Unveiling Russian Surveillance Tech Expansion in Central Asia and Latin America

recordedfuture.com/research/tracking-deployment-russian-surveillance-technologies-central-asia-latin-america

Research (Insikt)

Tracking Deployment of Russian Surveillance Technologies in Central Asia and Latin America

Posted: 7th January 2025

By: Insikt Group®

Insikt Group®

Summary:

Several countries in Central Asia and Latin America almost certainly base their digital surveillance capabilities on Russia's System for Operative Investigative Activities (SORM), indicating that Russian surveillance technology has proliferated in Russia's near abroad and among its allies. Insikt Group identified evidence of at least eight SORM providers exporting to these regions, with at least fifteen telecommunications companies as likely customers. The largest Russian SORM providers like Citadel, Norsi-Trans, and Protei, export and participate in trade expositions across Africa, Latin America, and the Middle East, highlighting efforts to further expand globally. While these systems have legitimate security applications, the governments outlined in this report have a history of misusing surveillance capabilities , including repression of political

opposition, journalists, and activists, without effective or independent oversight. SORM facilitates interception of a wide range of internet and telecommunications traffic by authorities without the knowledge of the service providers themselves, reducing transparency and oversight of surveillance operations and increasing opportunities for abuse. Companies operating in or looking to establish physical operations in these countries should assess surveillance risks and adopt privacy tools like encryption and VPNs — to the extent permitted by local law — to mitigate sensitive communications being intercepted.

What is SORM?

Russia's SORM underpins the Russian Federation's electronic surveillance apparatus, which involves all telecommunications and ISP companies installing monitoring equipment under strict government oversight. Security and intelligence services gain direct access to telecommunications traffic passing through the installed equipment, bypassing service providers, who are not authorized to access information regarding interceptions. SORM has evolved from intercepting landline and mobile communications to monitoring internet traffic, Wi-Fi, and social media, with the latest iteration (SORM-3) enabling the collection and long-term storage of traffic and subscriber metadata in a searchable database. This system allows law enforcement authorities and security services to filter data by identifiers such as phone numbers, geolocations, IP addresses, and usernames, all supported by legal frameworks mandating compliance. The nature of SORM's integration into telecommunications and internet infrastructure facilitates potential interception and reduces visibility into surveillance operations, raising the risk of abuse, especially in countries with limited or nonexistent oversight.

Risk of Russian Government Access

Foreign deployments of SORM-based surveillance systems using Russian-manufactured components likely entail a risk of Russian access, given the close ties between SORM providers and the Russian government and the likely high value of information intercepted via these systems. Previous cases, such as the suspected exploitation of Kaspersky exports, support the assessment that Moscow can likely access exported SORM technologies. In June 2024, the US Department of Commerce's Bureau of Industry and Security (BIS) prohibited Kaspersky Lab from providing technologies and services in the US or to US persons, citing several factors of "unacceptable" risk to national security. Similar concerns apply to SORM providers, such as Citadel, which has been tied to Russian security services, specifically the Federal Security Service

(FSB), and oligarchs close to President Vladimir Putin. Citadel’s major role in the consolidation of the Russian SORM market also underscores likely connections to the Russian government. Notably, Kazakhstan and Kyrgyzstan have raised concerns about backdoors in SORM equipment, with evidence suggesting that Russian manufacturers maintained access to systems deployed abroad.

Mitigations

Companies operating in countries using SORM-based systems should mitigate the risk of interception by securing online communications with reputable encryption tools, avoiding services on hosting providers with top-level domains of these countries, limiting or removing access to sensitive corporate data during travel, and conducting comprehensive assessments of state digital and physical surveillance capabilities, focusing on evidence of malign misuse against business travelers.

In this report, Insikt Group has provided a list of indicators that companies can use to assess data privacy and surveillance risk in the context of SORM. While none of these factors guarantee a country uses SORM, the presence of several indicators is indicative of a higher state surveillance risk, including imports from known Russian SORM providers, legislation requiring the installation of interception technologies akin to SORM, joint telecommunications projects with Russian SORM providers, state control over telecommunications infrastructure, reports of intrusive or malign surveillance, and restrictions on encryption technologies. Recorded Future’s Country Risk feature offers regularly updated analysis and mitigation guidance for assessing such risks.

Outlook

The marketing materials and trade show participation of major SORM providers suggest that these organizations will very likely continue to seek opportunities for foreign expansion. Countries with close ties to Russia — especially those with histories of cybersecurity or intelligence cooperation or joint projects in the telecommunications sphere — will likely continue to source digital surveillance components from Russian providers. SORM deployments in these regions will almost certainly continue to present data security risks, particularly where oversight of government surveillance is weak. More broadly, the export of Russian surveillance technologies will continue to offer Moscow opportunities to expand its influence, particularly in its "near abroad", and potentially enhance intelligence collection capabilities, though the degree of potential access is unclear.

To read the entire analysis, click here to download the report as a PDF.

Related