NSSG®
an AVANTE company

GHOST DOMAIN · INTELLIGENCE BRIEFS ON THE .SU ECOSYSTEM

SERIES 2 OF 3 — GERMANY IP BRIEF

The German File

Two decades of Soviet-coded web addresses, quietly hosted in Germany — and the fraud, impersonation and recruitment infrastructure hiding inside them.

Bucharest Headquarter:
Grigore Alexandrescu Street, 26, 010626
+40 21 795 7601
servicedesk@nssg.global

1. WHY GERMANY

Brief 1 in this series mapped the .su ecosystem at global scale. This brief takes one country apart.

Our first report mapped the .su namespace worldwide: **over 109,000 active domains registered to a country that stopped existing in 1991 and was never formally decommissioned online**. Its central finding was structural, not anecdotal. .su creates what we called infrastructure distance — a Russian-administered registry, typically a Russian-language registrar, and a server sitting anywhere else in the world. No single national authority holds the full picture. No single regulator can act alone.

That report also **flagged two Western European jurisdictions where infrastructure distance concentrates most heavily: the Netherlands and Germany**. This brief takes Germany on its own terms.

Of the roughly 109,000 domains in the global dataset**, close to 2,000 currently resolve to a German IP address** — the second-largest Western European concentration in the census, and by far the oldest. Drawing on the available dataset (snapshot dated 12 July 2026), we selected a **working sample of these domains for individual investigation — WHOIS, DNS, TLS certificates, and, where the page still loads, live content — historical where it doesn't, and report what we found, and what we could not resolve**.

A note on method

We grouped these domains by where their servers currently sit, not by who registered them. **Hosting location cannot tell you a registrant's nationality or whereabouts**. What it tells you is **which infrastructure an operator chose — and that choice is rarely accidental**. Bad actors gravitate toward hosts that ask few questions and act slowly on abuse reports: cheap, permissive, and hard to shut down quickly. So when dozens of near-identical sites cluster on the same server, the same nameservers, the same jurisdiction, that is rarely a coincidence of geography. It is a shared playbook — the same kit, the same reseller, the same blind spots. Hosting clusters do not, by themselves, reveal who is behind a scam. **They reveal where the shadows fall, and which corners of the internet's infrastructure keep attracting the same kind of trouble**.

Germany is one of those corners

Germany's own security services describe a threat environment that is, in their words, persistently high and worsening, with Russian state-linked activity as a primary and recurring concern. In 2025, German police logged 321 suspected sabotage cases nationwide targeting critical infrastructure — rail, energy and military sites — the majority of which German intelligence attributes to Russian actors or their proxies. **In May 2025, a joint advisory co-signed by Germany's BSI, BfV and BND, alongside the United States' CISA, NSA and FBI and the UK's NCSC, formally attributed a two-year cyber-espionage campaign to GRU Unit 26165** — better known as APT28 or Fancy Bear — targeting Western logistics, transport and technology

Bucharest Headquarter:
Grigore Alexandrescu Street, 26, 010626
+40 21 795 7601
servicedesk@nssg.global

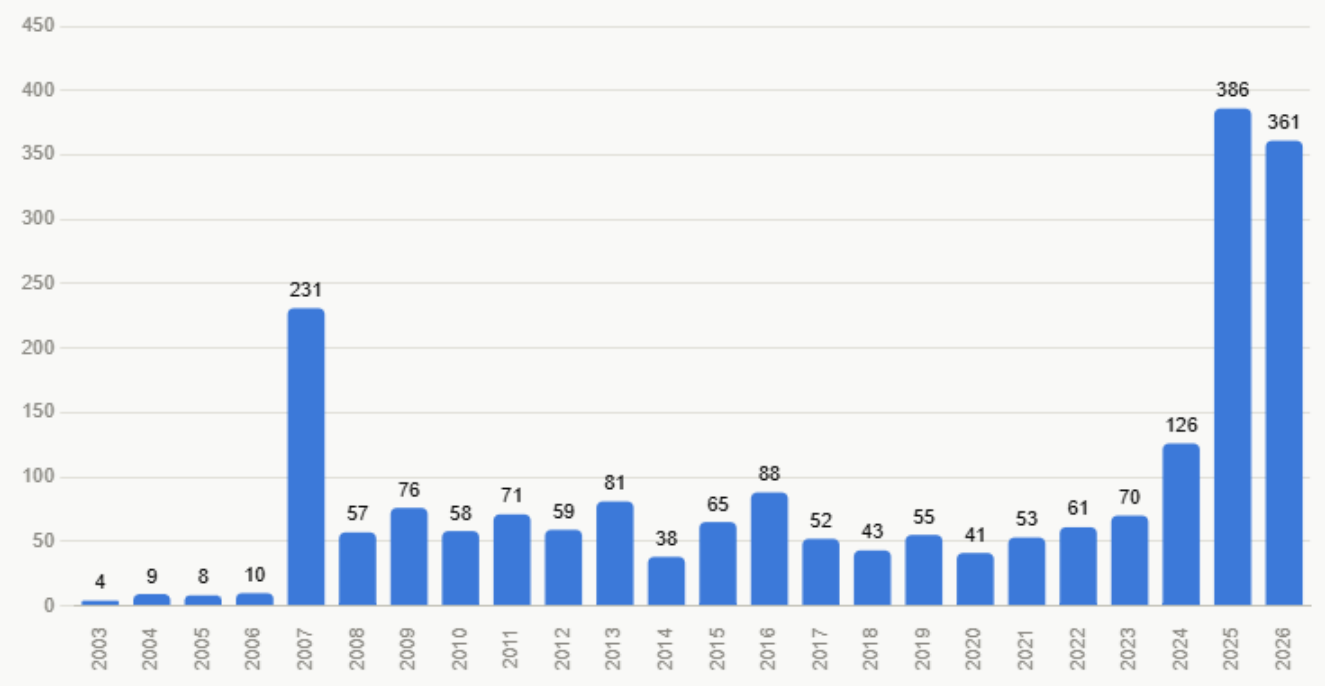
firms supporting Ukraine, with ports, airports and maritime infrastructure named explicitly among the sectors affected.

We draw no direct line between any single domain in this dataset and a named intelligence service. We simply note that **Germany already sits inside an active, publicly acknowledged, Russian-linked threat picture** — precisely the kind of environment in which quiet, jurisdictionally ambiguous infrastructure tends to be most useful, and most easily overlooked.

2. THE REGISTRATION CURVE

This is not a pre-deadline rush. It is a mature, twenty-year infrastructure base that recently began accelerating sharply.

Other slices of the .su namespace, as later briefs in this series will show, carry registration curves dominated by a single spike in the run-up to a known deadline. Germany's curve tells a different story: **activity beginning in the early 2000s, a first major event in 2007**, then two steady decades before a **sharp acceleration in the last eighteen months**.



The 2007 spike, examined in full in Section 4, was a **single domain speculator moving in on a one-day price cut**. The 2010s held to a steady, unremarkable rhythm — 40 to 88 new German-hosted .su registrations a year, consistent with defensive brand registrations, hobbyist purchases and small-scale investing. Then the pattern breaks: 126 in 2024, 386 in 2025, and 361 in the first half of 2026 alone — a run rate that, if it holds, will make 2026 the busiest year for German-hosted .su registration in the zone's history.

Bucharest Headquarter:
Grigore Alexandrescu Street, 26, 010626
+40 21 795 7601
servicedesk@nssg.global

*The surge looks less like one cause than a **convergence of several** — but the clearest signal is what's actually landing on these domains: **the job-abroad scams, visa impersonation, crypto lures and carding hub documented in this brief were all registered in this exact window (January 2025 through mid-2026)**, which points to word-of-mouth adoption inside Russian-language scam-kit circles once a few operators demonstrated the pattern works. A second, plausible driver is the hosting choice itself: keeping the registrar Russian (cheap, low-KYC) while moving hosting to Germany — e.g. via Hetzner — lets operators sidestep the default suspicion and geo-blocking that Western corporate firewalls and threat-intel feeds increasingly apply to Russian-origin IP space, **making German infrastructure a deliberate laundering layer rather than a coincidence of geography**. And the timing likely isn't isolated to .su at all: 2025 saw phishing domains rise 38% globally, with 77% maliciously registered and over a third acquired through bulk-registration services, so .su may simply be catching the same wave hitting other lightly-scrutinized TLDs, attractive precisely because major blocklists and reputation systems are tuned around mainstream gTLDs rather than an obscure Soviet-era ccTLD. Layered underneath both is the anticipation effect of Russia's incoming ESIA identity-verification mandate (effective 1 September 2026) and the announced 2030 phase-out of .su itself — both of which give operators, legitimate and illegitimate alike, a reason to register now, while the namespace is still cheap, lightly monitored, and effectively anonymous.*

3. KEY FINDINGS AT A GLANCE

The numbers behind Germany's .su footprint, and why each one matters.

~2,000	69%	25	10%
.su domains resolving to a German IP	carry a measurable crawl-relevance score	use Cyrillic / internationalised encoding	expire before the 1 Sept 2026 ID-check deadline

Each figure earns its place in this brief. The 69% crawl-relevance rate is the most consequential: it means **more than two in three of these domains are not sitting inert**. They are indexed, discoverable, and actively serving content to visitors — this is a live population, not a museum of abandoned registrations.

The 25 Cyrillic or internationalised (IDN) domains confirm that Germany's .su footprint, though hosted in Western Europe, is still **overwhelmingly built for a Russian-speaking or Cyrillic-reading audience** — a

Bucharest Headquarter:
Grigore Alexandrescu Street, 26, 010626
+40 21 795 7601
servicedesk@nssg.global

detail that matters for takedown and content-moderation cooperation, since German hosts and registrars will rarely be equipped to read what they are hosting.

The fourth figure is the one with a clock attached. Under Russian Federal Law No. 569-FZ, from 1 September 2026 every operation on a .ru, .рф or .su domain — registration, renewal, transfer, even a DNS change — will require the registrant to verify their identity through ESIA, Russia's national Gosuslugi identification platform. Domains that cannot complete verification will not renew. Our dataset shows **221 of Germany's roughly 2,000 .su domains — about one in ten — carrying an expiration date before that deadline even arrives**, meaning their holders face a compliance decision within weeks of this brief's publication, whether they are a legitimate Western brand running a defensive registration or an operator running the infrastructure described in the sections that follow.

Zoom out further and the deadline carries a second layer. In February 2026, ICANN's technical operator quietly notified the .su registry of a planned phase-out of the zone by 2030. Combined with the September 2026 identity-verification mandate, the .su namespace is now on a visible, dated countdown — which raises the operative question for the rest of this brief: is that countdown pushing legitimate holders out, or simply filtering out the operators unwilling to put a verifiable identity behind what they are running?

4. THE 2007 LAND GRAB

The largest single-day registration event in the entire .su namespace happened at midnight on 3 December 2007 — and it was priced, not political.

On 2 December 2007, one registrant — almost certainly a single domain speculator, or a small syndicate operating in close coordination — registered 196 short, dictionary-word .su domains in a single automated burst. It remains the largest one-day registration event ever recorded in the .su zone.

Why that date, to the minute

The **.su registry cut its registration price from roughly 3,000 rubles (about $125) to 600 rubles (about $25) effective 3 December 2007**, in a deliberate move to **drive adoption and stave off the zone's elimination by ICANN**. It worked: registrations rose 45% in the following quarter alone. Our registration timestamps — almost all logged at 21:00 UTC on 2 December — line up to the minute with that change: Russia sat at UTC+3 that winter, so 21:00 UTC was exactly midnight in Moscow, the instant the new price took effect. This has the signature of an automated script, poised and ready to fire the moment the gate opened.

Bucharest Headquarter:
Grigore Alexandrescu Street, 26, 010626
+40 21 795 7601
servicedesk@nssg.global

What the names reveal

- **Pure short-word inventory:** the bulk of the list — any.su, fair.su, pure.su, wild.su, zed.su, and dozens of non-dictionary but pronounceable strings like bap, khz, oaf, sri — is classic premium short-domain harvesting. Brevity, not meaning, is the asset.
- **An off-road and 4x4 accessories cluster:** interco.su, intercotire.su, procomp.su, superswamper.su, hi-lift.su, tire.su, tyre.su and land-cruiser.su cluster tightly around real, trademarked off-road brands (Interco's Super Swamper tyre line, Pro Comp, Hi-Lift Jack) and Toyota's Land Cruiser — a popular platform in the Russian and CIS 4x4 market. Several of these are live third-party trademarks, placing this sub-cluster on the edge of cybersquatting rather than neutral word-farming.
- **A travel-booking pair and Russian cultural references:** aviaticket.su and aviatickets.su point to a flight-booking or affiliate play; tusoffka.su transliterates Russian slang for a social hangout, and akbars.su echoes a well-known Tatarstan financial and sporting brand.

Taken together, this was never 196 independent buyers who happened to like short words. It is the fingerprint of one operator — or a tightly coordinated few — running an automated registration pass at the exact second the price dropped, and combining pure speculative inventory with at least one identifiable commercial niche. Whether these domains are still active investments or long-since-abandoned relics, their presence in today's German-hosted footprint shows how far back some of this infrastructure's roots actually go — twenty years, in some cases, from a single midnight transaction to a dataset a security team is reading in 2026.

5. THE ALPHABET ON THE SERVER

Twenty-seven domains, one IP address, one recruitment funnel — and a naming pattern built to borrow trust from a name nobody registered.

The most operationally revealing cluster in this brief **follows a single naming convention: [redacted1].su, then [redacted1]-a.su through [redacted1]-z.su, skipping only [redacted1]-j.su**. All 27 were registered progressively between **January and August 2025**, all through the same Russian registrar (REGRU-SU), and all resolve to the identical IPv4 address — 136.243.14.123 — on Hetzner Online infrastructure in Germany, served through link-host.net, a Russian-language hosting reseller operating since 2009. Every domain shares the same nameservers, the same SOA record, and an unusual SPF configuration in which the server's own IP address appears duplicated — a fingerprint distinctive enough to say with confidence that all 27 sit under one operator's control.

Bucharest Headquarter:
Grigore Alexandrescu Street, 26, 010626
+40 21 795 7601
servicedesk@nssg.global

Not a parked portfolio — a working mail system

This is the detail that separates the cluster from ordinary domain squatting. Every domain in the series carries its own individual MX record — mail.[redacted1]-a.su, mail.[redacted1]-b.su, and so on through the alphabet — meaning each is independently configured to receive email. **None carries a DMARC record**, **so none enforces sender authentication on outbound mail**. MX proves the capacity to receive; permissive SPF allows the server to send mail that most recipients will still accept; the absence of DMARC means no recipient has a reliable way to verify whether a message claiming to come from any of these 27 addresses is genuine. Put simply: **this is a single-operator, mail-enabled infrastructure set, built for two-way correspondence with real people — not a dormant brand-defense portfolio**.

What visitors actually see

The domains — including the [redacted1]-j.su variant, which is absent from the raw dataset crawl but confirmed live at time of writing — present a **Russian-language recruitment pitch along the lines of** "Do you want to work in the European Union and earn from $4,000 a month?", with only slight variation from one to the next. **Each shows a single clickable element, linking through to a Telegram or WhatsApp contact**.

Historical captures from earlier in 2025 show near-identical copy pointing to a different Telegram handle entirely — **the front-end template has stayed fixed while the human contact layer underneath it has already been rotated at least once**, a hallmark of operational security in scam and trafficking-adjacent recruitment networks, not of a legitimate employment agency.

The domain's WHOIS record ties its registrant email to Russian-language platform activity — the Yandex ecosystem, the Tilda website builder, and the Whoxy domain-lookup service — alongside a Swedish mobile number. A currently valid Let's Encrypt TLS certificate, issued 5 June 2026 and expiring 3 September 2026, confirms the site is actively maintained, not abandoned.

The twenty-sixth domain: harvesting identity, not just trust

One further domain sits inside the same letter sequence but resolves outside Germany, and it does something the rest of the cluster does not: **rather than a job pitch, it presents a page styled as "[redacted]", requesting a face photograph, scanned identity documents and proof of residence,**

Bucharest Headquarter:
Grigore Alexandrescu Street, 26, 010626
+40 21 795 7601
servicedesk@nssg.global

wrapped in GDPR-consent language to look like routine account onboarding. This is not a recruitment funnel. It is **an identity and biometric harvesting mechanism** — the raw material criminal networks buy and sell to bypass real Know-Your-Customer checks and open verified "mule" bank or exchange accounts, sometimes paired with tools that spoof "liveness" checks using someone else's face or a deepfake.

Whether this domain and the recruitment cluster are one pipeline or two is genuinely unclear. The shared naming sequence and infrastructure make a common origin — the same kit, or the same registration batch — highly likely. What it does not prove is a single operator running both as one business. Two readings stay on the table: **a single coordinated pipeline, in which the job-abroad pitch grooms a compliant target who is then walked toward the "banking verification" page as a plausible next step in onboarding**, harvesting identity documents under that pretext; or **shared infrastructure serving separate customers**, where a kit or hosting reseller supplied both operations independently and the naming overlap is closer to reused inventory than coordinated design. The domain's position inside the exact same letter sequence, rather than on unrelated infrastructure, makes the first reading the stronger one — though confirming it would require visibility into the actual message exchange a target receives, which is outside what open-source review can establish.

The impersonation widens: visa services and crypto "education"

Two further domains — [redacted2].su and info-[redacted2].su — sit on the exact same infrastructure fingerprint: identical IP address, nameservers, SOA record and SPF pattern as the redacted domain cluster above. [redacted2] is a real, established visa-processing service operating at [redacted2].com; the co-located lookalike domains connect the same operator's infrastructure to visa-service impersonation as well as recruitment fraud. At the time of review, info-[redacted2].su displayed a third, entirely different pitch: a **Russian-language "Crypto Edu" page promising up to 20% annual returns from crypto staking**, funnelling every visitor to a single Telegram contact under the name [redacted] — free-education framing, an unverifiable yield, and a private-chat handoff, the standard shape of an advance-fee investment scam.

One IP address. One operator. Three storefronts — a job abroad, a visa service, a crypto course — each a different lure pointed at a different anxiety, all running on infrastructure built to send and receive mail nobody can verify.

This is not a themed scam site, but a shared infrastructure serving multiple, simultaneous fraud verticals — which is precisely the operating model that makes this class of network resilient. If one storefront is reported and blocked, the underlying mail-enabled infrastructure, and the rest of the naming series, keeps running underneath it.

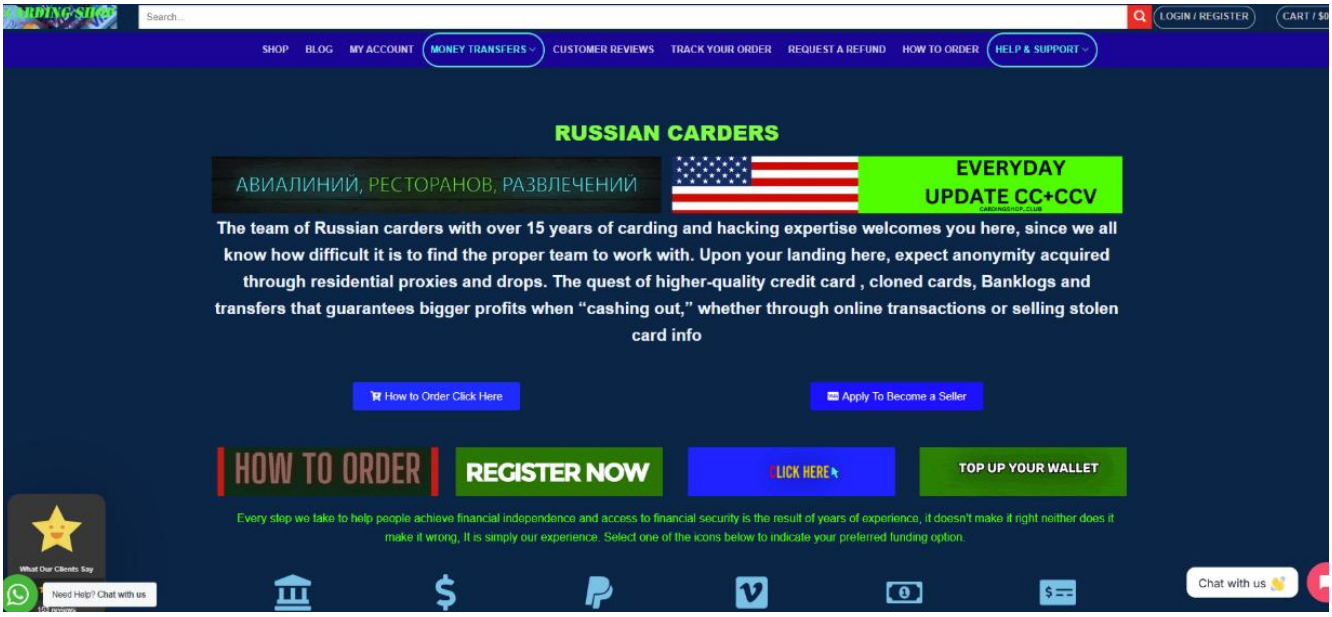
Bucharest Headquarter:
Grigore Alexandrescu Street, 26, 010626
+40 21 795 7601
servicedesk@nssg.global

6. THREE WEBSITES, THREE PLAYBOOKS

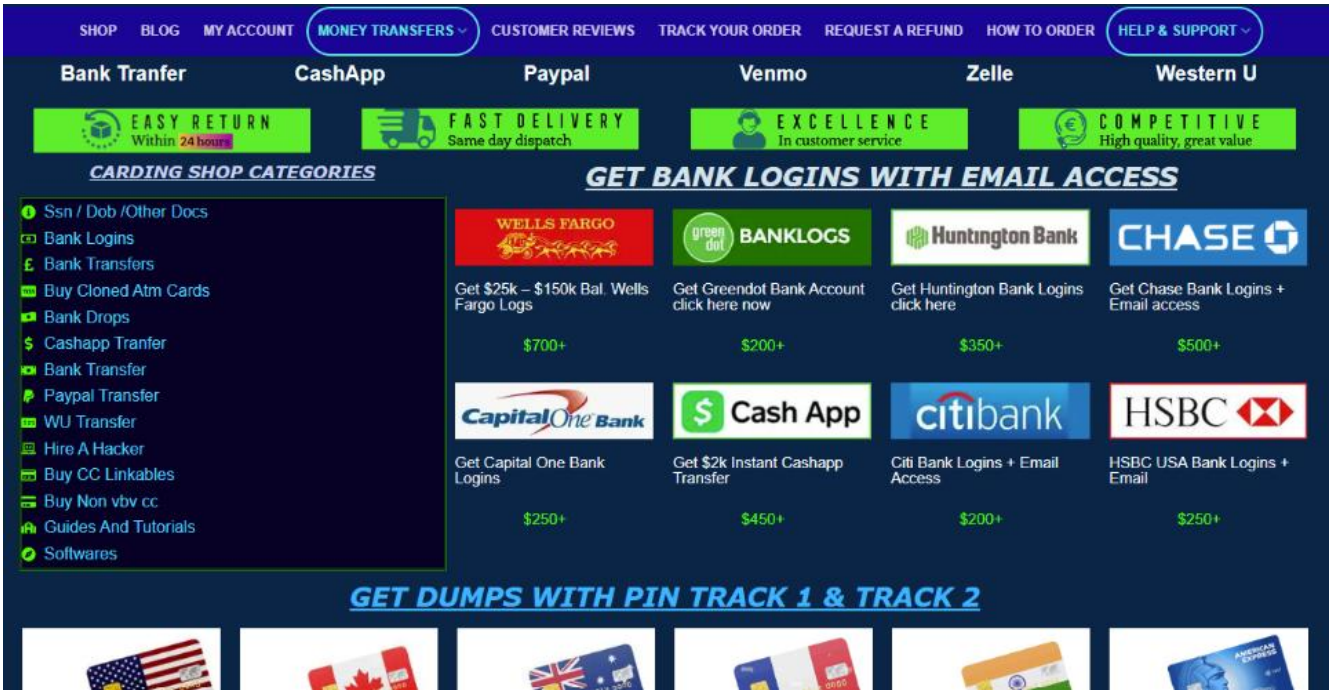
Not every notable domain in this footprint fits the recruitment-and-impersonation model. Three further cases show just how wide the .su namespace's abuse surface really is.

[redacted3].su — a dark-web marketplace, hosted on the clearnet

Registered in **May 2026, [redacted3].su operates as a hub-and-spoke directory linking to affiliated "shops" (on .ru, .to, .co, .net domains) — offering close to the full catalogue of financial cybercrime: stolen card dumps and CVVs, compromised bank logins for named US institutions, cash-out services across CashApp, PayPal and Western Union, EMV skimmer software, OTP-bypass bots, stolen identity documents, and a "dark-web marketplace script" for sale**, suggesting the **operator's real product may be the shop template itself**.



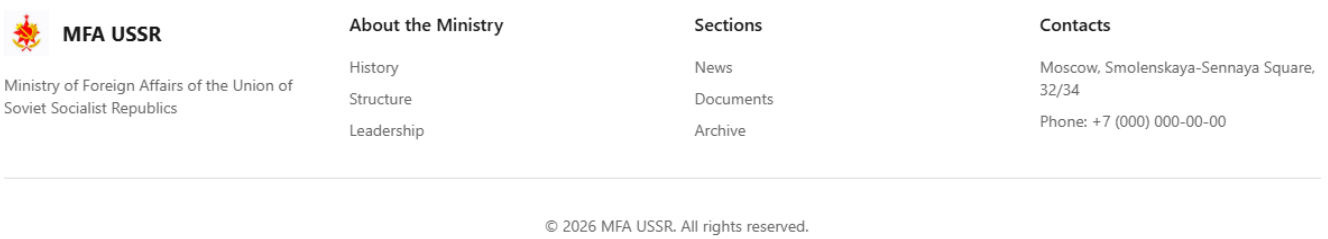
Bucharest Headquarter:
Grigore Alexandrescu Street, 26, 010626
+40 21 795 7601
servicedesk@nssg.global



This content has historically lived almost exclusively on Tor hidden services; what we are seeing is a well-documented industry shift toward clearnet storefronts on cheap, loosely regulated TLDs, chosen precisely because they are indexable, shareable, and faster to stand up and abandon than any hidden service. "Russian carders, 15 years of experience" branding and genuine Cyrillic copy tap a real underground reputation; a passage invoking North Korean state hacking reads as borrowed headline drama rather than a genuine claim. Identical marketing text and template-grade fake reviews across the linked shops point toward a low-effort, kit-based operation — quite possibly a "ripper" site built to defraud its own criminal customers on top of whatever real data it also moves.

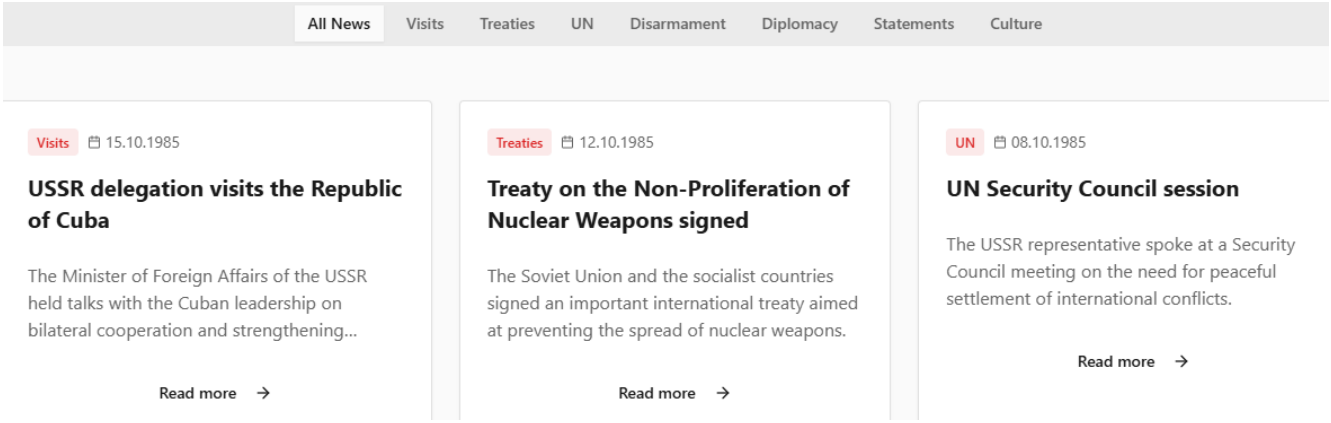
ussr-mid.su — a pseudo-state with an AI-generated front door

Presenting itself as "**the official information portal of the Ministry of Foreign Affairs of the USSR**", this domain slots into a real and long-documented movement in Russia and the post-Soviet space**: groups asserting that the USSR never legally dissolved, publishing shadow ministries and pseudo-legal decrees**, and in some well-documented cases selling fake "USSR citizenship" to followers as a claimed escape from Russian taxes or legal obligations. What makes this entry distinctive is its build: **page metadata traces to Lovable (formerly GPT Engineer), a modern AI-assisted app builder — a freshly assembled, JavaScript-rendered site, not an old hand-built archive**.



Bucharest Headquarter:
Grigore Alexandrescu Street, 26, 010626
+40 21 795 7601
servicedesk@nssg.global

It offers content in five languages, including English, French, German and Italian, and — in one detail we could not explain — its "**latest news**" section is dated to 1985.



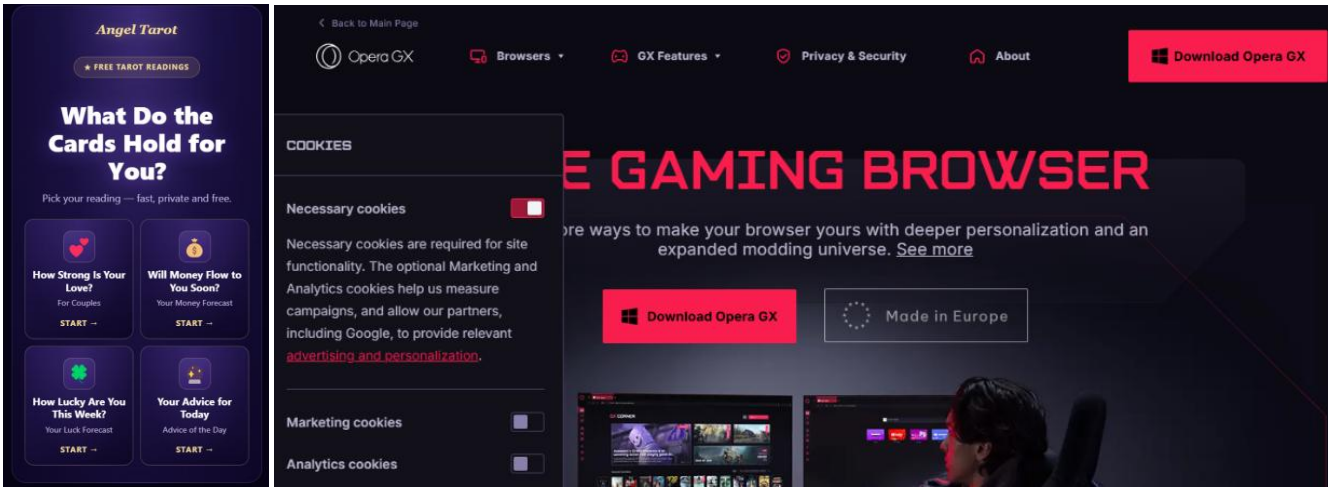
Broken pipeline or deliberate Cold War theatre, it illustrates how easily AI tooling now lets one operator stand up a multilingual, institution-shaped shell in an afternoon.

dailystormer.su — an extremist name, recycled for ad revenue

This domain carries the name of a notorious, repeatedly deplatformed neo-Nazi commentary site — and the .su zone's own history confirms that .su, alongside .ru, did briefly host the genuine Daily Stormer after it was removed from mainstream hosting elsewhere, before Russia's internet regulator forced its removal from both TLDs. Its history shows 85,864 captures, a substantial footprint confirming that earlier life as a real, active mirror rather than an opportunistic name-squat.

What the domain does today is different. Rather than resolving to any fixed page, it **routes visitors through a rotating ad-arbitrage chain: the same URL sends different visitors to different destinations depending on location, device, and which advertiser currently has budget in the broker's pool**. In our review, the domain resolved on separate visits to a quiz-funnel lead-generation page (tarot reading) and to an affiliate promotion for a gaming browser, the latter carrying UTM tracking parameters that identify it as **paid-affiliate traffic run through an ad network rather than organic browsing**. This is the signature of a **domain plugged directly into a traffic-monetization broker**: every visit functions closer to a real-time auction than a static redirect, with the domain owner earning per-click or per-lead revenue regardless of which advertiser wins any given request.

Bucharest Headquarter:
Grigore Alexandrescu Street, 26, 010626
+40 21 795 7601
servicedesk@nssg.global



The domain's current WHOIS record is consistent with this: registered through DOMAINSHOP-SU (2022-03-10), with nameservers pointed at ns1/ns2.parkingcrew.net — ParkingCrew being a domain-parking and ad-monetisation service, not a hosting provider for original content. Nothing in the current redirect chain suggests any ideological content remains; the infamous name appears to be functioning purely as a traffic magnet, monetising residual curiosity and search volume rather than serving any of the site's original purpose.

Worth flagging: a redirect chain of this kind is also a common vector for malvertising — the advertiser rotation that serves a quiz funnel one visit and a browser promo the next could just as easily serve something more harmful on a different visit, from a different network or device. Its **current behavior should be treated as untrusted traffic infrastructure rather than assessed as a single, static page**.

7. WHAT THIS MEANS, AND WHAT COMES NEXT

Country-by-IP slices of the .su namespace do not behave uniformly — which is exactly why each one has to be investigated on its own terms.

What looks, in one country's footprint, like a harmless collection of defensive brand registrations can look, in another, like an active fraud cluster running on shared, mail-enabled infrastructure. Germany's footprint contains both: a genuinely old, mature base of legitimate and speculative registrations stretching back two decades, sitting alongside a newer, faster-growing layer of recruitment scams, impersonation infrastructure, a dark-web marketplace hosted in plain sight, and at least one AI-built pseudo-state shell. The only responsible way to tell which is which is the discipline we applied here: rank the domains, date them, match the names, verify through WHOIS and DNS, and report honestly on what the evidence does, and does not, support.

The September 2026 ESIA identity-verification deadline turns that discipline into a live decision point. Every Western brand holder, law firm, or security team currently managing a defensive .su registration

Bucharest Headquarter:
Grigore Alexandrescu Street, 26, 010626
+40 21 795 7601
servicedesk@nssg.global

through German infrastructure now faces a genuine choice: complete Russian state identity verification to keep the domain, or let it lapse into the redemption pool — where, as this brief's earlier sections show, it can be picked up in hours by the next opportunist, speculator, or scam operator waiting for exactly that kind of opening.

This Report Is Part of a Series

This is Report 2 of 3 in Ghost Domain, our ongoing intelligence series on the .su ecosystem. Brief 1 established the global picture; this brief examined Germany in depth.

A third and final brief will follow, turning the same disciplined process — rank, date, name-match, verify, report — on another country's .su footprint.

If you would like the underlying dataset, a tailored .su exposure review for your organisation, or to discuss a digital monitoring, brand-protection or threat-assessment engagement covering Germany or any other jurisdiction, please contact us directly.