IBI SOVEREIGNTY THREAT BRIEF

SCAM STATE:

How Wartime Ukraine Became a Protected Territory for Cross-Border Fraud

An OSINT investigation into scam call centers, Operation Midas, and the corruption vertical surrounding strategic assets

June 2026

All sources verified · Open data (OSINT)

ibi-institute.org

Table of Contents

Format:	IBI analytical report, designed for a 15–20-page A4 layout
Focus:	threats to the financial and institutional sovereignty of EU member states
Case-boxes:	Ukraine, Moldova, Romania, Israel
EU jurisdictions:	France, Germany, Italy, Ireland, and other states

PAGES 2–3 | SECTIONS 1–3

1. Introduction

Between 2023 and 2026, wartime Ukraine became not only a theatre of military operations and Western mobilizational support, but also one of the most visible hubs of industrial-scale telephone and investment fraud targeting citizens of European Union member states. Evidence gathered from Eurojust press releases, OCCRP investigations, materials published by the Global Initiative against Transnational Organized Crime (GI-TOC), and corroborating media reports points to a stable, reproducible model: call centers staffed by hundreds of operators, systematic targeting of elderly and Russian-speaking victims, infrastructure that persisted through multiple police operations, and a protective environment rooted in the intersection of organized crime and political-administrative influence.

At the same time, Ukrainian anti-corruption bodies and international observers documented the largest corruption scandal surrounding President Volodymyr Zelensky's inner circle: Operation Midas, which implicated senior officials and figures linked to Energoatom in a scheme assessed at approximately USD 100 million. The Kozyn / "Dynasty" case added a material dimension: the laundering of UAH 460 million through elite residential construction in a Kyiv suburb. These parallel cases do not prove a chain of command from the state to scam call centers, but they do define a common political-economic environment in which large criminal-financial structures operated with sustained impunity.

2. Key Findings

- Ukraine functioned as a major regional hub of scam call centers targeting citizens in Europe and beyond, and the international operations of 2025–2026 indicate recurring infrastructure rather than isolated episodes.
- GI-TOC characterizes the Ukrainian model as a highly networked criminal ecosystem linked to organized crime, corruption-based protection, and the development of crime-as-a-service practices [3].
- In December 2025, Eurojust reported the dismantling of a network of call centers in Dnipro, Ivano-Frankivsk, and Kyiv that targeted victims across Europe; the damage exceeded EUR 10 million and more than 400 victims were documented [4].
- In May 2026, NABU and SAPO reported the laundering of more than UAH 460 million through elite construction in Kozyn, with part of the funds linked to schemes surrounding Energoatom and the Midas investigation [11][12].
- From the standpoint of EU sovereignty, the key threat lies in the fact that the territory of an allied and subsidized state was effectively used for the systematic extraction of funds from citizens of donor countries.

3. Methodology and Limits of Attribution

This report is based on open sources, including Eurojust press releases, NABU and SAPO materials, GI-TOC research publications, and corroborating media reports that summarize anti-corruption and

cross-border criminal investigations. All factual claims are referenced to verifiable primary or secondary sources; no classified or confidential materials are used.

The existence of scam call centers on Ukrainian territory, their targeting of European victims, corruption schemes surrounding Energoatom, and the laundering of proceeds through the Kozyn project are each documented independently. The report does not claim to prove a formal chain of command between the Ukrainian state and scam call centers, nor does it assert that political corruption and financial fraud are institutionally integrated. The report does assert that these phenomena coexisted in a common political-economic environment, and that this coexistence has consequences for the European Union's approach to conditionality.

Box 1. Central Argument

The central problem is not the proven existence of direct command-and-control by Ukrainian intelligence services over scam call centers, but the existence of a durable model of state tolerance under which cross-border fraud persisted within a warring, over-the-top centralized state [3][9].

Box 2. Limit of Attribution

The operative formula of this report is as follows: not a proven centralized special operation, but a systemically tolerated criminal environment, capable of intersecting with the interests of individual security, political, and criminal actors [9][3].

PAGES 3–5 | SECTIONS 4–5

4. Ukraine as an Operational Hub of Cross-Border Fraud

GI-TOC materials on Eurasia identify Ukraine directly as one of the most consequential regional cases within the scam-center ecosystem, where a “highly networked illicit industry” emerged on the basis of organized crime, corruption-based protection, and crime-as-a-service infrastructure [3]. The geography of confirmed operations spans Ukraine’s major cities, and the typology of schemes recurs consistently across multiple investigations.

In December 2025, Eurojust reported the dismantling of a network operating out of Dnipro, Ivano-Frankivsk, and Kyiv, describing systematic fraud against victims across Europe. In February 2026, OCCRP reported a subsequent Eurojust-backed operation in Dnipro targeting fraudulent crypto investments. In May 2026, a call center in Kharkiv was shut down following a Eurojust-supported investigation [10].

Infographic 1. Geography of Confirmed Operations

Period	Locations in Ukraine	Schemes	Scale / Scope
Nov 2023	Dnipropetrovsk + Czechia	Voice phishing / investment	Tens of millions € (Czechia)
Dec 2025	Dnipro, Ivano-Frankivsk, Kyiv	Fake police / bank / “safe account”	EUR 10M+, 400+ victims
Feb 2026	Dnipro	Fraudulent crypto investments	Victims across Europe, 11 suspects
May 2026	Kharkiv	Telephone fraud	Hundreds of thousands €, 4 leaders

5. The Architecture of Ukrainian Scam Call Centers

The underlying operational model recurs from case to case: a false legend, psychological pressure, transfers to controlled accounts, remote access to victims’ devices, and the use of drops and dead drops for proceeds. Eurojust materials consistently describe organized divisions of labor, with operators, supervisors, technical staff, and financial coordinators functioning within a single enterprise [4][2].

It is precisely this standardization that justifies speaking of an industry rather than a collection of ad hoc groups. The recurrence of the same architecture across different cities, the presence of formal management structures, and the scale of recruitment all reflect a business model, not improvised criminality [3].

Box 3. The Standard Fraud Pipeline

Standardized chain: call — pressure — transfer — repeated contact. The organizational logic is similar to legal call centers: scripts, KPIs, recruiting, team management.

Infographic 2. Operational Chain

Stage	Action	Instruments	Victim Vulnerability
Initial capture	Call from a “bank,” “police,” or “broker”	Spoofing, CRM systems, phone databases [4]	Anxiety, trust in institutions
Escalation	Urgency pressure	Scripts, psychological manipulation [3]	Fear of financial loss
Extraction	Transfer to controlled account / crypto wallet	Online banking, remote access tools [4][2]	Lack of time and control
Secondary harvest	“Fund recovery,” additional deposits	Renewed contact, drop networks [3]	Shame and desire to recover losses

PAGES 5–6 | SECTIONS 6–7

6. From Financial Fraud to Instruments of Coercion

Open-source evidence from the Russian direction suggests that the call-center model can extend beyond purely financial extraction. Mediazona documented at least 187 arson attacks against enlistment offices across Russia in 2024, with a significant share attributed to individuals recruited via telephone by operators whose style and methods are consistent with post-Soviet vishing operations [9]. Although the direct chain linking these incidents to Ukrainian call centers has not been formally established, the functional overlap is analytically significant.

Even if these incidents do not prove formal state command, they do demonstrate the functional suitability of such infrastructure for coercion, destabilization, and grey-zone operations [18]. For a European audience, the significance is different: infrastructure built for financial fraud can be repurposed for pressure operations targeting individuals across national boundaries.

7. The Corruption Vertical: Operation Midas

The anti-corruption investigation known as Operation Midas does not directly concern scam call centers, but it illustrates the political-economic environment in which large corruption schemes were able to persist and scale. NABU announced the investigation in November 2025, describing a high-level criminal organization that had extracted rent from Energoatom through “shadow managers” who exercised control over decisions without formal authority [12].

The Washington Post reported that investigators assessed the scheme at approximately USD 100 million and described a 15-month investigation involving a substantial body of audio recordings. Additional reporting in The Guardian and Brookings Institution analysis placed the investigation in a broader context of wartime rent extraction at strategic state assets [6][7][16].

Box 4. Why Midas Matters for the Fraud Question

Midas demonstrates that the issue is not confined to street-level criminality, but concerns the quality of political protection: strategic assets, wartime emergency conditions, and anti-corruption rhetoric coexisted with large-scale rent extraction [7][6].

Infographic 3. The Midas Vertical

Node	Function in the Scheme	Relevance to the Report
Energoatom	Strategic state asset, source of contract-based rent [12]	Depth of institutional penetration
“Shadow managers”	Control over decisions without formal authority [6][7]	Example of state capture
“Laundromat”	Legalization and redistribution of funds [11][8]	Bridge to elite real estate

Political circle	Protective environment and capacity to pressure investigations [7][16]	Indicator of institutional vulnerability

PAGES 6–7 | SECTIONS 8–9

8. Kozyn / “Dynasty”: The Materialization of Corruption Rents

On 11 May 2026, NABU and SAPO announced suspicions against seven members of an organized group in a case involving the laundering of more than UAH 460 million through the construction of an elite complex in Kozyn, a prestigious suburb of Kyiv. The court ordered the arrest of the real estate project, freezing assets whose total value has been assessed at several hundred million hryvnias [11][8].

Crucially, NABU stated explicitly that the project was partly financed with funds derived from corruption schemes at Energoatom. This ties elite real estate not to incidental abuse, but to the systematic rent extraction that the Midas investigation documented at the institutional level [12][31].

9. The Threat to the Sovereignty of EU States

For EU states, the threat has at least three aspects. The first is financial: European citizens become direct victims of fraud schemes organized from Ukrainian territory. According to Deutsche Welle, total losses across Europe from Ukrainian and broader Eurasian scam infrastructure have been estimated at upward of USD 57 billion per year [1][22]. The second aspect is legal: the cross-border character of the schemes creates jurisdictional complexity that burdens joint investigation teams, Eurojust mechanisms, and national law-enforcement agencies. The third aspect is political: the coexistence of EU assistance to Ukraine and systematic fraud against EU citizens creates a structural credibility problem for the political logic of unconditional solidarity.

France, Germany, Italy, Ireland, and other states are therefore not abstract “partners,” but spaces of final harm. Even when specific Eurojust releases do not enumerate all jurisdictions of the victims, the pattern of targeting is consistent with a pan-European exposure that the EBA and ECB data confirm at the regulatory level [23][4].

Infographic 4. Matrix of Threats to EU Sovereignty

Aspect	Manifestation	Consequence
Financial	Direct household losses, elderly and vulnerable groups [4][2]	Declining trust in the financial system
Legal	Cross-border jurisdictional complexity [4][14]	Greater burden on JITs and Eurojust
Political	Gap between reform rhetoric and criminal practice [3][6]	Erosion of support for Ukraine within the EU
Security	Potential shift from fraud to coercion [9][3]	Expansion of grey-zone pressure

PAGES 7–8 | SECTION 10

10. The Moldova Case

In this configuration, Moldova should be understood not merely as a vulnerable neighbor of Ukraine, but as a potential buffer through which the Ukrainian, and more broadly post-Soviet, criminal ecosystem extends into the European Union's immediate neighborhood. The country's regulatory and law-enforcement capacity remains limited relative to EU standards, while its proximity to Ukraine and Romania creates conditions for the formation of mixed-nationality criminal networks [5].

In June 2025, Eurojust reported the dismantling of an organized criminal group operating from professionally organized call centers in Moldova and targeting victims across the EU; the network consisted of Moldovan, Romanian, Ukrainian, and Italian suspects [5]. A further case, reported in Moldovan sources after Operation Crypto Wave, showed the use of Moldova as a platform for cyber fraud and money laundering targeting companies and citizens in Romania, the United Kingdom, and other EU states.

The sovereignty risk for the EU is therefore twofold. On the one hand, Moldova is an object of European integration and political stabilization; on the other, its weaker regulatory and law-enforcement environment creates a structural vulnerability that criminal actors are actively exploiting.

Box 5. Moldova as a Buffer Risk

Moldova is no longer merely an analytically plausible transit zone; in Eurojust materials it appears as a confirmed site of professionally organized call-center and laundering schemes involving Moldovan, Romanian, Ukrainian, and Italian suspects [5].

Infographic 5. The Moldovan Risk Scenario

Scenario Element	What the Case Demonstrates	Relevance for the EU
Professional call centers	OCG targeted victims across the EU [5]	Moldova already embedded in transnational circuit
Mixed network	Moldovan, Romanian, Ukrainian, Italian suspects [5]	Threats are networked, not nationally isolated
Crypto Wave	Victims in Romania, UK, and other EU states [17]	Moldova suitable as multi-country fraud platform
Political context	Country moving toward EU yet institutionally fragile [3]	Anti-scam work becomes part of EU enlargement agenda

PAGES 8–9 | SECTIONS 11–12

11. The Romania Case

Romania is not merely another neighboring state; it is an external frontier of the European Union through which logistical, financial, and human flows connected to the Ukrainian crisis pass. For that reason, the threat from cross-border scam operations is qualitatively different for Romania: it is both a victim country and a potential institutional gateway.

The June Eurojust operation against a network operating through call centers in Moldova demonstrated the Romanian dimension directly: Romanian nationals were among the suspects, while victims were spread across multiple EU jurisdictions [5]. This dual role — suspects and victims simultaneously occupying Romanian space — makes Romania analytically distinct from states where the exposure is purely on the victim side.

This allows us to consider Romania in two roles: the country of direct damage (the victims are its own citizens) and the EU's institutional gateway (legalizing movement, documents, and infrastructure access for actors from Ukraine). If the Ukrainian criminal and financial environment retains political protection, the transmission pathway into the EU runs, among other routes, through Romania.

Infographic 6. The Romanian Threat Contour

Contour	Manifestation	Consequence
Citizens	Romanian victims of telephone and financial fraud [17]	Direct household losses, declining trust
Banking system	Use of Romanian financial space within regional networks [5]	Greater pressure on AML and cross-border investigations
Legal infrastructure	Participation of Romanian suspects in mixed networks [5]	Blurring of boundary between internal and external threat
EU sovereignty	Romania as gateway into European law and mobility	Transmission of Ukrainian risk into the Union itself

12. The Israel Case

Israel demonstrates how the post-Soviet and Russian-speaking vishing model scales beyond the European space proper. Israeli sources documented a wave of what was termed the "Russian scam," directed above all at elderly Russian-speaking citizens, including immigrants and Holocaust survivors; the National Council for the Crime Victim was reported to have received thousands of complaints [19][20].

Although official Israeli materials do not always specify the country of origin of the operators, GI-TOC identifies Ukraine as one of the key nodes of the Russian-speaking scam-center ecosystem in Eurasia. The Israeli case is therefore analytically important as an example of model exportability: language and social geography determine targeting, not national boundaries [21][44].

PAGES 9–10 | SECTIONS 13–14

13. The Profile of Organizers and Protectors

The available materials make it possible to distinguish at least three layers of actors. The first layer consists of criminal entrepreneurs who manage sites, recruitment, scripts, payment channels, and the withdrawal of proceeds. The second layer consists of corrupt intermediaries and protectors who insulate operations from law enforcement, facilitate money movement, and provide legal and logistical infrastructure. The third layer — the most inferential — concerns the political environment that creates and maintains the conditions for systemic impunity [3][6].

From the standpoint of evidence, the first and second layers are the most firmly established. The third layer is reconstructed through the Midas case, the Kozyn case, and the political consequences of those investigations, including the involvement of high-ranking officials and figures close to the presidential administration [11][8][27].

Infographic 7. Pyramid of Actors

Level	Who Is Included	Role
1. Implementers	Operators, recruiters, technical staff	Victim contact and primary extraction [4]
2. Organizers	Network owners, proceeds coordinators	Scaling and business sustainability [3][2]
3. Protectors	Corrupt officials, local security-linked intermediaries	Protection from dismantling [3]
4. Political environment	Circles surrounding strategic assets and senior offices	Reproduction of impunity [6][11]

14. Political Consequences for the European Union

For a prolonged period, European policy toward Ukraine was shaped by a moral-political presumption of exceptionalism: external aggression was treated as though it required the temporary suspension of hard questions concerning internal corruption and criminal ecosystems. Yet, the materials of Eurojust, NABU, and independent investigative organizations make clear that this suspension had material costs for European citizens [3][4][6].

If an allied state is simultaneously a recipient of large-scale assistance and a platform for systematic fraud against citizens of donor countries, the issue ceases to be merely criminal and becomes one of sovereignty. For France, Germany, Italy, Ireland, and other states, the question concerns not only law enforcement cooperation but the credibility of the political framework within which that cooperation is supposed to take place.

15. Recommendations for European Institutions

1. Conditionality of assistance

Budgetary and sectoral support to Ukraine should be more tightly linked to the dismantling of call centers, public reporting on liquidated networks, and verifiable outcomes in strategic corruption cases [12][4].

2. Focus on organizers

Joint investigation teams should focus not only on operators, but also on organizers, intermediaries, and protectors who ensure the resilience of the schemes [3][4].

3. Protection of vulnerable groups

The EU should expand anti-fraud prevention programs for the elderly, migrants, and Russian-speaking communities, since these groups display heightened vulnerability in comparable cases [19][4].

4. Sovereignty audit

A dedicated European mechanism is needed to monitor threats to financial sovereignty emanating from partner states, including Ukraine [4][3].

5. Institutional resolution

Support for Ukrainian anti-corruption bodies should be shielded from political fluctuation and accompanied by external auditing in cases involving strategic assets [6][12].

16. Conclusion

The cumulative weight of the open-source record permits a cautious but firm conclusion: Ukraine in the period of full-scale war became not only a theatre of resistance to external aggression, but also a protected environment for large-scale cross-border criminal-financial activity. Scam call centers targeting European citizens, systemic corruption surrounding strategic assets, and the laundering of proceeds through elite real estate are not coincidental features of an exceptional emergency; they are structurally related symptoms of an institutional environment in which political protection, criminal enterprise, and wartime exceptionalism have coexisted and reinforced one another.

For Europe, this implies the need to move beyond strategic sentimentalism and toward a language of sovereignty, conditionality, and enforced transparency. Otherwise, the alliance with a wartime state risks becoming a regime of political blindness toward a system that simultaneously requests trust, resources, and integration while tolerating the systematic extraction of wealth from the citizens of its partners.

PAGES 13–15 | SECTION 17

17. Additional Evidence: France, Germany, Italy, Ireland and the Broader EU Context

A wider European picture reinforces the central argument of this report: Ukrainian and wider Eurasian scam infrastructures are dangerous not only because they operate transnationally, but because they land in national environments already experiencing very substantial fraud exposure. In this sense, each of the major EU economies represents both a target environment and a sovereign interest directly at stake.

France

France illustrates the scale at which fraud has already become a systemic national problem. BioCatch's France-focused reporting states that French citizens lost an estimated EUR 4.5 billion to fraud in 2023, while a later 2025 survey-based estimate placed scam losses over the previous 12 months at EUR 2.5 billion. Banking fraud in France is dominated by account takeover and social-engineering schemes — exactly the typologies documented in Ukrainian call-center operations.

For the logic of this report, France is important not only in volume, but also in modality: spoofing schemes with imitation of banking and law enforcement institutions — exactly those that Eurojust recorded in Ukrainian call center cases — dominate the country's digital banking fraud [24][4].

Germany

Germany represents an equally important case of mass vulnerability. According to GASA estimates for 2025, the annual damage from fraud in Germany reached 10.6 billion euros; 54% of adults had experienced at least one fraud attempt, and 19% reported a direct financial loss. At the same time, 84% of fraud went unreported — indicating that official statistics substantially underestimate actual exposure [45].

German losses are not reduced to abstract cybercrime metrics, but directly fall on the social engineering model. Germany should be considered both as an end market for victims and as a jurisdiction whose payment infrastructure is under constant pressure from transnational criminal systems [23][1].

Italy

The Italian picture is more fragmented, but no less significant. In Verafin's European report for 2025, cumulative fraud losses in Italy were estimated at $3.7 billion, including $2.9 billion in bank fraud and hundreds of millions more in advance-fee scam, cyber-enabled scam, impersonation fraud, and investment fraud. These categories map directly onto the typologies that Eurojust documented in Ukrainian and Moldovan-Romanian call center networks [24].

Ireland

Ireland is particularly important as an illustration of under-reporting, retail vulnerability, and the growing role of investment fraud. According to a study by the Central Bank of Ireland (April 2026), more than one in three adults in Ireland experienced fraud, almost two thirds of victims lost money, and the median loss was EUR 300. At the same time, 62% of victims did not report the incident — indicating that aggregate figures substantially understate actual harm.

In the logic of this report, Ireland is almost a textbook example of how fraud damage can be politically underestimated, when many individual losses are moderate in size, the level of disclosure is low, and only certain categories like investment fraud generate large public figures [1][23].

The Wider EU Context

At the European level, the broader institutional picture confirms that payment fraud and scam activity are not marginal phenomena. The EBA's Consumer Trends Report for 2024/25 identified payment fraud as the most significant issue affecting EU consumers, emphasizing the growth of social-engineering schemes and the need for enhanced consumer-protection frameworks. The ECB/EBA joint report on payment fraud (December 2025) assessed total fraud in the EEA at EUR 4.2 billion in 2024 — up 20% year-on-year (from EUR 3.5 billion) — separately noting that in the credit transfers subcategory alone, growth was 17% [23].

This pan-European institutional evidence is important because it shows that the vulnerability being exploited by Ukrainian and wider Eurasian scam infrastructures is not anomalous but structural. Over the past year, Europeans in all the surveyed countries have lost an estimated 57 billion US dollars to scam and fraud — a figure that dwarfs the budgets of most national law-enforcement agencies dedicated to the problem [22][1][23].

Box 6. Why National Evidence Matters

The significance of France, Germany, Italy, Ireland, and other EU states is not merely that they contain victims, but that their national fraud burdens create a receptive environment in which additional cross-border scam pressure translates into political distrust, regulatory overload, and widening sovereignty costs [22][1][23].

PAGES 15–18 | SECTION 18: REFERENCES

18. References

All sources have been verified as of June 2026. Primary sources from official Eurojust, NABU/SAPO, ECB, and EBA resources take precedence over secondary media.

I. Eurojust — Official Press Releases

[4] Eurojust. Fraudulent call centers in Ukraine rolled up. 15 December 2025.
https://www.eurojust.europa.eu/news/fraudulent-call-centres-ukraine-rolled

[10] Eurojust. Scam call center shut down (Kharkiv). 28 May 2026.
https://www.eurojust.europa.eu/news/scam-call-centre-shut-down-thanks-eurojust-supported-investigation

[5] Eurojust. Eurojust assists in operation in Romania and Moldova. 12 June 2025.
https://www.eurojust.europa.eu/news/eurojust-assists-operation-romania-and-moldova-against-laundering-phishing-fraud-proceeds

[28] Eurojust. Fraud — summary page of operations 2025–2026.
https://www.eurojust.europa.eu/term/fraud

II. NABU / SAPO — Official Materials

[12] NABU. Operation Midas: high-level criminal organization in energy sector exposed. 10 November 2025.
https://nabu.gov.ua/en/news/operatciia-midas-vykryto-vysokorivnevu-zlochynnu-organizatciiu-shcho-diiala-u-sferi-energetyky/

[11] Euromaidanpress. Ukraine's anti-corruption agencies uncover major laundering scheme. 11 May 2026.
https://euromaidanpress.com/2026/05/12/ukraines-anti-corruption-agencies-uncover-major-laundering-scheme/

[8] Hromadske. Former presidential chief-of-staff Andriy Yermak charged. 10 May 2026.
https://hromadske.ua/en/amp/politics/263844-nabu-oholosylo-yermaku-pidozru

[15] Pravda.com.ua. Operation Midas: five detained. 10 November 2025.
https://www.pravda.com.ua/eng/news/2025/11/11/8006815/index.amp

[31] Interfax Ukraine. Corruption scheme to embezzle Energoatom funds. 1 June 2026.
https://en.interfax.com.ua/news/general/1172953.html

III. OCCRP

[2] OCCRP. Eurojust-Backed Operation Takes Down Ukrainian Scam Call Center. 22 February 2026.
https://www.occrp.org/en/news/eurojust-backed-operation-dismantles-european-scam-call-center-network

[22] OCCRP. A $57 Billion Toll: How Evolving Scams Are Fleecing Europe. 8 June 2026.
https://www.occrp.org/en/news/a-57-billion-toll-how-evolving-scams-are-fleecing-europe

IV. GI-TOC

[3] Global Initiative against TOC. Scam centers: Combating a global phenomenon. 27 May 2026.
https://globalinitiative.net/analysis/scam-centres-combating-a-global-phenomenon/

[33] University of Glasgow / GI-TOC. War in Ukraine is transforming criminal landscape. 17 July 2025.
https://www.gla.ac.uk/news/archiveofnews/2025/july/headline_1197071_en.html

V. Mediazona

[9] Mediazona. In Russia, phone scammers talk people into arson. 16 January 2025.
https://en.zona.media/article/2025/01/16/scam_arsons

VI. International Media — Midas and the Yermak Affair

[6] Washington Post. Ukraine announces energy corruption probe. 11 November 2025.
https://www.washingtonpost.com/world/2025/11/11/ukraine-corruption-investigation-energoatom/

[7] The Guardian. Ukraine's energy sector corruption crisis. 19 November 2025.
https://www.theguardian.com/world/2025/nov/19/ukraine-energy-sector-corruption-crisis

[16] Brookings Institution. War, peace, and corruption in embattled Ukraine. 7 December 2025.
https://www.brookings.edu/articles/war-peace-and-corruption-in-embattled-ukraine/

[27] Al Jazeera. Zelensky's ex-chief of staff appears in court. 13 May 2026.
https://www.aljazeera.com/news/2026/5/13/zelenskyys-ex-chief-of-staff-appears-in-court-in-money-laundering-case

VII. Ukrainian Law Enforcement Agencies

[17] Attorney General's Office cracking down on fraudulent call centers.
https://gp.gov.ua/en/posts/ofis-generalnogo-prokurora-znishhuje-rinok-saxraiskix-call-centriv-a-ne-okremi-ofisi

[41] Attorney General's Office. Over 45 thousand EU citizens defrauded.
https://gp.gov.ua/en/posts/v-ukrayini-vikrito-miznarodnii-saxraiskii-call-centr-yakii-osukav-ponad-45-tisyaci-gromadyan-jevropi

[13] UNN. In Dnipro, fraudsters profited from deceiving EU citizens with crypto. 22 February 2026.
https://unn.ua/en/news/in-dnipro-fraudsters-profited-from-deceiving-eu-citizens-with-crypto-through-call-centers

VIII. Moldova and Romania

[18] Radio Moldova. Moldovan and Romanian call centers linked to financial fraud. 17 February 2026.
https://radiomoldova.md/p/70046/moldovan-and-romanian-call-centers-linked-to-financial-fraud-organizers-detained-in-a-eurojust-l

[18b] Moldova1. Percheziții la call-centre din R. Moldova și România. 19 February 2026.
https://moldova1.md/p/69071

IX. Czech Republic / Ukraine, November 2023

[14] Europawire / Europol. Czech and Ukrainian Police Disrupt Prolific Phishing Gang. 17 November 2023.
https://news.europawire.eu/czech-and-ukrainian-police-disrupt-prolific-phishing-gang-defrauding-victims-across-europe

X. Israel

[19] The Jerusalem Post. Knesset committee discusses scam vs elderly Russian-speakers. 15 May 2025.
https://www.jpost.com/israel-news/crime-in-israel/article-854212

[20] Time Ukraine-Israel. "Russian scam" continues to hit Israel. 16 October 2024.
https://timeukraineisrael.com/en/news/society/russian-scam-continues-to-hit-israel-thousands-of-victims-among-returnees/

[21] LinkedIn / Alex Gaft. Israel plans to combat telephone fraud targeting elderly. 19 April 2025.
https://www.linkedin.com/pulse/may-2025-the-global-initiative-against-tran-vbalf

[42] Ynet News. Police arrest 3 suspects for hacking elderly Israeli accounts. 25 December 2022.
https://www.ynetnews.com/article/bjfmqywko

[44] The Jerusalem Post. Communications Minister promotes regulation protecting elderly. 31 March 2024.
https://www.jpost.com/israel-news/article-794638

XI. EBA / ECB / EU Regulators

[23] ECB / EBA. Joint report on payment fraud: strong authentication effective. 15 December 2025.
https://www.ecb.europa.eu/press/pr/date/2025/html/ecb.pr251215~e133d9d683.en.html

XII. GASA / Anti-Fraud Organizations and Media

[1] Deutsche Welle. Rising cyberscam losses expose gaps in EU response. 9 June 2026.
https://amp.dw.com/en/rising-cyberscam-losses-expose-gaps-in-eu-response/a-77487321

[24] Fintech Global / Nasdaq Verafin. How Europe is battling a $103.6bn fraud menace. 31 March 2025. https://fintech.global/2025/03/31/how-europe-is-battling-a-103-6bn-fraud-menace/

[45] Global Anti-Scam Alliance. Policy Agenda 2026. 4 March 2026. https://gasa.org/knowledge-base/blog/gasa-policy-agenda-2026