NSSG®
an AVANTE company

GHOST DOMAIN:

Threat Intelligence Brief PART 1:

The Soviet Union's Internet Never Died

How a Relic of the Cold War Became One of the Most Dangerous Corners of the Modern Internet - and Why a New Russian Law Is About to Change Things Again.

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

The .su top-level domain - assigned to the Soviet Union in September 1990, fourteen months before it ceased to exist - **should not still be running in 2026. It is.** With over **109,000 active domains across 80 countries,** it functions today as a ghost state in cyberspace: jurisdictionally ambiguous, lightly regulated, weaponised by cybercriminals, appropriated by political extremists.

A critical regulatory change effective September 1, 2026 is about to alter who can operate there - and that change has already drawn the first interest from brands protecting their intellectual property portfolios.

This brief is the first in a series of three intelligence reports examining the .su domain - its governance, ownership structure, and ecosystem. Two subsequent country-specific analyses will explore how the characteristics of individual jurisdictions, together with Russia's geopolitical influence, shape the scope, content, and risk profile of .su domains.

109,269	Active .su domains as of June 3, 2026
80	Countries represented in the .su registrant base
77%	Share of .su domains registered from Russia
Sept. 2026	Deadline - Russian Federal Law 569-FZ mandatory identity verification for all .su administrators
2030	ICANN[1] projected retirement date for the .su TLD - still five years away

1. A DOMAIN THAT SHOULD NOT EXIST

The .su top-level domain is the internet's most improbable survivor. Assigned to a state that no longer exists, it has outlasted the Cold War, survived international pressure for its deletion, and quietly become one of the most dangerous - and least monitored - corners of the global internet.

On September 19, 1990, a group of Soviet scientists at the Kurchatov Institute of Atomic Energy in Moscow registered .su as the country code top-level domain for the Union of Soviet Socialist Republics.

The first website launched on the domain was the Mathematics division of the Russian Academy of Sciences. The network, called Relcom, was built by Valery Bardin and colleagues at the Kurchatov Institute; its first international connection was established with a computer at the University of Helsinki in August 1990 - just fourteen months before the Soviet flag was lowered over the Kremlin for the last time.

The USSR dissolved in December 1991. Its domain did not. While the country codes of other collapsed states were quietly retired - .dd for East Germany was never fully implemented, .cs for Czechoslovakia was deleted in 1995, .yu for Yugoslavia finally removed in 2010 - .su persisted.

[1] Internet Corporation for Assigned Names and Numbers

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

2. WHY IS IT STILL ON?

The technical and legal explanations are straightforward. The strategic and political context, however, adds important dimensions to the picture.

Formally, the .su domain continues to exist because no single international authority has the power to unilaterally shut it down. While ICANN, the organization responsible for coordinating the global Domain Name System, can remove .su from the root zone, it cannot compel Russia to cease operating the domain's nameservers or supporting infrastructure.

Over the years, ICANN has repeatedly raised concerns regarding .su. At the same time, the Moscow-based Foundation for Internet Development (FRI), one of the entities responsible for managing the domain, has **publicly acknowledged shortcomings in its regulatory framework and limitations in its ability to remove malicious or criminal content**.

"We realise it's a threat for our image" - Sergei Ovcharenko, Director for .su development, Foundation for Internet Development, May 2013.

In February 2025, ICANN's operational arm reportedly informed the .su administrator of plans to retire the domain by 2030 under a ccTLD retirement policy adopted in 2022, nearly three decades after .su lost its ISO 3166-1 country code designation. The issue is particularly sensitive given the current geopolitical environment, where **actions affecting Russian-administered internet infrastructure may be perceived as politically motivated**. The case is also being closely watched because it **may establish a precedent for other legacy country-code domains, including .io**, whose future has come under scrutiny following the planned transfer of the British Indian Ocean Territory to Mauritius.

From a technical perspective, .su remains fully operational because the infrastructure supporting it continues to function. Since 2009, the domain has been maintained by Technical Center of Internet LLC (TCI), a subsidiary of Rostelecom, Russia's state-owned telecommunications operator. **TCI also operates the .ru and .рф registries, making it a key component of Russia's national internet infrastructure** and ensuring the continued availability of .su despite ongoing discussions about its eventual retirement.

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

The more interesting question is: who benefits from .su remaining active? The answer involves at least four distinct interest groups.

- **Russia's state actors benefit from the jurisdictional ambiguity.** A domain administered under the ghost flag of the Soviet Union sits in a legal grey zone that complicates enforcement by Western governments, ICANN, and law enforcement agencies. When a criminal site operates from .su, the question of which state has regulatory authority is genuinely unclear - and Russia has historically shown little urgency in resolving that ambiguity.
- **Cybercriminals benefit from lax enforcement.** When Russian authorities tightened oversight of .ru domains around 2011-2012, scammers and hackers migrated en masse to .su. The domain's population doubled in 2011 and again in 2012. Group-IB's Andrei Komarov estimated in 2013 that more than half of cybercriminals in Russia and the former Soviet Union used the .su space. Botnet command-and-control infrastructure, ransomware distribution, credential theft operations, and phishing networks have all made extensive use of .su domains.
- **Ideological actors benefit from its symbolic weight.** The hammer-and-sickle resonance of .su carries meaning for Russian ultranationalists, Eurasianist movements, and pro-Soviet political networks. As this brief documents below, Alexander Dugin's Fourth Political Theory network - one of the intellectual foundations of Russian expansionist ideology - operates its international website on 4pt.su. Igor Girkin (Strelkov), the former FSB officer and Russian commander in the 2014 Donbas conflict, launched his personal website on igorstrelkov.su. The domain is not chosen at random.
- **Registrar businesses benefit commercially.** The .su domain generates registration fees. RuCenter, Reg.ru and the broader Runiti Group collectively manage hundreds of thousands of domain registrations. The new legislation being introduced in September 2026 is, among other things, a revenue opportunity: it allows these registrars to offer "trusted administrator" services to non-resident domain holders who cannot otherwise comply with the new identity verification requirements.

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

3. THE SEPTEMBER 2026 CHANGE - AND WHY IT MATTERS NOW

A new Russian law is about to bring the .su domain into a state-controlled identity verification system. The consequences - for cybercriminals, for legitimate users, and for international brands - will be significant.

Effective September 1, 2026, Federal Law No. 569-FZ from December 2025 requires mandatory identification of all administrators of .ru, .рф, and .su domains through Gosuslugi - Russia's centralised national identity portal, formally known as the Unified Identification and Authentication System (ESIA). Every domain administrator must have a verified account.

The practical challenge is immediate: approximately 80,000 non-resident clients currently registered with Reg.ru alone hold .su (and .ru) domains that **they cannot verify without a Russian ESIA account, which typically requires a physical local presence in Russia to create**. A "trusted administrator" service was launched, under which verified entities hold formal administrative responsibility for a domain on behalf of a non-resident, while actual DNS management and renewal rights remain with the non-resident through their personal account. This structure satisfies the legal requirement while preserving non-resident access.

"The first to show interest in our service were large international companies providing intellectual property and digital asset protection services to global brands. RuCenter has long been a partner of these companies in managing the Russian segments of their domain portfolios." - Ekaterina Bobrova, COO, RuCenter, June 2026

The implications of this quote deserve attention. **Major international brands - in fashion, technology, consumer goods, and elsewhere - already maintain .su domain registrations as a defensive measure: registering their own brand names in the .su space prevents impersonators from doing so first**. The new law creates a compliance burden for these defensive registrations that registrars are already moving to solve commercially.

For the threat landscape, the September 2026 deadline creates a predictable pattern: some illegitimate domain holders will exit the .su space ahead of the identity verification requirement, others will route around it using the trustee services or by registering under Russian shell identities. The overall effect is likely to be a modest contraction in the total domain count accompanied by a paradoxical increase in Russian state visibility into who holds what - which is itself a reason why some sophisticated actors will choose to leave.

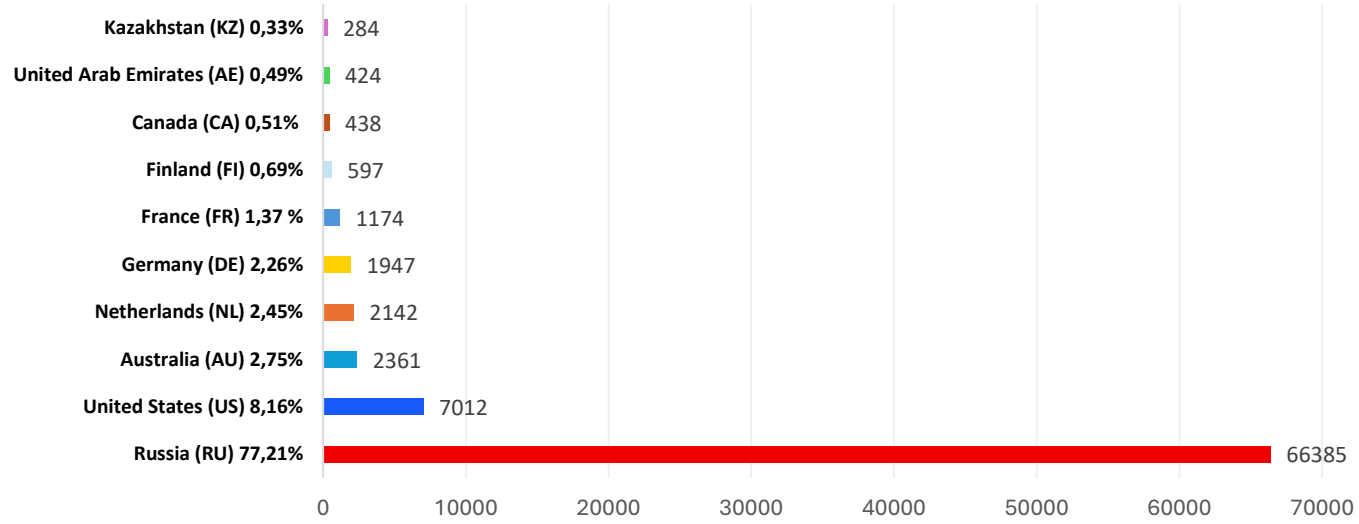
As of early June 2026, administrators of 256,000 domain names on RuCenter and 456,000 on Reg.ru had already authenticated through ESIA - suggesting that compliance is proceeding ahead of the deadline, and that the ecosystem is adjusting rather than collapsing.

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

4. WHO REGISTERS THEM - AND WHY

The .su registrant base spans 80 countries but is overwhelmingly Russia-dominated. The non-Russian slice, however, is where the most analytically interesting users are found.

The following table shows the current distribution of .su domain registrations by top 10 countries, based on current webatla.com snapshot as of June 2026:



The Russia-dominance of the registrant base is expected and reflects the domain's primary audience. The non-Russian holders fall into broadly three categories: diaspora users and cultural organisations with historical ties to the Soviet space; cybercriminals and fraudsters using non-Russian registrations to add a layer of geographic distance to their operations; and legitimate international businesses registering defensively to protect brand names.

The Netherlands (2,142 domains) and Germany (1,947) warrant specific attention as European jurisdictions: both are well-established locations for VPN providers, bulletproof hosting proxies, and shell company registrations that are used as intermediary layers for criminal .su operations. The Australian figure (2,361) is partly explained by an entirely different phenomenon: UK and Australian universities and student unions frequently use .su as an abbreviation for Students' Union, an entirely legitimate but context-confused use of the TLD.

The Cloudflare anomaly of late 2025 provides a striking illustration of how .su is weaponised at infrastructure level: **when Cloudflare launched a DNS Magnitude ranking system measuring how many unique clients queried each TLD, .su briefly ranked higher than .com in global DNS traffic**. Investigation revealed that a **botnet - the Aisuru/Kimwolf botnet, which at its peak generated DDoS attacks approaching 30 terabits per second - was using .su domains as command-and-control infrastructure**, generating **massive artificial DNS query volumes**. Cloudflare subsequently redacted the specific botnet domains from its data, but the episode demonstrated that .su is not just used for websites: it is embedded in **active global attack infrastructure**.

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

5. WHAT .SU SITES ACTUALLY CONTAIN - A RISK-ORIENTED TAXONOMY

A domain often associated with cybercriminal activity and political extremism also hosts astrology portals, online retailers, and Soviet-themed memorabilia galleries. The .su ecosystem is considerably more diverse-and therefore more difficult to assess at a glance - than its reputation would suggest.

Based on open-source analysis, and active domain monitoring, .su content falls into the following principal categories:

Cybercriminal Infrastructure

This is the category that generates the most serious documented risk. .su domains have been used for: botnet command-and-control servers (including the Aisuru botnet documented in late 2025); ransomware distribution and payment portals; credential theft and phishing operations; financial fraud platforms; and breach data publishing sites. The **most notorious documented case remains Exposed.su, which published the alleged credit records of Michelle Obama, Donald Trump, Mitt Romney, Mitt Romney, Beyoncé, Jay-Z, and Tiger Woods**, among others. The site has since been taken down, but it operated openly for an extended period - a demonstration of how long malicious .su sites can remain active.

Political Extremism and Influence Operations

The domain hosts a **notable concentration of ideologically motivated content on both ends of the political spectrum, united primarily by hostility to Western liberal institutions**. The most significant documented example is 4pt.su - the official website of **Alexander Dugin's Fourth Political Theory**, Eurasianist philosophy, and affiliated content. Dugin, who has been described as the intellectual architect of Russian expansionism and whose work provided ideological underpinning to Russia's foreign policy of the 2010s and 2020s, operates a multilingual platform from this domain - including content in Italian, English, Spanish, and Russian.

Igor Girkin (Strelkov), the former FSB officer who played a central command role in Russia's 2014 Donbas operation and the annexation of Crimea, maintained a personal website on igorstrelkov.su. The Donetsk People's Republic - Russia's proxy statelet in eastern Ukraine - has also registered its presence under .su. The Donetsk People's Republic website wpered.su carries content in Italian among other languages. The symbolic logic is deliberate: .su invokes Soviet legitimacy for actors seeking to project a post-Western political order.

While .su is often associated with pro-Russian and Soviet-nostalgic actors, its user base is heterogeneous and has at times included actors from across the broader Russia–Ukraine information space.

Enhanced Risks for Counterfeit Goods, Diverted Supply Chains, Brand Impersonation

This category may be of relevance to clients in the fashion, retail, and consumer goods sectors. Some .su domains appear to market luxury-branded products, raise questions regarding the authenticity or provenance of goods offered. In certain cases, these domains may redirect users to alternative storefronts or third-party sales platforms, potentially creating brand protection and consumer trust concerns.

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

The enforcement difficulty is compounded by the jurisdictional complexity outlined throughout this report. UDRP[2] complaints against .su domains face structural obstacles: the .su dispute resolution process is not aligned with standard WIPO[3] procedures, and takedown requests require cooperation from Russian-controlled infrastructure operators.

"Enforcement and takedowns would usually be advisable from a defensive perspective. Unfortunately, enforcing against them is certainly less successful compared with our usual enforcement work." - Andre Stadelmaier, Senior Director of Sales, eBrand (domain monitoring firm), July 2025

Unregulated Commercial and Entertainment Content

A significant portion of .su content is commercially motivated but not obviously criminal: illegal sports streaming platforms; online casinos and gambling platforms; grey-market software distribution; and commercial retail sites of ambiguous legitimacy.

Ideologically Curated and Nostalgic Content

A smaller but analytically interesting category consists of sites that use .su for its nostalgic or symbolic resonance: defunct Soviet-era sites preserved as digital archaeology; communist party websites never updated; and cultural or historical resources associated with the Soviet period. These sites represent minimal risk but maximum symbolic signal: the domain itself performs a political and cultural function independent of its content.

6. WHAT HAPPENS NEXT — INTELLIGENCE PERSPECTIVE

The September 2026 mandatory identity verification deadline will reshape the .su ecosystem in ways that are already visible in advance.

Three developments are likely:

- A defensive registration wave by major international brands. The immediate interest in RuCenter and Reg.ru's trusted administrator service from IP and digital asset protection firms signals that blue-chip global brands are moving to formalise their .su domain registrations before the deadline, protecting against impersonation. This is the correct defensive move — and organisations not yet monitoring their own brand presence in the .su space should do so immediately.

[2] Uniform Domain-Name Dispute-Resolution Policy

[3] World Intellectual Property Organization

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

- **A criminal infrastructure migration or adaptation.** Sophisticated cybercriminal operators who rely on .su domains will not simply comply with identity verification requirements. They will either route around them — using Russian shell entities or the trusted administrator mechanism under false identities — or migrate operational infrastructure to adjacent TLDs (.ru remains problematic, but other jurisdictionally difficult TLDs such as .st and others in the botnet space are already in active use). Monitoring for such migration is part of the threat intelligence picture.
- **Increased Russian state visibility into the .su registrant base.** The identity verification requirement, administered through Gosuslugi, means that the Russian state will have far better visibility into who holds .su domains than it does today. For non-Russian registrants, this raises legitimate questions about data security and the use to which registration data may be put by Russian state actors. Organisations with sensitive .su registrations should seek legal advice on the implications of their registration data being held in Russian government systems.

This Report Is Part of a Series

Ghost Domain: Intelligence Briefs On The .su Ecosystem

- Brief 1 of 3 — The Architecture: What .su is, who controls it, and the September 2026 law. (This document).
- Briefs 2 and 3 of 3 — Country Focus, with deep-dive into the .su domain registrant base in selected jurisdictions — examining how local factors (criminal networks, Russian communities, internet infrastructure, historical Soviet ties, and Russia's current strategic interests in the country) are reflected in and shape the .su domains registered or operated there.

If you would like to receive Briefs 2 and 3 as they are published, or to discuss a tailored digital monitoring or threat actor protection engagement for your organisation, please contact us directly. Our intelligence, cyber, and advisory teams are available for an initial briefing at short notice.