergence and adherence to Russian positions

The testimonies collected in Gagauzia are striking in how closely they echo the recurring narratives spread by Russia or its allies. The examples transcribed below, although often intertwined, fall into four categories: nostalgia for the Soviet Union and its socio-economic

model; adherence to Russia's positions, its worldview, its values and its narrative of the war in Ukraine; criticism of the European Union and of liberal and progressive values; and criticism of Moldova's central government.

We are Gagauz. We have a genetic memory. We have always had very good relations with the Russians. We like Europe too, but we like Russia more. Because it was the Russians who came here, who built schools for us, who built this House of Culture. When the USSR collapsed, we cried. We really cried. We were thrown back a hundred years. Everything was sold off: the Turks and the Romanians came and bought our carpets for next to nothing and resold them for a fortune.

Polina A., employee of a cultural institution, Comrat, 24 August 2025

I was brought up with a sense of dignity, the feeling that I am not inferior to others. And do you know when I understood that best? When, after the collapse of the Soviet Union, with my degree in cultural studies, I went to Turkey to earn a living because there was absolutely nothing left here. (...) What shocked me was that, since I was a maid, I had to keep my head down and not raise my eyes. That didn't exist in the Soviet Union, I had never experienced it. We spoke to each other as equals. We were taught to respect our elders, of course. But not servility. This sense of dignity is precisely something we acquired in the Soviet Union, not today. What worries me today is that even at school they teach that individual rights come first.

Maria P., head of a cultural institution, Congaz, 25 August 2025

I'm for the Russian World. I can explain why. I was born in the Soviet Union. Under the Russians, it was like this: everyone worked, everyone got a salary. The clothes were different, we didn't have yours, all right. And now? The European Union. For 30 years they've abandoned us, not a single factory built, 30 years! Since independence.

Mikhail B., resident of Congaz, 25 August 2025

We all went to Russian schools, we grew up with Russian literature and culture. Gagauz culture has its own identity, but it was in Russian culture that we were formed. Here you find people who don't know their own culture, but they always know Russian culture.

Polina A., employee of a cultural institution, Comrat, 24 August 2025

As some Gagauz have said, perhaps there is already somewhere in our genetic memory a gratitude toward Russia for accepting us as equals of the whole world community. Not as an appendage of another people, but as full equals.

Maria P., head of a cultural institution, Congaz, 25 August 2025

When the Russians need something, people talk about democracy, and afterwards they shut them out. 'We are whiter than white', 'they are all black' – no, everyone is the same! Enough. The Russians will end up pressing the button and bombing everything. They are patient, but there are limits. They'll bomb France, everyone, us too. This has to stop. I'm telling you as an old man, it will end badly [...]. In one year, maybe in ten years. But Russia is not alone. China, India, Brazil are with it. If NATO attacks Russia, everyone will rise up. Don't think that Russia is alone.

Mikhail B., resident of Congaz, 25 August 2025

A: Guys, Europe means war, it means NATO!
Q: Who started the war [in Ukraine]?
A: The Europeans, the Americans [...]. Russia has nothing to do with it.

Anonymous passer-by, resident of Ceadîr-Lunga, 23 August 2025

We are Christians, Orthodox. Our values are these: the family, the husband, the wife, the children, marriage, the grandchildren who come to visit. Traditional values, as they say. And in Europe, what is going on? They play ping-pong in the churches because nobody goes there anymore. [...] You don't look like you'd marry a man, you don't have time for that. But over there where you live, people are turning into animals without realizing it. It's not normal. Europe is Sodom and Gomorrah. Do you know why God burned Sodom and Gomorrah?

Mikhail B., resident of Congaz, 25 August 2025

A vegetable seller we met at the market in Ceadîr-Lunga, a small Gagauz town on the border with Ukraine, suggested that "people here want to be occupied by Russia" and that "Kishinev [the Russian name of Chișinău] wants to make Moldova NATO's rear base" (23 August 2025). A pacifist discourse, combined with a strong attachment to maintaining ties with Russia, attachment to Moldova's constitutional neutrality and a massive rejection of the foreign policy choices of Maia Sandu's government, was also widespread in our conversations. Some remarks were conspiratorial: Mikhail B., quoted above, claimed that "Western elites are Satanists and pedophiles."

On 23 August 2025, we also spoke with Moldovan activists – including Gagauz activists – in favor of Moldova joining the European Union, who had come to canvass in the town of Ceadîr-Lunga. The slogan "*Rossiya! Rossiya!*" ("Russia! Russia!") was chanted several times as they passed by, while they were handing out leaflets. Some passers-by called them "traitors" (*predateli*), a term often used to discredit supporters of closer ties with the European Union or of Maia Sandu's government. Sergei G., one of these activists, who lives in Gagauzia, shared with us his view of the causes of pro-Russian sentiment in the region:

> *Here in Gagauzia, there is respect for the elderly, for parents and grandparents. It's a tradition. And our grandparents tell us [that we must love Russia]. That's all. 'Everything was better before', that's what they tell us.*
>
> *People here are afraid of anything new. They are used to the past. They are used to a firm hand. But if Russia takes charge of what is new, they will be ready. Whatever Russia says, they will do it.*
>
> *The mentality is a bit different. People live in a completely different information bubble, they have always watched Russian television. I used to watch it myself when I was younger. These channels were banned, but no alternatives were offered, even though many people don't speak Romanian. So people buy decoders that come directly with a VPN [to keep watching Russian television].*

Q: Why is pro-Russian sentiment stronger here than in the other regions of the country?

A: Because we were isolated for a long time. For thirty years, Kishinev had absolutely no need for us. The former politicians were not interested in Gagauzia. They didn't teach us Romanian. They didn't care. The current government has a different approach. But if this had happened ten years earlier, everything would have been different. Now it's very difficult.

Conversely, when we asked him about the reasons for the hostility toward Moldova's European orientation, Sergei answered:

[People think that the Europeans] are going to sell our land to the Americans. We will be cannon fodder in the war against Ukraine. Our children will become gays, lesbians, transsexuals. All the food will be full of chemicals and GMOs. And local trade won't work anymore, because the European leaders will come and beat us. They also say that the Romanians will come and beat us up. It already happened a long time ago, the Romanians didn't like us. They say they will come and beat us with sticks.

These testimonies are consistent with the results of a survey conducted by Kyle Marquardt in 2023.[1] It shows the clear popularity that Russia enjoys in Gagauzia. Russian is the predominant language, with 98% of respondents saying they use Russian all the time or often, ahead of Gagauz (74%) and Moldovan/Romanian (12%). According to this survey, Vladimir Putin is the favorite political figure of respondents in Gagauzia, with 87% support (against 6% for Maia Sandu), while 90% of them consider that Russia is governed more democratically than, or as democratically as, Moldova. However, the majority support of the Gagauz population for the Russian leader and political system does not translate into massive support for Russia's invasion of Ukraine (only 30% approve of it).

Hostility toward the central government in Chișinău is obvious in Gagauzia, where 95% of voters rejected Moldova's pro-European orientation in the 2024 referendum. In the September 2025 parliamentary

1. Kyle L. Marquardt, "What Does Support for Russia Mean? Evidence from Gagauz Yeri, Moldova," November 2023, https://www.ponarseurasia.org/what-does-support-for-russia-mean-evidence-from-gagauz-yeri-moldova/#_ftn1

elections, PAS received only 3.19% of the vote there, its worst result (compared with 29% in Transnistria). This observation, which is already well established, raises a broader question: why is Gagauz society so porous to the strategic narratives shaped by Russia and its proxies, which reach a wide audience and enjoy broad approval?

In recent years, a dynamic strand of research on the reception of disinformation and influence operations has examined, on the basis of the Russian case, the conditions that explain the persuasiveness of Russia's strategic narratives. Several findings have emerged. On the basis of a survey conducted in Sweden on narratives produced by the Russian state outlet Sputnik, Charlotte Wagnsson and Magnus Lundström showed that these narratives could be perceived as credible by people with no first-hand experience of the topic, but that their effects on behavior and preferences were much stronger when they were accepted and appropriated by their audiences.[1] Russian strategic narratives are thus all the more effective when they connect with local political myths, as Olivier Schmitt shows in the case of French elites.[2] Taking the case of Ukraine, other researchers show that these narratives work better when they echo the historical and memory references of the targeted audiences,[3] or when they are disseminated by a narrator with whom the recipient shares cultural and identity ties.[4] In a different dimension, Maxim Alyukov shows that adherence

1. Charlotte Wagnsson, Magnus Lundström, "Ringing true? The persuasiveness of Russian strategic narratives," *Media, War & Conflict* 16, no. 3 (2023): 383–400.
2. Olivier Schmitt, "When Are Strategic Narratives Effective? The Shaping of Political Discourse through the Interaction between Political Myths and Strategic Narratives," *Contemporary Security Policy* 39, no. 4 (2018): 487–511.
3. Natalia Chaban, Svitlana Zhabotynska, Michèle Knodt, "What makes strategic narrative efficient: Ukraine on Russian e-news platforms," *Cooperation and Conflict* 58, no. 4 (2023): 419–440.
4. Joanna Szostek, "The Power and Limits of Russia's Strategic Narrative in Ukraine: The Role of Linkage," *Perspectives on Politics* 15, no. 2 (2017): 379–395; Vera Tolz, Stephen Hutchings, "Truth with a Z: Disinformation, War in Ukraine, and Russia's Contradictory Discourse of Imperial Identity," *Post-Soviet Affairs* 39, no. 5 (2023): 347–365.

to these narratives is all the stronger when their dissemination is synchronized across traditional and social media.[1]

The fieldwork in Gagauzia shows that most of these conditions are met, which favors the circulation and appropriation of, and adherence to, Russian and pro-Russian strategic narratives among part of the Gagauz population. This study adds one more condition to this literature: a widespread feeling of marginalization within this population, which is extensively instrumentalized by Russian and pro-Russian actors.

The feeling of marginalization, fertile ground for Russian and pro-Russian strategic narratives

One of the main findings of this study is the deep instrumentalization – or even weaponization – by Russia and by pro-Russian actors in Moldova of a real, exaggerated or imagined feeling of marginalization and exclusion among the Gagauz population. These conditions form both a receptive ground for Russian interference and a critical vulnerability for Moldova and, by extension, for Europe. The interviews conducted on site reveal four types of marginalization: political, identity-based, memory-related and socio-economic.

a) **Political marginalization**, based on the conviction that Gagauzia is excluded from public decision-making, which is monopolized by "Chișinău," and that the region's elites are repressed by the central authorities. The arrest in Chișinău in March 2025 of the pro-Russian head of Gagauzia (*bashkan*), Evghenia Guțul, on corruption charges linked to the businessman Ilan Shor, did much to fuel this feeling in Gagauzia.

1. Maxim Alyukov, "News reception and authoritarian control in a hybrid media system: Russian TV viewers and the Russia-Ukraine conflict," *Politics* 44, no. 3 (2021): 400–19.

b) **Identity-based, ethnolinguistic and cultural marginalization**, according to which the Gagauz are discriminated against, their culture erased by Romanian-speaking and "unionist" Moldovan elites (supporters of unification with Romania), and their (often conservative) values threatened by the liberal and progressive orientations attributed to the European Union. This feeling, the most pervasive one, is easily grafted onto the Russian conservative narrative that defends "traditional values" and the heteronormative family against the "liberal West" and its "Gayropa" project. Although its conservative dimension is not obvious, the "Gagauziya Land" amusement park built in the Gagauz village of Congaz with financial support from Ilan Shor clearly presents itself as a project to support Gagauz families. It is one of several projects presented as "humanitarian" by local actors who also say they are ignored by the central authorities in Chișinău.

c) **Memory-related marginalization**, based on a persistent nostalgia for the Soviet period, on the rejection of government policies banning Communist symbols (banned in 2012 by a law later ruled unconstitutional in 2013) and Russian symbols (ban on the St George ribbon, a symbol of Russian patriotism, in 2022), and on the rejection of the Romanian nationalist narrative, in a country marked by strong "competing narratives",[1] especially about the Second World War. The preservation of Soviet heritage in Gagauzia (statues of Lenin, "Lenin streets/avenues," Soviet symbols, monuments to the glory of the "Great Victory" of 1945, "Houses of Culture") is much more extensive than in the rest of the country. Here again, this feeling echoes the Russian memory narrative of the "Great Patriotic War," which is the real cement of contemporary Russian patriotism.

1. Florent Parmentier, "Le 9 mai vu de Moldavie : une 'mémoire Smuglyanka'," *The Conversation*, May 7, 2020, https://theconversation.com/le-9-mai-vu-de-moldavie-une-memoire-smuglyanka-137760

d) **Socio-economic marginalization**, in a predominantly rural region that is among the poorest in the country.[1] The precariousness of a large part of the population creates opportunities for influence entrepreneurs such as Ilan Shor, who is suspected of buying the support of part of the population (especially pensioners) through bribes meant to make up for the lack of state assistance and presented as "humanitarian aid."

While this "feeling of marginalization" must always be put in context, its recurrent exploitation by Russian and pro-Russian actors in Moldova provides an analytical framework that can be applied to other spaces exposed to Russia's influence and interference strategies in Europe. Reception conditions similar to those in Moldova can thus be observed in other countries with significant Russian-speaking minorities, such as Latvia, Estonia, Lithuania, Ukraine, Belarus or Germany. Beyond these populations, the instrumentalization of "marginalized publics" (politically, socially, in terms of identity...) in Europe by Russian influence actors is a vulnerability that it would be unwise to neglect.

1. According to Moldova's National Bureau of Statistics, GDP per capita in Gagauzia was about 3,100 euros in 2023 (61,000 Moldovan lei), compared with 6,200 euros for the country as a whole (123,000 lei) and 14,000 euros (278,000 lei) for the capital, Chișinău. See: Biroul Național de Statistică al Republicii Moldova, Conturi Naționale 2024 și Conturi Regionale 2023 [National Accounts 2024 and Regional Accounts 2023], Chișinău, 2026, https://statistica.gov.md/files/files/publicatii_electronice/Conturi_nationale/Conturi_Nationale_ed_2025.pdf

III. Making narratives circulate in a hostile space

Strategies and tactics of information clandestinization

The instrumentalization of a heterogeneous feeling of marginalization is a resource through which Russia tries to maintain the support of part of the Moldovan population. Yet this capacity for influence could not work without networks able to circulate Russian strategic narratives effectively. The ability to reach such populations has therefore become a major geopolitical issue for Moscow, in a context of "borderization" through which Moldova seeks to reduce the intensity of the flows (of information, money, etc.) coming from Russia.

To achieve this, Russian or pro-Russian Moldovan actors show creativity. They must circumvent an increasing number of blocking measures and get around the various limits that Moldova and the European Union try to impose on them. The physical and digital fieldwork allowed us to identify several types of "clandestine" tactics for circumventing information blocking, notably through the exploitation of technical and cyber vulnerabilities. These tactics range from the most rudimentary to the most sophisticated, and they are part of an overall strategy whose aim is not only to reach Moldova's Russian-speaking populations, but also to use them as a springboard toward Western Europe.

Rudimentary techniques of information clandestinization: the case of *Komsomolskaya Pravda* (KP)

In most cases, the circumvention tactics developed by Russian actors seek to exploit vulnerabilities that are both geopolitical and cyber-related, so that physical and digital actions end up closely linked. This is the case, for example, of the media outlet *Komsomolskaya Pravda* (KP), which since 2023 has opted for clandestine distribution in the country, for both its digital and its print versions. Founded in 1925 and present throughout the Russian-speaking world, *Komsomolskaya Pravda* has evolved over the past fifteen years or so toward a format comparable to that of the British tabloids. Its readership comes from the former Soviet working classes, but the newspaper's editorial line has gradually radicalized as official Russian positions have evolved since 2014.

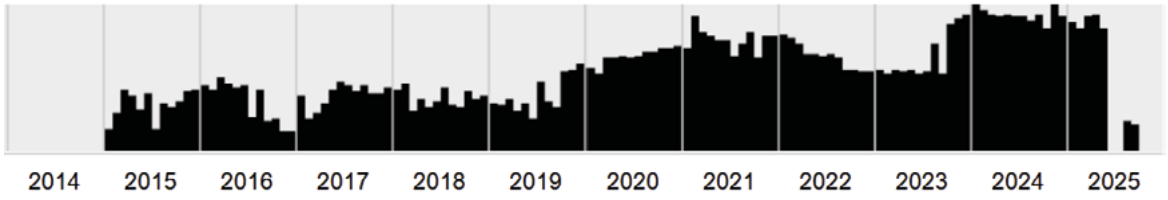
In June 2023, the Moldovan edition of *Komsomolskaya Pravda* came under the control of the company Media Contact, owned by the businessman Ilan Shor.[1] A few weeks later, in October, the Moldovan authorities decided to block the outlet in the country. This resulted in two separate measures. First, the print version of KP stopped being distributed after its main distributor to Moldovan newsstands terminated its contract with the Russian-language newspaper – officially for non-payment. This was a significant measure, as KP's aging readership is attached to the print version. Second, the digital version of the newspaper saw its domain, kp.md, shut down at the request of the national telecommunications regulator. This action went much further than the one taken by European authorities against RT and Sputnik when the dissemination of these media in the European Union was suspended in March 2022. In the case of RT and Sputnik, operators in

1. "Imperiul lui Șor. Posturile TV, ziarele, site-urile, canalele de Telegram [Shor's Empire: TV Channels, Newspapers, Websites and Telegram Channels]," NewsMaker, October 4, 2023, https://newsmaker.md/ro/imperiul-lui-sor-posturile-tv-ziarele-site-urile-canalele-de-telegram

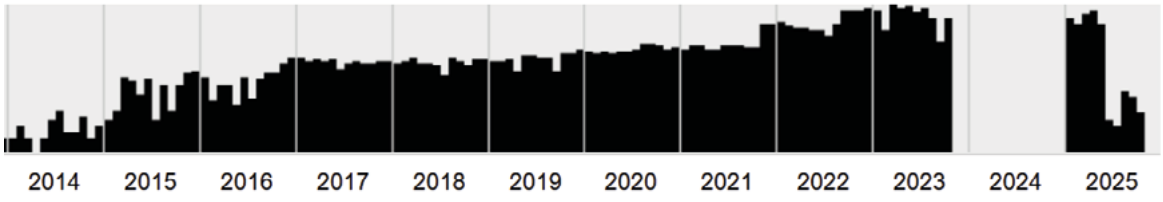
the various EU countries simply blocked the domains, which therefore remain accessible through VPNs.[1]

In the case of the Moldovan KP, the authorities went much further, since they deleted the domain itself. The Moldovan government thus wiped out the website by acting directly on the DNS: the IP address of KP's server suddenly no longer corresponded to anything, since the domain kp.md no longer existed. This was made possible by the fact that KP had chosen a .md domain name for its Moldovan edition, and this top-level domain is managed by STISC, the national information and cyber security center of the Republic of Moldova.

I FIGURE 1
Availability of the domain fr.sputniknews.com on the Wayback Machine



I FIGURE 2
Availability of the domain kp.md on the Wayback Machine



The domain's return in early 2025 corresponds to its purchase to host an AI-generated news website that apparently has no connection with Komsomolskaya Pravda.

1. Maxime Audinet, *Un média d'influence d'État : Enquête sur la chaîne russe RT* (INA, 2024).

On 30 October 2023, STISC thus terminated the kp.md domain, as can be seen in the domain availability graph from the *Wayback Machine*. The difference with the French strategy of blocking fr.sputniknews.com, the domain of the French-language edition, is clearly visible. Since the French state had no power to have a domain name ending in .com deleted, this domain remained available long after it was blocked in Europe in March 2022.

Faced with the deletion of its domain, the newspaper acted quickly to get around the measure. Within 24 hours of its entry into force, *Komsomolskaya Pravda* had set up a proxy infrastructure so that its Moldovan readers could keep accessing the newspaper despite the ban imposed by the Moldovan authorities. In practice, KP's engineers did two things. First, on 31 October 2023, they bought a new domain name, kp.media, which was therefore not blocked by the Moldovan authorities and which these authorities have no power to delete. Second, they created a proxy server dedicated to Moldova, kpmd-proxy.kp.ru, which itself points to an IP address belonging to the parent company of *Komsomolskaya Pravda* in Russia.

This technique represents the rudiments of information clandestinization: it had in fact already been used by RT and Sputnik after their historical domains (rt.com and sputniknews.com) were blocked in Europe. However, apart from the nature of the action – deleting the domain in the Moldovan case rather than simply blocking it – there are several differences in the circumvention method used in these two cases.

The first is the time it took the Russian outlets to switch to alternative domains: in the case of Sputnik, five days passed between the blocking of sputniknews.com in France (3 March 2022)[1] and the purchase of the outlet's main alternative domain, sputniknews.africa (8 March 2022).[2] In the case of KP, less than 24 hours passed between the deletion of kp.md and the purchase of kp.media to replace it.

1. M. Audinet and C. Gérard, "Under the radar."
2. See the GoDaddy website: https://ie.godaddy.com/whois/results.aspx?itc=dlp_domain_whois&domain=sputniknews.africa

This shows that Russian media are now more experienced with this domain-circumvention tactic, since they react faster. It also suggests that they buy their domains at the last minute to prevent their adversaries from engaging in typosquatting.[1]

The second difference with RT and Sputnik is the persistence of KP's physical footprint in the Moldovan media landscape. In the case of the Russian state media in France, these were pure players with no print activity, which were quickly placed in judicial liquidation. In the case of KP, a legal gray area allowed the print newspaper to continue to be distributed in some parts of the country, despite the bans. While KP cannot be found at newsstands in the capital or in the Romanian-speaking parts of the country, the same is not true in Russian-speaking regions such as Gagauzia, where the distribution of KP's print version has even been staged. We observed this on the main square of Comrat, the capital of Gagauzia, where a red kiosk bearing the KP logo occupies a visible and central spot. Opened in summer 2024, this kiosk sells only KP and coffee to go. In August 2025, the kiosk was still active, with a large LED screen showing the address of the alternative domain kp.media together with the slogan "We are back!". This peculiarity is due to the fact that KP is not formally banned in the country: its print distribution and access to its digital version are merely obstructed, so that an entrepreneur who decides to open a kiosk to distribute the newspaper on his own account will not be bothered. In the case of the Comrat kiosk, details are scarce, but everything points to an initiative funded by Ilan Shor, with print distribution run at a loss for the duration of the election period.

1. The French agency VIGINUM defines typosquatting as "a modus operandi consisting in impersonating well-known websites by registering a domain name very close to the official domain name (e.g. lefigaro[.]me instead of lefigaro.fr, or washingtonpost[.]ltd instead of washingtonpost.com)" (our translation). See: VIGINUM. 2025. *Protéger le débat public numérique en contexte electoral : guide de sensibilisation à l'attention des équipes de champagne*, Paris: Secrétariat général de la défense et de la sécurité nationale (SGDSN).

Growing recourse to cybercrime: the case of bulletproof hosters (BPH) and IPTV

The circumvention tactics used in the KP case to reach the Gagauz audience remain technically rudimentary. Other operations analyzed in the field, by contrast, reveal networks that use far more sophisticated techniques, potentially with ramifications throughout Europe. Unlike those used by KP, these advanced techniques do not act only on the DNS by using alternative domains. They also, and above all, act on the layers of cyberspace located below the DNS, and more specifically on the layer concerned with the allocation of IP addresses, by using alternative servers and autonomous systems known as bulletproof hosters (BPH). A BPH is a pirate infrastructure whose purpose is to be immune to injunctions from the authorities: its whole organization is designed so that its administrators remain untraceable, while its infrastructure is highly mobile. BPHs are thus used to support all kinds of illegal or illicit activities, whether hacking, child sexual abuse material or illegal online gambling. In practice, BPHs use IP address ranges abandoned by their owners and take over disused autonomous systems to host their infrastructure. This is therefore a form of cybersquatting.

The use of BPHs in information campaigns is recent: until 2022–2023, most known Russian interference actors used "legitimate" infrastructures. They tried to hide neither their existence nor the identity of their administrators. The media outlets funded by Prigozhin, for instance, used dedicated infrastructures rented or bought from well-established hosting companies. Others, such as the galaxy of fake media outlets promoted by InfoRos in 2022–2023, did not bother to erase their tracks, since the whois records clearly identified entities linked to the GRU.[1] As for RT and Sputnik, they were, and still are,

1. EU DisinfoLab, "How Two Information Portals Hide Their Ties to the Russian News Agency InfoRos," EU DisinfoLab, June 15, 2020, https://www.disinfo.eu/publications/how-two-information-portals-hide-their-ties-to-the-russian-news-agency-inforos/

hosted on the infrastructures of their respective holding companies, TV-Novosti and Rossiya Segodnya.

The situation changed in the aftermath of the full-scale invasion of Ukraine, with the multiplication of operations seeking to hide their nature and their sponsors more effectively. The first known use of a BPH by a Russian information interference actor thus dates back to 2022–2023, with the Doppelgänger operation. In a technical report, the Swedish NGO Qurium showed how some of the entities involved in this vast and still ongoing campaign were hosted on, or transited through, an autonomous system called "*the Evil Empire*."[1] Qurium's researchers were able to show that this name concealed a whole infrastructure of interconnected autonomous systems designed to mislead the cybersecurity engineers whose job is precisely to detect BPHs and disconnect them from the network.

The pirate application HaiTV, a textbook case of the entanglement between interference operations and cybercriminal groups

In Moldova, the use of BPHs is massive and is the cornerstone of many operations that took place in summer 2025. A particularly telling example is the HaiTV application, which has links with the Doppelgänger infrastructure. HaiTV is a mobile application for watching television directly on a smartphone or on a website through the IPTV protocol, which is widely used to stream video illegally. Many clandestine IPTV services exist around the world, in particular to watch pay-TV channels for free (especially those showing football matches). In the case of HaiTV, however, the aim is not to offer Moldovan users a way to watch their favorite teams' matches for free and illegally, but rather to circumvent the blocking of Russian channels decided by the Moldovan authorities as part of the decoupling from post-Sovietism discussed above. Although HaiTV, objectively speaking, never stresses this point, the timing and nature of its communication, as

1. Qurium Media Foundation, "How Russia Uses EU Companies for Propaganda – Exposing The Evil Empire of Doppelganger Disinformation," Qurium Media Foundation, July 11, 2024, https://www.qurium.org/alerts/exposing-the-evil-empire-of-doppelganger-disinformation/

well as the way its technical infrastructure works, prove that it is an interference operation designed to give Moldovan citizens who wish to do so the technical means to circumvent the blocking measures put in place by the state in the context of the autumn 2025 elections. During August 2025 (that is, four weeks before the vote), text messages were sent massively to the Moldovan population from a Russian number, encouraging them to use HaiTV to access the Russian channels banned in Moldova. In the Russian version of the text message sent to Moldovans, HaiTV promotes an application that gives access "to the best channels, honest reporting, objective information and popular programs". The subtext of this clandestine advertisement echoes the strategic narratives discussed above: it implies that there is censorship in Moldova.

A brief OSINT analysis of HaiTV's infrastructure reveals links with an ecosystem of BPHs involved in other interference operations, notably in France. The application's main mirror site was accessible at the IP address 95.181.173.105, which belongs to the autonomous system AS210644, known as AEZA INTERNATIONAL LTD. AEZA is far from unknown in the field of BPHs and interference: besides being now sanctioned by the British and US governments for hosting numerous cybercriminal activities,[1] AEZA is directly linked to "the Evil Empire", the infrastructure that supported the Doppelgänger operation.[2] The operation thus gets around the limits imposed by the Moldovan state on its information space by using cyber "guerrilla" tactics that combine the use of cybercriminal structures with aggressive SMS marketing strategies.

1. "Les États-Unis sanctionnent Aeza Group, un fournisseur de services russe utilisé par les cybercriminels," *Le Monde*, July 2, 2025, https://www.lemonde.fr/pixels/article/2025/07/02/les-etats-unis-sanctionnent-aeza-group-un-fournisseur-de-services-russe-utilise-par-les-cybercriminels_6617365_4408996.html
2. "Exposing The Evil Empire of Doppelganger Disinformation," Qurium, July 2024, https://www.qurium.org/alerts/exposing-the-evil-empire-of-doppelganger-disinformation/

Cyber autopsy of a clandestine device: uncovering a possible Russian-Iranian-Chinese cybercriminal network

The HaiTV example is not an exception in Moldova. In a country where a large part of the population is aging and keeps information consumption habits inherited from the pre-digital era (print newspapers, television), IPTV services that circumvent the blocking of Russian channels are a major economic and strategic issue. Home devices for receiving Russian channels are therefore widespread in the country and very easy to find on the black market, in small shops usually located on the outskirts of towns. They allow a whole aging population used to television to access Russian channels and their regime of truth. In Gagauzia, a region largely deserted by its young people, such practices are very widespread, so that IPTV boxes are a case study of prime importance.

We obtained one of these devices and set about dissecting it in order to understand which actors benefit from this highly political trade. In practice, we had someone buy, at a market in southern Moldova, a Chromecast-type device containing a paid application that gives access to all the channels available on the territory of the Russian Federation. This type of device takes the form of a small box with a Wi-Fi antenna and an HDMI port that plugs directly into a television. To work, it requires a subscription, which is paid in cash to intermediaries present in the markets. With the help of a group of cybersecurity students from Polytech Chambéry (Université Savoie Mont Blanc) and of the GEODE research center, we took the device apart and carried out a reverse-engineering exercise after subscribing for one month on site.[1]

We studied the internal source code of the applications installed on the Chromecast, as well as all the signals that the device exchanges

1. We are very grateful to Maxence Ambert and Louis Amoudruz, cybersecurity students at Polytech Chambéry, and to their supervisor Paul Mathieu, PhD candidate in computer science at the GEODE research center. As part of their practical coursework, they carried out this reverse-engineering work, which was decisive for our demonstration.

over its Wi-Fi connection once it is plugged in to watch Russian channels. The second method proved the more productive. By scanning the device's incoming and outgoing traffic with the Wireshark software, we identified several IP addresses with which the device communicates, and which themselves point to BPHs with a murky profile. Among the mass of IP addresses with which the device constantly exchanges data, two caught our attention.

The first suspicious IP address, 185.156.74.112, is registered to AS210848, itself known as Telkom Internet ltd. The registries place it in the Seychelles, a country known for hosting many pirate infrastructures. A closer look, however, reveals a structure that is much more post-Soviet than Seychellois. Part of Telkom Internet's infrastructure was previously registered to an AS called TOV VAIZ PARTNER, registered in Azerbaijan in the name of one Khnykin Vitaly Yakovlevich, a digital entrepreneur from the Novosibirsk region. Moreover, the infrastructure used by Telkom is not unknown to cybersecurity researchers: in August 2025, a report by the cybersecurity company Intrinsec[1] showed how the same servers that are now used to broadcast pirated television content in Moldova for interference purposes had been used in brute-force attacks.[2] In short, this is a clear illustration of the new convergence between cybercrime and interference, aimed at circumventing the mechanisms that protect the Moldovan information space.

This connection between cybercriminals and Russian interference operators is not new in itself; it rather confirms trends already observed elsewhere (see above). On the other hand, connections between interference actors, Russian hackers and Chinese and Iranian actors are rarer to observe, because they are usually very well hidden. Such a convergence does, however, appear with a second suspicious

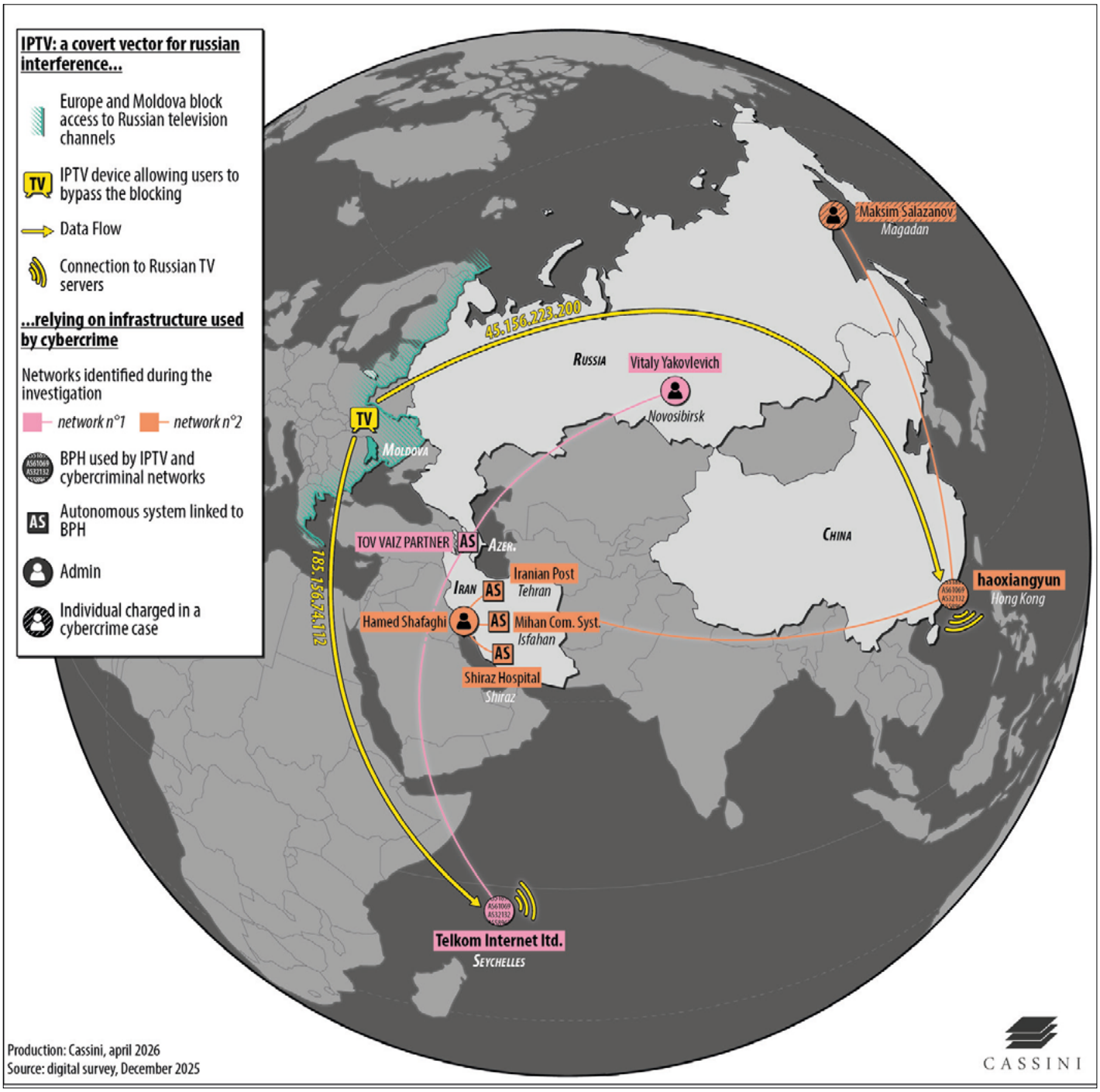
1. D. Sardinha, VAIZ, FDN3, TK-NET: Ukrainian Networks Driving Brute Force Attacks, INTRINSEC, August 2025, https://www.intrinsec.com/vaiz-fdn3-tk-net-ukrainian-networks-driving-brute-force-attacks/
2. A brute-force attack consists in trying, one after the other, every possible combination of a password or key for a given username in order to log in to the targeted service.

IP address with which our pirate Chromecast was trying to communicate: 45.156.223.200. Everything indicates that this is the address used to access the pirated video streams, and therefore the core of the Chromecast's set-up. This IP address is declared as belonging to the autonomous system AS141718, registered under the name *haoxiangyun*. Hosted in an office tower on the outskirts of Hong Kong, this autonomous system is very clearly a BPH. The IP ranges that belong to it are named after their former owners. This is a classic BPH technique: they buy up large numbers of IP ranges declared "legitimate" in order to use them for illicit activities without raising the suspicion of detection systems. In addition, *haoxiangyun* acts as a transit manager for a set of autonomous systems located upstream of it, so that they can reach the large systems that govern the global Internet, located downstream. This is another classic BPH technique for avoiding the suspicion of automated security systems: they operate in "clusters" of interconnected systems, and, as with IP ranges, many of these pirate ASes are former legitimate ASes that have fallen into disuse and been squatted by BPHs.

Among the ASes located upstream of *haoxiangyun*, there are at least two Iranian systems (AS51897 and AS61008) registered to the company Mihan Communication Systems. This company, active from 2016 to 2019, sold connectivity between Iran and several countries of the Near and Middle East. Its administrator, Hamed Shafaghi, had even registered a subsidiary of Mihan in the United Kingdom in 2016.[1] Shafaghi also appears as the administrator of at least two other autonomous systems, one of which belongs to the Post of the Islamic Republic of Iran.

1. See the gov.uk website: https://find-and-update.company-information.service.gov.uk/officers/ldgrf7IZ-_bNwuci_IeFH6nWUQk/appointments

I MAP 2
On the trail of a Russo-Iranian-Chine network: the convergence between Russian interference and cybercrime



These Iranian connections do not allow any definitive conclusion. The most plausible hypothesis remains that of a trade in IP addresses in Iran, which were then bought up by BPHs such as *haoxiangyun*. Given the digital repression currently under way in Iran, former international peering infrastructures may also have been abandoned after the 2021 uprisings, which had led to a tightening of digital censorship in the country. This policy, which resulted in a drastic reduction in the number of crossing points between the Iranian network and the international network (and therefore in the number of ASes and IP addresses connected internationally), also explains the over-representation of Iranian elements in the *haoxiangyun* system.

While the BPH's infrastructure is therefore Chinese, with possible Iranian connections, the administrators who use it to run the clandestine IPTV services are indeed Russian. This is what emerges from an analysis of the domains redirecting to the IP addresses squatted by *haoxiangyun*, listed below:

rostelekom.xyz
maxfolker.rosssteleccom.net
kamil.rosssteleccom.net
ottrast.com
ottclub.xyz
tvclub.xyz
unikhtxl.ottclub.xyz
cbilant.com
kartoshkaka.ru
megogo.xyz
akciatv.ru
ottolok.net
akadatel.com
kazaktelekom.com
melpakomn.ru
russtv.net
megatv.fun
rosssteleccom.net
ucomist.net
otttv.pw
siauliairsavlt.pw
amazzin.pw
edmonst.net
edemist.com
dienalt.org
kazmazpaz.ru
gufengmh8.com

Most of these domains are used extensively to redirect pirated video streams, which is consistent with the purpose of our Chromecast. Among them are several typosquatting domains intended, here again, to avoid raising the suspicions of administrators or moderators tracking illicit content. Thus rosstelecom.net, rostelekom.xyz and kazaktelekom.com typosquat the domains of the national telecom operators of Russia and Kazakhstan. Others, such as russtv.net, tvclub.xyz or megatv.fun, imitate the names of online television channels and look perfectly legitimate. The choices made by the administrators of this galaxy of domains clearly show a marked preference for the Russian-speaking world.

The domains hosted by *haoxiangyun*, some of which are called by the streams of the Moldovan Chromecast, therefore belong to a group of pirates specializing in the piracy of Russian television channels' video streams.

IV. Moldovan BPHs and IPTV: a threat to Europe?

The case of InterDnestrKom (IDK) and Kartina TV

While the use of BPHs reflects the clandestinization of Russian information maneuvers aimed at Moldova, some of the infrastructures studied are also used in campaigns targeting Europe as a whole. This is the case of the BPH Aeza, used both in the Russian Doppelgänger operation – the main information modus operandi of the Social Design Agency – and in the HaiTV campaign in Moldova. Which malicious actors based on Moldovan soil are able to conduct operations in Europe?

The most emblematic case is that of the galaxy of actors and infrastructures revolving around InterDnestrKom (IDK), the national telecom operator of the self-proclaimed republic of Transnistria. Founded in the 1990s, IDK belongs to the large Sheriff conglomerate, which brings together the assets owned by the oligarch Viktor Gushan and accounts for more than 60% of Transnistria's GDP. This operator acts as an Internet access provider but also as a provider of digital services in the self-proclaimed entity. IDK is also involved in several ventures that go far beyond its core commercial activity and fall within the realm of hybrid maneuvers. These ventures range from money laundering through the development of crypto-assets to the hosting of cybercriminal infrastructures, as well as investment in potentially risky cultural industries in Germany, the United Kingdom and Canada.

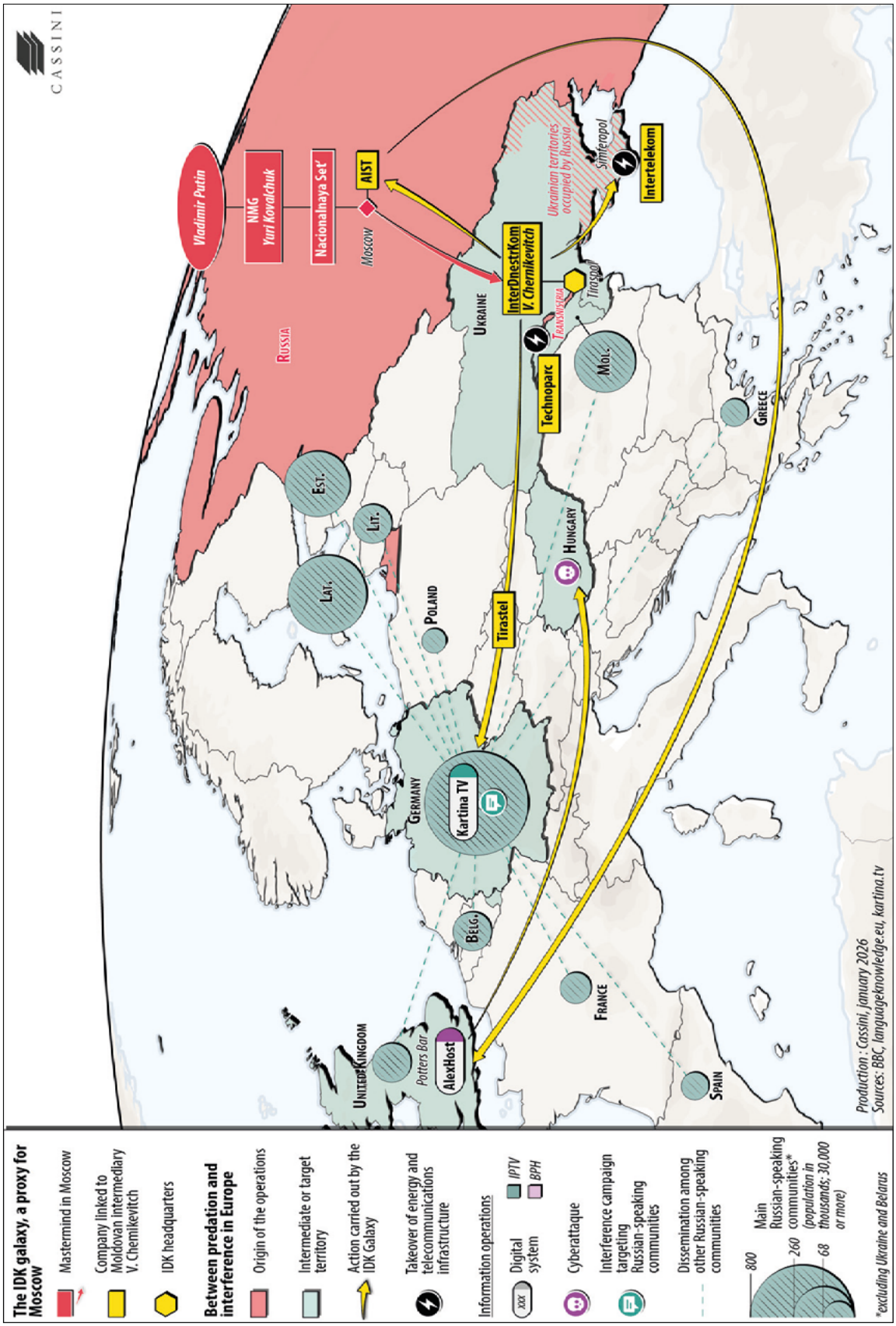
IDK is thus linked to a whole system in which cybercrime, financial crime and interference are intertwined. At the heart of this system is one man, Vyacheslav Chernikevich, who was for a long time IDK's director of business development. Several elements link Chernikevich

to the Russian services: Moldovan investigative journalists have shown the role of intermediary that he played in 2014, at the time of the annexation of Crimea, so that IDK could take over part of the peninsula's cyber infrastructure.[1] At the time, Russia had launched an operation called Miranda to seize and take control of the telecommunications infrastructure of the newly annexed territory. Companies were then created to operate this infrastructure, stolen from Ukrainian operators. Among them was a company called Intertelekom, founded in Simferopol by Chernikevich two months after the invasion of the peninsula.

Chernikevich was therefore involved in an enterprise of appropriation, or even plunder, of cyber resources and infrastructures that previously belonged to Ukrainian companies. This is only one of his many activities: Chernikevich also founded the company Technoparc in Transnistria, which aimed to create a business zone dedicated to cryptocurrency mining, in a region known as a hotspot for laundering through crypto-assets. Before the full-scale invasion of Ukraine, Transnistria was the main transit point for supplying Moldova with electricity and gas from Russia. The self-proclaimed entity then had access to very cheap energy, which it resold at a high price to Chișinău, keeping some of the surplus for crypto-asset mining – a trade from which Chernikevich profited through his company Technoparc.

1. Iurie Sanduta, Прямая связь: ФСБ могла прослушивать всю Украину через фирму приднестровского олигарха [Direct line: the FSB could have wiretapped the whole of Ukraine through a Transnistrian oligarch's company], Rise Moldova, February 17, 2017, https://www.rise.md/ru/statya/%D0%BF%D1%80%D1%8F%D0%BC%D0%B0%D1%8F-%D1%81%D0%B2%D1%8F%D0%B7%D1%8C-%D1%84%D1%81%D0%B1-%D0%BC%D0%BE%D0%B3%D0%BB%D0%B0-%D0%BF%D1%80%D0%BE%D-1%81%D0%BB%D1%83%D1%88%D0%B8%D0%B2%D0%B0%D1%82%D1%8C-%D0%B2/

I MAP 3
Moldova, a hub for Russian clandestine operations into Europe: the case of IDK



At the same time, Chernikevich also set up in Russia the company AIST, specializing in data hosting. Its digital infrastructure has been used in several politically motivated hacking campaigns, including a distributed denial-of-service (DDoS) attack against more than forty Hungarian media websites hostile to Viktor Orbán.[1] In addition, the infrastructure used by AIST (AS48753) is connected upstream to a single autonomous system called AlexHost (AS200019), which behaves like a BPH. AlexHost is registered at a postal address known as "one of the world's dodgiest addresses."[2] According to the BBC, this address is linked to more than 2,000 suspicious activity reports filed by banks around the world with the US Financial Crimes Enforcement Network (FinCEN). It has served as a mailbox for many entities which, while probably unconnected to one another, all share the same concern for discretion: they include companies involved in the Beirut port explosion, while the NGO Transparency International has identified at this address numerous entities with links to suspicious Russian activities.[3]

These various threads thus connect Chernikevich to a galaxy of relatively discreet companies and actors involved in illicit activities in the fields of cybercrime and crypto-assets. Chernikevich is also active in information interference directed at Europe. In addition to the entities already mentioned, in 2015 Chernikevich founded a Russian company called *Natsionalnaya Set'* (National Network), in which he holds a 25% stake. Among the other shareholders is National Media Group (NMG, 25% stake), owned by the oligarch Yuri Kovalchuk, a former neighbor and friend of Vladimir Putin.

According to RBC, *Natsionalnaya Set'* was created as a joint venture between NMG and Transnistrian businessmen in order to launch, in

1. Qurium Media Foundation, "DDoS attacks traced to proxy infrastructure 'White Proxies'," *Qurium*, 2 November 2023. Available at: https://www.qurium.org/weaponizing-proxy-and-vpn-providers/ddos-attacks-traced-to-proxy-infrastructure-white-proxies/
2. "FinCEN Files: One of the world's 'dodgiest addresses' is in leafy Hertfordshire," BBC, September 21, 2020, https://www.bbc.com/news/uk-54204053
3. *Russia in Exile: Ten Years of UK-Russian Trade-Based Money Laundering*, Transparency International, December 18, 2023, https://ti-russia.org/en/wp-content/uploads/sites/2/2024/06/ten-years-of-uk-russian-tbml-2023.pdf

several Western countries (notably Germany, the United Kingdom and Canada), an IPTV service giving access to all Russian-language channels. Specifically aimed at the Russian-speaking populations of these countries, this service is called Kartina TV and still exists today.[1] It takes the form of a box to be connected to a television set, using technologies similar to those of the Chromecast analyzed above. The Kartina TV service was used during the German federal elections to encourage viewers to vote for the AfD, a far-right party known for its partial alignment with Kremlin positions. The maneuver relied on targeted advertisements broadcast on Kartina TV at peak viewing times and on the main Russian channels retransmitted by the service.[2] As Russian-speaking voters are an important pool of votes for the AfD, this advertising campaign is a form of interference that went relatively unnoticed because of its community dimension. To this day, the Kartina service is freely sold in France on several e-commerce platforms, such as those of Leroy Merlin or Cdiscount (Casino Group).

Kartina TV is thus very similar to the systems used in Moldova, but this time on an industrial scale, targeting all the Russian-speaking expatriate populations on the continent. In addition to the ownership structure that links Kartina to Chernikevich and to Transnistria, the cyber infrastructure of this IPTV service has several features suggesting a service that seeks not to attract attention. For instance, one of Kartina's domains, kartina-canada.com, gives in its whois record an administrator to be contacted at the address d.dietrich@tirastel.de. The person who, at the very least, set up Kartina's infrastructure therefore works for a German company called Tirastel. Yet Tirastel operates as the German subsidiary of InterDnestrKom, the Transnistrian national operator, without this link ever being mentioned explicitly. IDK's entry on PeeringDB, a database used by system administrators worldwide to find peering partners, lists the address peering@tirastel.

1. The link between Natsionalnaya Set' and Kartina is established by the fact that Andrei Reich, who holds 25% of Natsionalnaya Set', is also the managing director of Kartina GmbH, a company registered in Germany to operate the Kartina TV service.
2. https://newtimes.ru/articles/detail/119403/

de as its main contact. The fact that these technical details, entered by IT specialists and system administrators, are the only information available to establish a direct link between Tirastel and IDK points to a deliberate effort at concealment: an activity carried out openly would have left far more abundant traces.

This arrangement forms a complex network of companies and infrastructures which, under the guise of giving Russian-speaking populations in Western Europe access to Russian channels, engages in interference and influence operations, notably in connection with elections. In this respect, Chernikevich appears here as an influence entrepreneur, since it is he who makes possible this techno-economic system in which a leading oligarch is involved, and he who played an active role in the illegal annexation of Crimea. Kartina is a vector of destabilization designed to fly "under the radar", that is, outside the social networks and platforms usually monitored by the European counter-disinformation community. Yet, with several million Russian speakers living in Western Europe, Kartina has access to a considerable potential audience. In France, this concerns first and foremost certain municipalities and departments where Russian-speaking communities form significant minorities (notably Alpes-Maritimes, the Paris suburbs and Pyrénées-Atlantiques).

Conclusion

This study of Russian interference in Moldova is based on a mixed approach combining digital investigation and ethnographic fieldwork. The fieldwork in Gagauzia, the interviews with local populations and the OSINT investigations proved particularly fruitful for drawing up a map – at once physical, narrative and cyber – of the vulnerabilities of a territory that is key to the security of the European continent and of France. The study has also shown that the analysis of narratives and of their reception cannot be separated from the geographical conditions in which the populations they target live. By geographical, we mean the socio-economic conditions of these populations as well as the spatial planning of the territory where they live, and the organization of the digital networks that allow narratives to circulate. These different spatial dimensions are so many theaters in which vulnerabilities will be exploited by the adversary and will produce combined effects.

In the case of Gagauzia, the feeling of socio-spatial marginalization is a key driver of adherence to Russian narratives. This attachment holds, however, only as long as these narratives still reach the Gagauz clandestinely despite the blocking of Russian media. Marginalization and clandestinization are therefore intrinsically linked, and they combine to produce destabilizing effects not only in Moldova but also in the rest of the European Union. In this respect, observing the information techniques, tactics and procedures deployed by Russian actors ahead of upcoming elections in Europe, notably in France in 2027, will not be enough to fully understand and counter this phenomenon. This phenomenon feeds on the frustration of part of the targeted populations, who see themselves as peripheral and are inclined to consume, and adhere to, content that reinforces these representations. These endogenous socio-economic vulnerabilities – social inequalities, distrust of institutions, intercommunity tensions, etc. – form, and will continue to form, fertile ground for the actors of Russian interference as long as they are not reduced. Beyond the indispensable

counter-influence policies adopted in Europe in recent years, notably by Moldova and France, the response to hostile foreign interference must therefore go beyond a strictly security-based framing. It must be conceived within a broader perspective of reducing these vulnerabilities and must inform other essential public policies in fields as diverse as education, culture, health and justice.

Étude n°140

Kevin Limonier and Maxime Audinet

The Last Mile of Russian Interference

An Ethnographic and Digital Investigation in Southern Moldova

How do Russian and pro-Russian strategic narratives circulate within an information space that is officially closed to them? And why do certain audiences embrace them?
Drawing on fieldwork conducted in Moldova in the summer of 2025, notably in the autonomous southern region of Gagauzia, this study examines the evolving forms of Russian interference and the conditions under which it is received. Combining ethnographic fieldwork with digital investigation, it traces these narratives all the way to their target audiences and sheds light on the infrastructures that enable their covert circulation.
Moldova emerges as a laboratory for Russian influence strategies. The laundering of media content, the bribing of prospective voters, and clandestine equipment providing access to Russian television channels, linked to cybercriminal networks, all point to a diversified form of influence entrepreneurship aimed at advancing Russia's interests and undermining this former Soviet republic's European anchoring.
The study shows that the circulation of narratives alone cannot account for their reception. In Gagauzia, their success is also rooted in a real or perceived sense of political, social, ethnocultural and territorial marginalisation. Ultimately, this work calls for moving beyond an exclusively security-driven approach in responding to foreign interference.

IRSEM I École militaire
1, place Joffre, case 38
75700 Paris SP 07
irsem.fr

INSTITUT DE RECHERCHE STRATÉGIQUE DE L'ÉCOLE MILITAIRE
irsem

MINISTÈRE DES ARMÉES ET DES ANCIENS COMBATTANTS
Liberté
Égalité
Fraternité