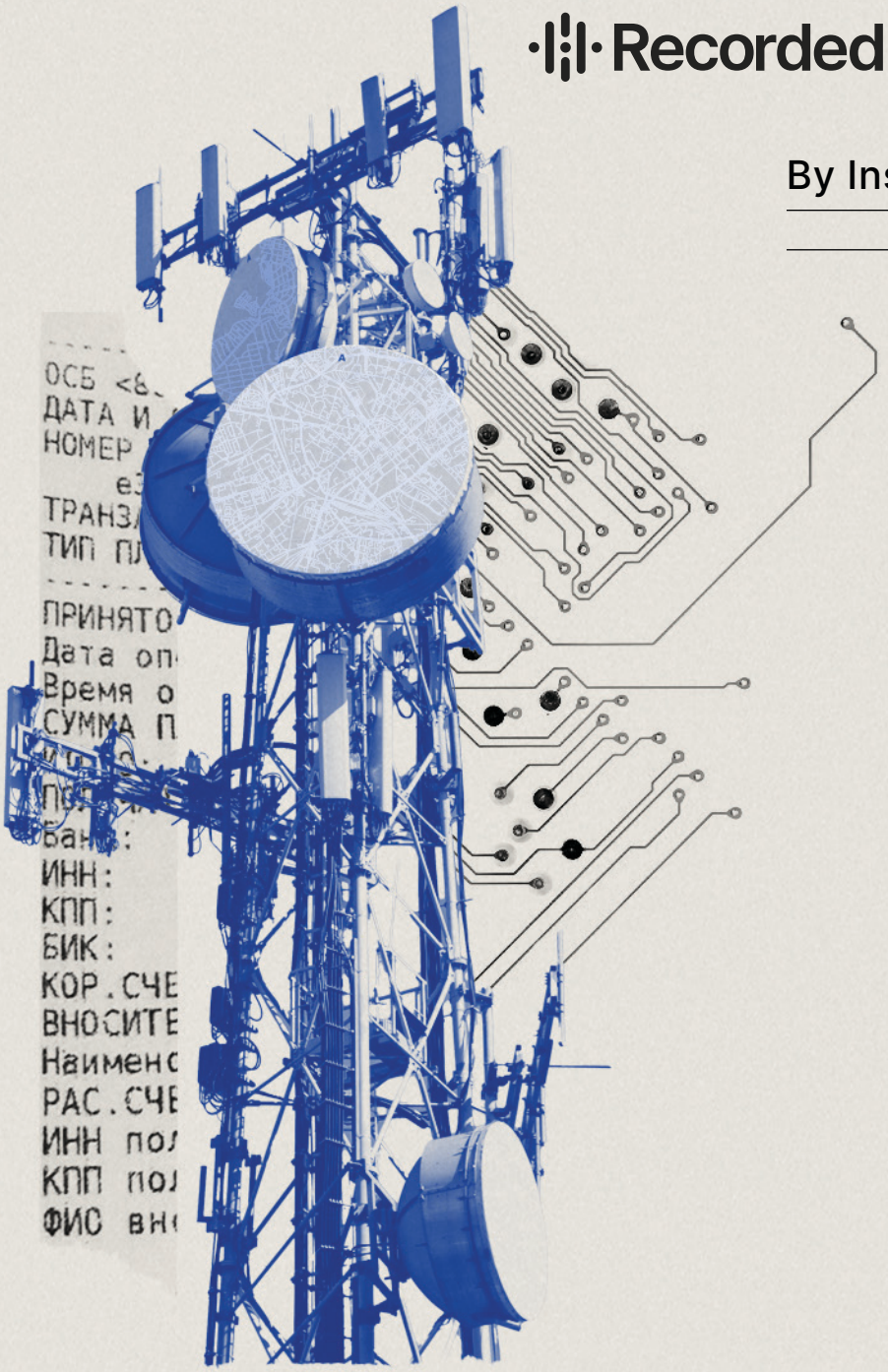
THREAT ANALYSIS

RUSSIA

Recorded Future®

By Insikt Group®

January 7, 2025




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

**Multiple Russian providers export System for Operative Investigative Activities (SORM) surveillance tools** — the backbone of Russia's digital monitoring system — to Central Asia and Latin America.

**Governments using SORM-based surveillance systems are almost certainly able to intercept a wide range of internet traffic** with little oversight, expanding opportunities for surveillance abuses.

**Moscow can likely gain access to SORM-based systems deployed abroad,** particularly those delivered by Russian providers tied to Russian security services, raising data privacy and surveillance risks.

## Executive Summary

Several countries in Central Asia — Belarus, Kazakhstan, Kyrgyzstan, and Uzbekistan — and in Latin America — Cuba and Nicaragua — 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. Russia's largest SORM technology providers — most notably, Citadel, Norsi-Trans, and Protei — export to and participate in regional trade expositions in Africa, Latin America, and the Middle East, further indicating continued efforts to expand globally.

Insikt Group identified evidence of at least eight Russian SORM providers exporting to the above countries and at least fifteen telecommunications companies that are likely customers of these providers. While there are legitimate security applications for these capabilities, the governments of these countries have a history of deploying surveillance capabilities with limited oversight for malign purposes, including repression of political opposition, journalists, and activists.

SORM deployments almost certainly increase state surveillance risks due to the breadth of data this technology is capable of ingesting and the opaque nature of its operation. Specifically, SORM facilitates interception of telecommunications data by authorities without the knowledge of the service providers themselves, reducing transparency and oversight of surveillance operations and increasing opportunities for abuse. Further complicating the threat, Russia can likely gain access to SORM-based systems abroad built with components from Russian SORM providers, based on the ties these providers have with Russian intelligence and security services, and the very likely high intelligence value of the data they contain.

Companies seeking to establish physical operations in, relocate employees to, or conduct business travel to countries employing SORM-based systems can take steps to reduce the accompanying risks to data privacy and security of data transmission. This includes conducting a comprehensive assessment of the country's surveillance capabilities and associated risk, focusing specifically on evidence of these capabilities being used against corporate interests and foreign travelers. Companies should also employ privacy tools, such as encrypted messaging applications and virtual private networks (VPNs), where legal, to mitigate the risk of sensitive communications being intercepted.

## Key Findings

- Governments in Central Asia — Belarus, Kazakhstan, Kyrgyzstan, and Uzbekistan — and in Latin America — Cuba and Nicaragua — have purchased surveillance solutions from Russian SORM providers, significantly expanding their capacity to conduct digital surveillance.
- Russian SORM providers such as Protei market their products toward governments in Africa, Latin America, and the Middle East, and participate in regional trade shows — signaling their desire to expand the market for Russian surveillance technology.

- The presence of SORM-based surveillance systems in a country almost certainly indicates government capability to intercept telecommunications and internet traffic without notifying service providers, denoting a heightened level of state surveillance risk.
- Each of the countries analyzed in this report is assessed to have high or very high state surveillance risk, has historically conducted intrusive domestic surveillance with limited oversight, and is likely to monitor foreign travelers of interest.
- In light of these risks, companies seeking to establish physical operations or conduct business travel in markets where government surveillance capabilities are based on SORM should take steps to secure online communications and limit exposure of sensitive data, including using encrypted messaging applications and VPNs.
- The provision of SORM hardware and software to foreign governments by Russian companies, particularly those with close ties to Russian security services, likely entails a degree of access to these systems by Russian intelligence. Thus, exports from Russian SORM providers likely both expand Russia's influence and enhance Moscow's intelligence collection capabilities globally.

## Methodology

To identify countries employing SORM-based surveillance systems, Insikt Group first identified Russian companies producing hardware and software solutions for SORM (**Appendix A**), based on company websites, Russian-language news, and reports from nongovernmental organizations (NGOs). Insikt Group then identified governments likely purchasing from these companies, including specific telecommunications and internet service provider (ISP) customers, where possible (**Appendix B**), based on local news reporting, company press releases, and legislation governing telecommunications interception.

## Foundations of SORM

Russia's SORM (*система оперативно-розыскных мероприятий*) underpins the Russian Federation's electronic surveillance apparatus. The system involves the installation of monitoring equipment at all telecommunications and ISP companies — a practice supported by the government's strict oversight over these providers, who are compelled under existing law to install and maintain monitoring devices.[1] Control panels (пульт управления) provide security and intelligence services direct access to all telecommunications traffic passing through the installed equipment without any further involvement from service providers, who themselves are not authorized to access information regarding interceptions. First implemented in the early 1990s, three iterations of SORM — SORM-1, SORM-2, and SORM-3 — have gradually expanded Russian authorities' ability to directly collect, monitor, and store data pertaining to telecommunications and online activity without notifying service providers, beginning with landline and mobile telephone communications and extending to internet traffic, Wi-Fi networks,

[1] *https://www.kommersant[.]ru/doc/5394668*

and social media.[2] [3] Specifically, SORM-3 enables the collection and long-term storage in a searchable database of traffic and subscriber metadata.[4] [5]

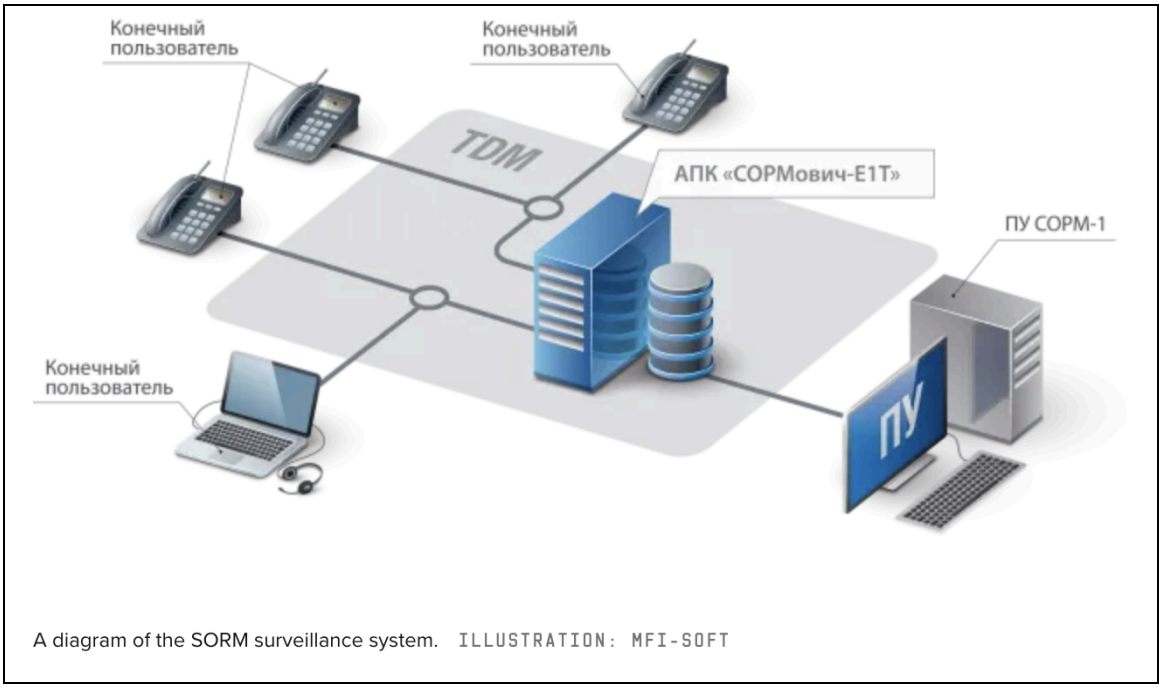



***Figure 1:*** *Diagram of SORM surveillance system, consisting of monitoring equipment, in this case APK SORMovich-E1T from SORM provider MFI-Soft, ("АПК СОрМович-E1T", denoted by the center icon) installed at a service provider, which enables monitoring of end users ("конечный пользователь", denoted by several laptop and phone icons) from the control panel "PU SORM-1" ("ПУ СОРМ-1", denoted by the monitor icon on the right) (Source: Wired)*

This system provides law enforcement and security service authorities with access to a wide range of online communications, internet traffic, and user data; Russian investigative organization Dossier Center reported that SORM allows agencies "to filter data by mobile numbers and IMEI of phones, geolocation, full name, legal entity name, IP address, email, username in messenger, and even by part of the address, phone number or other identifier".[6]

Notably, SORM is underpinned by a legal framework for "lawful interception", which requires communications service providers to comply with the establishment of the monitoring system. Russian law requires the installation of SORM equipment in all data centers and at all internet traffic communication points, including search engines, hosting sites, messaging platforms, and social networks.[7] [8] Providers that do not comply with legal requirements to install these devices risk fines and losing operating licenses, or must install the equipment in order to obtain operating licenses in the first

[2] *https://www.vedomosti[.]ru/technology/articles/2017/08/14/729199-fsb-dannim-polzovatelei*
[3] *https://archive.agentura[.]ru/dossier/russia/fsb/structure/uotm/*
[4] *https://vasexperts[.]ru/blog/sorm/osobennosti-i-otlichiya-sorm/*
[5] http://archive.today/2013.01.09-103146/http://www.norsi-trans.ru/pcategory/sorm-123/
[6] *https://dossier[.]center/sorm/*
[7] *https://roskomsvoboda[.]org/en/post/yarovizaciya-tehsetey/*
[8] *https://roskomsvoboda[.]org/en/cards/card/about-ori/*

place. Similar legislation imposes equivalent mandates for telecommunications and internet service providers in countries outside of Russia that implement SORM-based surveillance systems.

Russian state bodies very likely involved in approving or shaping export decisions of SORM technologies include Rosoboronexport, the state intermediary for the import and export of defense-related and dual-use technologies, and the Military-Industrial Commission (военно-промышленная комиссия, VPK), a permanent state body in charge of policy pertaining to "military-technical provision of national defense, state security, and law enforcement activities".[9] The export and deployment of SORM components abroad involves several primary actors:

- Commercial producers of SORM hardware and software components installed at service providers and of control panels used by government agencies
- Telecommunications equipment manufacturers and network infrastructure providers, who ensure equipment is compatible with SORM
- Intermediaries and local resellers, who may facilitate the export and sale of SORM components
- Local telecommunications and internet service providers who install SORM-compliant equipment
- Government agencies that access the data intercepted by the system — primarily, but not exclusively, intelligence services and law enforcement
- Individual end users of telecommunications and internet networks, whose data is intercepted

The nature of SORM as a surveillance system built directly into telecommunications and internet infrastructure facilitates potential interception of a vast range of data and significantly reduces visibility into digital surveillance operations, almost certainly raising the risk of abuse for countries that have historically conducted intrusive domestic surveillance with limited oversight. As SORM provider VAS Experts notes, "the person who is being monitored cannot in any way determine that this is happening, just as the [service] provider does not know who the special service is following".[10] In this, identifying deployments of SORM becomes more difficult compared to commercial off-the-shelf spyware tools, such as Predator, which can be identified and traced via changes in infrastructure. In the December 2015 case *Roman Zakharov v. Russia*, the European Court of Human Rights also expressed concern that logs of search activity via SORM are not available, virtually preventing any investigation of potential unauthorized use of the system for surveillance.

[9] *http://www.kremlin[.]ru/structure/regulation/41*
[10] *https://vasexperts[.]ru/blog/sorm/osobennosti-i-otlichiya-sorm/*

# Export of Russian SORM Technology

## Known Providers

Numerous Russian corporate entities produce SORM-compliant equipment for installation at network operators and ISPs, although the overall market share is primarily controlled by a few major corporations. This equipment includes three basic components: hardware and software installed by ISPs and telecommunications providers; control panels for remote access installed at security and intelligence services' facilities; and data transmission channels to establish the flow of data from providers to the control panel.[11] [12] The market for SORM providers is relatively consolidated, with Citadel LLC almost certainly representing the largest provider.[13] Major providers of SORM components, specifically Citadel, Norsi-Trans, and Protei, are briefly detailed below; see **Appendix A** for information on additional providers.

### *Citadel*

Registered in 2015, the Citadel (Цитадель) group became a major SORM provider by 2018, consolidating several SORM component manufacturers — Malvin Systems, MFI Soft, Osnova Lab, Signatek, and TekhArgos.[14] [15] According to Citadel's website, its companies' primary service is to "develop, implement, and provide support for software and hardware systems of SORM for network operators, owners of autonomous systems, information dissemination organizers and hosting providers".[16] In February 2023, the United States (US) imposed sanctions on Citadel and affiliated entities, estimating that Citadel accounted for 60–80% of the Russian SORM production market.

Citadel has actively sought to expand its international footprint. Citadel's website states that it develops technical solutions "for the installation of SORM 1-3 on the territory of CIS countries and other states", accounting for each country's regulatory, legal, and technical requirements, almost certainly indicating that Citadel sells to the Commonwealth of Independent States (CIS) — which includes Armenia, Azerbaijan, Belarus, Kazakhstan, Kyrgyzstan, Russia, Tajikistan, and Uzbekistan — and other countries.[17] Archived websites for Citadel companies MFI Soft and TekhArgos list multiple telecommunications customers in CIS countries (see **Figure 2**, below).[18] [19] As of August 2022, Canada-based ALOE Systems reportedly exported MFI Soft solutions for tracking user traffic, including to Argentina, Brazil, Canada, Costa Rica, El Salvador, Peru, Uruguay, and the US — although the details of these exports are unclear and almost certainly do not indicate SORM deployment in all of these countries.[20]

[11] *https://www.vedomosti[.]ru/technology/articles/2018/09/27/782237-partner-usmanova-prodolzhaet-skupat-zakona-yarovoi*
[12] *https://digital.gov[.]ru/ru/documents/3923/*
[13] *https://www.rbc[.]ru/technology_and_media/07/08/2019/5d49925e9a79473386b2d28d*
[14] *https://spark-interfax[.]ru/moskva-butyrski/ooo-tsitadel-inn-9701012339-ogrn-1157746895690-ba0ec793699c4d239e5b3479c9f1fa2a*
[15] *https://www.rbc[.]ru/technology_and_media/21/08/2017/5997071c9a7947ba1404384d*
[16] *https://ctdl[.]ru/*
[17] *https://ctdl[.]ru/solution/*
[18] https://web.archive.org/web/20180812203005/http://www.mfisoft.ru/company/clients/
[19] https://web.archive.org/web/20220815012949/https://t-argos.ru/clients/
[20] *https://mergers[.]ru/news/Struktury-sovladelca-Esforce-Antona-Cherepennikova-kupili-MFI-Soft-63311*


***Figure 2:*** *Archived version of TekhArgos's website advertising customers in CIS countries (Source: TekhArgos)*

### *Norsi-Trans*

According to Russian news outlet RBC, Moscow-headquartered Norsi-Trans (Норси Транс) controlled approximately 20–40% of the Russian SORM market in 2019, making it likely the second-largest provider after Citadel.[21] US sanctions placed on SORM providers in 2023 characterized Norsi-Trans as "one of the few companies in Russia manufacturing, developing, and selling hardware and software related to SORM capabilities". Specifically, Norsi-Trans produces various solutions for SORM-1, SORM-2, and SORM-3 under the "Vitok" ("Виток") and "Yakhont" ("Яхонт") brands (see **Figure 3**).[22] [23] For example, Norsi-Trans's "Vitok-3X" solution is marketed as an interface for analyzing information from multiple sources, including data on communication network subscribers (including IP addresses, e-mails, URL addresses, and VoIP connection session identifiers), telephone connections, financial transactions, and operations "conducted during registration of customs declarations".


***Figure 3:*** *Norsi-Trans's "Yakhont" and "Vitok" SORM solutions, translated via Google Translate (Source: Norsi-Trans)*

[21] *https://www.rbc[.]ru/technology_and_media/07/08/2019/5d49925e9a79473386b2d28d*
[22] https://web.archive.org/web/20220214225920/https://norsi-trans.ru/catalog/sorm-123
[23] *https://norsi-trans[.]com/wp-content/uploads/2018/07/Brochure_Yakhont_TLF.pdf*

Since at least 2016, Norsi-Trans has also attended multiple iterations of the ISS World Europe conference in the Czech Republic, which hosts major commercial surveillance technology providers and bills itself as "the world's largest gathering of regional law enforcement, intelligence and homeland security analysts, [and] telecoms" — very likely indicating an effort to market its products at least regionally. Specifically, in 2016 and 2018, Norsi-Trans representatives conducted seminars on its Vitok-3X and Vitok-Cluster devices, described as a "universal platform for data collection and analysis".[24] Similarly, in June 2023, Norsi-Trans participated in Infoforum-Ugra [Инфофорум-Югра] in Khanty-Mansiysk, billed as the "6th international conference on information security with the participation of BRICS, SCO, and CSTO countries", including presenting a session titled "Russia - Kazakhstan, Belarus, CSTO, BRICS, SCO Countries and Other States: Priorities for the Provision of Information Security".[25]

### *Protei*

Originally part of the Leningrad Industry Research Institute of Communications under the Russian Ministry of Communications, Protei (Научно-Технический Центр ПРОТЕЙ, or NTC Protei) develops and sells SORM hardware and software for networks "in Russia and abroad".[26] According to its website, Protei currently advertises at least ten solutions for "the requirements of SORM-1, 2 and 3".[27] Protei very likely consists of five separate legal entities, including NEOS LLC (ООО "НЕОС"), which is specifically advertised as providing SORM solutions.[28]

Protei claims "more than 400 renowned customers in over 40 countries", although it is unclear which of these customers have purchased SORM solutions, as the company also develops technology unrelated to SORM for telecommunications, video conferencing, banking, and "Safe City" projects.[29] However, Protei specifically markets a SORM operating center for CIS countries, indicating that it almost certainly provides SORM hardware and software to CIS customers.[30] Protei's website currently identifies Belarus's Life:), Kazakhstan's Astel, Kyrgyzstan's KyrgyzTelecom, MegaCom, and O!, and Uzbekistan's Ucell and Uztelecom operators as customers in the CIS.[31] It currently lists multiple telecommunications providers outside the CIS as customers, including A1 Macedonia, Asiacell (Iraq), Batelco (Bahrain), Comores Telecom (Comoros), ETECSA (Cuba), Safaricom (Kenya), Niger Telecoms (Niger), Tunisie Télécom (Tunisia), and Umniah (Jordan).[32] According to a 2022 company profile, Protei conducts projects in Eastern Europe, the Middle East, Latin America, and Africa.[33] Additionally, company press releases indicate that Protei has attended trade expositions in Africa, Latin America, and the Middle East, indicating that it markets its products outside the CIS; for example, in 2020, Protei attended the GITEX Technology Week in the United Arab Emirates and the AfricaCom online event.[34]

[24] https://web.archive.org/web/20180110041108/http://www.issworldtraining.com/ISS_EUROPE/index.htm
[25] *https://infoforum[.]ru/download/program/358/pdf*
[26] http://archive.today/2024.08.26-232407/https://neo-s.ru/about.html
[27] *https://protei[.]ru/products/oborudovanie-sorm*
[28] *https://protei[.]ru/company*
[29] *https://www.protei[.]me/*
[30] *https://protei[.]ru/products/oborudovanie-sorm/sorm-123-sng*
[31] *https://protei[.]ru/clients*
[32] Ibid.
[33] *https://esp.protei[.]com/sites/default/files/2022-04/PROTEI%20Company%20Profile%202022_0.pdf*
[34] *https://www.protei[.]ee/events/past/*

## Countries Deploying SORM-Based Systems

Insikt Group research identified six countries in Central Asia and Latin America with histories of deploying surveillance capabilities for malign purposes — Belarus, Kazakhstan, Kyrgyzstan, Uzbekistan, Cuba, and Nicaragua — that source surveillance solutions from SORM providers and have legislation providing a legal basis for lawful intercept frameworks akin to Russia's legislative structure for SORM. This is not an exhaustive list of countries purchasing from Russian SORM providers; rather, the countries outlined here illustrate how Russian SORM providers market and export surveillance technologies globally to facilitate interception of communications by law enforcement and security services.

With regard to corporate interests, SORM deployment in states with histories of malign surveillance and little independent oversight almost certainly poses a risk to sensitive corporate data transmitted by business travelers or employees based in-country. It also likely poses legal and compliance risks for communications sector companies seeking to establish business operations in these countries, which will almost certainly need to comply with local regulations for installing and maintaining SORM on their networks. For example, prior to Tele2's exit from the Kazakh market, the company stated that it complied "with all applicable laws governing security, legal interception and legal customer data retention" — almost certainly referring to SORM regulations — and operated in Kazakhstan from 2010 to 2019 despite concerns regarding the transparency of communications interception.

### *Belarus*

Belarusian president Alexander Lukashenko signed Presidential Edict no. 129 implementing SORM in the country in March 2010.[35] As such, all telecommunications service providers are mandated to install SORM-compliant hardware, and must also ensure that communications networks, facilities, and equipment are compatible with SORM during construction or upgrade. In April 2012, state-owned Beltelecom reported that it had installed SORM. In October 2022, Presidential Edict no. 368 further required online platforms to store user data and provide direct access to authorities, allowing intelligence and law enforcement services to match telecommunications and online services data.[36] According to technical requirements developed by the Ministry of Communication and Information for the implementation of SORM, "operators are responsible for limiting access to SORM equipment by staff", and SORM equipment "must be designed not to leave traces of remote searches in the operators' logbooks", limiting visibility into digital surveillance operations. According to Amnesty International, there is no requirement in Belarus that security services or law enforcement show judicial authorization for interception to communications providers before accessing data.

Belarus has almost certainly procured SORM hardware and software from several Russian companies. According to the surveillance technology tracking project Surveillance Watch, at least three Russian SORM providers — Citadel, MFI Soft, and Protei — have sold surveillance technology to Belarus.

[35] *https://pravo[.]by/document/?guid=3961&p0=P31000129*
[36] *https://pravo[.]by/document/?guid=3961&p0=P32200368*

Analytical Business Solutions has reportedly sold its "Semantic Archive" system, assessed to support SORM, to Belarus's Ministry of Internal Affairs and police. A May 2020 review on the website of VAS Experts (a provider of SORM-2 and -3 components and compatible DPI technology) indicates that the company sold SKAT DPI technology, which is compatible with SORM, to Belarusian ISP Unet.[37]

### State Surveillance Risk: Very High

We assess there is a very high state surveillance risk in Belarus, based on the government's access to advanced digital surveillance capabilities, including SORM, its history of malign use of these capabilities, and a lack of effective judicial or independent oversight preventing abuses. While digital surveillance capabilities are frequently deployed against political opposition and activists, they also likely pose a risk to foreign travelers. The US Department of State warns that foreign travelers to Belarus may be placed under surveillance, including monitoring of telephones. On March 29, 2023, Belarusian defense lawyers reportedly received a letter from the Ministry of Justice ordering the provision of personal data and information on all consultations for foreign citizens in the country, except for Russian citizens. In June 2022, Radio Liberty's Belarusian service reported that Belarusian authorities systematically wiretapped high-ranking officials and foreigners, as well as political opposition. In 2024, Freedom House reported that there is no independent judicial review or legislative oversight that provides an effective safeguard against government surveillance abuses.

## *Kazakhstan*

In 2017, the Kazakh National Security Committee implemented regulations for its SORM system to allow real-time access to networks.[38] Like Russia, Kazakhstan requires ISPs to install monitoring equipment. Telecommunications equipment is reportedly either sold SORM-compliant to companies, or local companies ensure compliance with SORM after installation at telecommunications service providers. These providers are not authorized to receive information regarding surveillance operations; in a 2019 report outlining its exit from the Kazakh market, Swedish mobile network provider Tele2 stated that "it was not possible for Tele2 KZ to know how often the SORM system was used and whether the required warrant had been obtained".

Kazakhstan has almost certainly procured SORM hardware and software from several Russian companies. MFI Soft, Protei, and VAS Experts have all reportedly supplied SORM components to Kazakhstan.[39] Archived websites of MFI Soft from September 2019 state that it has partners in Kazakhstan, and list KazakhTelecom (Қазақтелеком) as a customer.[40] [41] Archived websites of TekhArgos from March 2022 list Kcell, a subsidiary of KazakhTelecom, and the ISPs 2Day Telecom, Beeline Kazakhstan, and TNS Plus as customers.[42] According to a March 2021 review on the website of VAS Experts, Kazakh ISP X-COMMUNICATION purchased the company's SKAT DPI solution, in part to

[37] https://web.archive.org/web/20240705044030/https://vasexperts.ru/about/reviews/
[38] *https://forbes[.]kz/articles/vladeltsa_kcell_bespokoit_novyiy_prikaz_glavyi_knb_kazahstana*
[39] *http://www.pro-tech[.]kz/index.php/produkty/sorm-3/ls-sorm-yanvar*
[40] https://web.archive.org/web/20181114005554/http://www.mfisoft.ru/partnery/
[41] https://web.archive.org/web/20181115015635/http://www.mfisoft.ru/company/clients
[42] https://web.archive.org/web/20220314164718/https://t-argos.ru/#

"collect data for SORM-3".[43] Protei has also completed network equipment modernization projects for Kazakh operators Nursat and JSC Arna, including an "integrated SORM system of PROTEI's own manufacture, which provides lawful intercept capabilities in accordance with government legislation".[44] Further, the Kazakh Ministry of Emergency Situations and KazakhTelecom reportedly purchased Analytical Business Solutions's Semantic Archive system.

### State Surveillance Risk: High

We assess there is a high state surveillance risk in Kazakhstan, based on the government's access to advanced digital surveillance capabilities, including SORM, and its history of malign use of these capabilities. In 2021, Forbidden Stories and a coalition of news outlets uncovered a list of 2,000 Kazakh nationals, including political figures and oligarchs, who were likely targets of NSO Group's Pegasus spyware. In 2020, Radio Liberty reported that the Ministry of Information and Social Development's Monitoring and Analysis Center and private contractors conduct social media monitoring of the population, with digital rights experts expressing concern that such monitoring enables authorities to identify and prosecute government critics. In 2019, the Kazakh government temporarily compelled ISPs to require customers to install its Qaznet Trust Certificate, ostensibly to prevent cyberattacks and data theft, which Apple, Google, and Mozilla subsequently banned on their web browsers for intercepting HTTPS traffic. The US Department of State warns that Kazakh authorities may place foreign travelers under surveillance, likely including digital surveillance.

## *Kyrgyzstan*

Kyrgyzstan uses a version of SORM, with all ISP and mobile service providers required to install equipment compliant with the latest iteration of SORM in order to receive a license under 2014 and 2022 resolutions.[45] Upon receiving an operating license, a service provider must develop a plan for implementing the technical requirements of SORM within 30 days, including ensuring that new facilities, technological solutions, and networks are compatible with the system. Specifically, service providers must maintain and store for three years databases of subscriber information and the communications services they use; subscriber data must include full name, address, information from payment systems for the communications service, and "other data that make it possible to determine or identify the subscriber or his end device". According to the Civil Initiative on Internet Policy, at least eleven Kyrgyz state agencies, including the Defense Ministry, Customs Service, and Border Service, can access SORM.

Kyrgyzstan has almost certainly procured SORM hardware and software from several Russian companies. Russian SORM providers MFI Soft, Oniks-Line, Signatek, and TekhArgos have each reportedly provided equipment to Kyrgyzstan. Specifically, an archived version of MFI Soft's website from September 2019 lists state-owned KyrgyzTelecom (Кыргызтелеком), the largest telecommunications provider in the country, as a customer.[46] An archived TekhArgos website from

[43]https://web.archive.org/web/20220819210041/https://vasexperts.ru/resources/success-stories/xcom-bng-i-ipv6-dlya-prostogo-upravleniya-setyu/
[44] https://web.archive.org/web/20240224091251/https://www.protei.me/protei-building-ngn-networks-in-kazakhstan/
[45] *http://cbd.minjust.gov[.]kg/act/view/ru-ru/96622?cl-ru-ru*
[46] https://web.archive.org/web/20181115015635/http://www.mfisoft.ru/company/clients

August 2022 lists telecommunications provider Beeline Kyrgyzstan as a "key customer".[47] The Kyrgyz Parliament's Defense and Security Committee conducted an economic analysis in 2012 that found Russian-made SORM equipment would be three times cheaper than equivalent technology from US-Israeli surveillance technology company Verint, supporting the assessment that Kyrgyzstan has sourced SORM components from Russian providers.

#### State Surveillance Risk: High

We assess there is a high state surveillance risk in Kyrgyzstan, based on the government's access to advanced digital surveillance capabilities, including SORM, and its history of malign use of these capabilities. The US Department of State warns that local security services may place foreigners under surveillance, including digital surveillance. In 2018, Citizen Lab identified Kyrgyzstan as one of 45 countries with suspected infections of NSO Group's Pegasus spyware, with network operators MegaLine Ltd., ElCat Ltd., SkyMobile Ltd., and Saimanet Telecommunications likely infected. While judicial authorization is required for operations infringing on constitutional privacy rights, such as wiretapping, multiple cases of illicit wiretapping and surveillance illustrate that authorities ignore legal privacy protections. In August 2021, the Ministry of the Interior acknowledged it had carried out wiretapping operations against more than 100 opposition politicians, lawyers, and activists in January and February 2021, purportedly in the course of investigations into October 2020 anti-government protests. However, the list of surveilled individuals also included those not participating in the protests.

### *Uzbekistan*

Under Uzbekistan's Law on Telecommunications and Presidential Decree 513 on Measures for Increasing the Effectiveness of Operational and Investigative Actions on Telecommunications Networks, internet service and telecommunications providers must install SORM-compliant equipment in order to receive an operating license.[48] Similarly to Russia, information on the extent and purpose of telecommunications monitoring is not shared with Uzbek telecommunications providers.

Uzbekistan has almost certainly procured SORM hardware and software from a range of Russian companies. According to a 2015 Privacy International report, Uzbekistan's State Unitary Enterprise Scientific Engineering and Marketing Research Center (UNICON) conducts SORM equipment certification, testing, and development. MFI Soft, Protei, and VAS Experts have reportedly exported SORM components to Uzbekistan. An archived version of MFI Soft's website from September 2019 lists state-owned Uzbektelecom (Узбектелеком) as a customer.[49] Specifically, MFI Soft has reportedly exported its SORMovich system to Uzbektelecom via ALOE Systems. Of note, Uzbektelecom is currently the only internet provider permitted to connect to the international internet, with other service providers required to route through Uzbektelecom's infrastructure until January 2025.

[47] https://web.archive.org/web/20220815012949/https://t-argos.ru/clients/
[48] *http://www.lex[.]uz/Pages/GetAct.aspx?lact_id=33152*
[49] https://web.archive.org/web/20181115015635/http://www.mfisoft.ru/company/clients

### State Surveillance Risk: High

We assess there is a high state surveillance risk in Uzbekistan, based on the government's access to advanced digital surveillance capabilities, including SORM, and its history of malign use of these capabilities. In January 2024, the US Department of State warned that security services closely monitor foreign visitors and that privacy in phone or internet communications should not be expected. Additionally, per the US Department of State, Uzbek law allows the National Guard, Prosecutor General's Office, and police to electronically surveil attorney-client communications. While law enforcement is required to obtain warrants for internet traffic interception, these are approved by prosecutors and do not require judicial review — likely limiting their efficacy as a check on government overreach.

## *Cuba*

While Cuba's legislation pertaining to telecommunications interception does not specifically cite SORM, its legislative framework is likely compatible with this type of mass surveillance technology. The government requires telecommunications providers to store data on users for at least one year, and has reportedly installed Ávila Link monitoring software at Cuba's state-owned monopoly, the Telecommunications Company of Cuba SA (ETECSA), and public access points. Additionally, the 2019 Decree Law 389 authorizes digital and physical surveillance without judicial approval, including intercepting and recording communications and accessing information and communication technology systems.

Cuba has very likely procured SORM hardware and software from Russian companies, most notably Protei. In November 2022, the US-based Institute for National Strategic Studies (INSS) reported that Protei provided Russian SORM technology to Cuba, Nicaragua, and Venezuela. INSS assessed that the "Russian National Committee for the Promotion of Economic Trade with Countries of Latin America", or NK SESLA (CN CEPLA in Spanish), serves as an "unofficial association of intelligence and surveillance providers".[50] Specifically, "NK SESLA continues to offer dozens of PROTEI surveillance products on its Spanish-language transactions, e-mails, phone calls, text messages, social networks, Wi-Fi networks, and forum posts". Protei has participated in multiple Havana International Fair (FIHAV) expositions, intended to showcase Russian products to Cuban and Latin American markets, and reportedly met with Cuban government representatives, based on press releases from 2009 to 2024 — indicating that Protei almost certainly seeks to market its products to Cuban and Latin American customers.[51] [52] [53] [54] Most recently, Protei signed an agreement with Cuban state-owned operator Movitel "to facilitate the construction of private network systems" in March 2024, after attending the Informática 2024 conference in Havana.[55] A 2022 company profile specifically identifies ETECSA as a Protei customer.[56]

[50] *https://cncepla[.]ru/es/*
[51] *https://www.cncepla[.]ru/press-center/events/1649/?PAGEN_3=86*
[52] *https://cncepla[.]ru/press-center/events/1765/?PAGEN_3=65*
[53] *https://fihav[.]ru/exhibitors-2018/*
[54] https://web.archive.org/web/20240614223547/https://fihav.ru/exhibitors-2018/
[55] *https://protei[.]ru/news/protey-podpisal-soglashenie-na-kube*
[56] *https://esp.protei[.]com/sites/default/files/2022-04/PROTEI%20Company%20Profile%202022_0.pdf*

### State Surveillance Risk: High

We assess there is a high state surveillance risk in Cuba, based on the government's access to advanced digital surveillance capabilities, including SORM, its history of malign use of these capabilities, and a lack of effective judicial or independent oversight preventing abuses. According to the US Department of State, agents from the Ministry of Interior's General Directorate for State Security regularly conduct surveillance, including electronic surveillance, on foreign journalists, diplomats, academics, and businesspersons. In recent years, digital rights groups have expressed concern that the government can conduct broad surveillance via access to data collected through state-affiliated applications. For example, in November 2022, YucaByte reported that ETECSA was cooperating with the Defense Information Technology Company (XETID), a subsidiary of Cuba's Revolutionary Armed Forces (FAR) — likely allowing the FAR to access personal data on Cuban citizens.

## *Nicaragua*

While Nicaragua's legislation pertaining to telecommunications interception does not specifically cite SORM, its legislative framework is very likely compatible with SORM. In January 2021, TELCOR published regulations for the implementation of the Special Cybercrimes Law, which requires telecommunications companies to collect and store data for tracing communications, including the recipient, time, date, and duration of communication; the regulations also require geolocation and identification of equipment used for communication. Further, under the 2010 Law on the Prevention, Investigation, and Prosecution of Organized Crime, telecommunications and online communication service providers must "allow the use of their equipment and facilities for the practice of the investigative procedures", referring to interception, and ensure that their facilities and equipment are designed to be technically compatible with such interception.

Nicaragua has very likely procured SORM hardware and software from Russian companies. The Nicaraguan government has reportedly used SORM technology obtained via the NK SESLA network since 2018. Further, according to a September 2019 report from the University of Oxford, St. Petersburg-based VAS Experts exported SORM equipment to Nicaragua. A February 2019 review available on the website of VAS Experts indicates that Yota Nicaragua purchased its SKAT DPI technology, which is compatible with SORM, and had been using it since 2014. The review cites "good cost-functionality ratio, Russian-language technical support, ease of integration with external systems, [and] desire to support a Russian manufacturer" as reasons for the purchase of SKAT DPI.[57]

### State Surveillance Risk: High

We assess there is a high state surveillance risk in Nicaragua, based on the government's access to advanced digital surveillance capabilities, including SORM, its history of malign use of these capabilities, and a lack of effective judicial or independent oversight preventing abuses. Nicaragua's 2015 Sovereign Security Law prohibits the interception of communications without a court order, but the US Department of State reported in 2022 that the government does not respect these restrictions. The

[57] https://web.archive.org/web/20240705044030/https://vasexperts.ru/about/reviews/

2020 Law on the Regulation of Foreign Agents subjects individuals and entities receiving funding from abroad or working for foreign businesses, governments, or organizations to extensive government scrutiny, which the Nicaraguan government likely exploits to gather detailed information on domestic targets. The US Department of State warns that Nicaraguan authorities and armed civilians known as "para police" may monitor or question US citizens regarding their activities and contact with Nicaraguan citizens — likely including digital surveillance.

## Risk of Russian Government Access

Foreign deployments of SORM-based surveillance systems using Russian-manufactured components likely entail a risk of Russian access, due to ties between major SORM providers and the Russian government and the very likely high value of information intercepted via these systems. Previous cases in which Moscow is suspected of exploiting other sensitive Russian technology exports — most notably, Kaspersky — support the assessment that it can likely access exported SORM technologies.

In June 2024, the US Department of Commerce's Bureau of Industry and Security (BIS) prohibited Russian anti-virus and cybersecurity company Kaspersky Lab from providing software or services in the US or to US persons. The factors cited by BIS in making this decision almost certainly apply to Russia-based SORM providers, raising the risk that Moscow can exploit SORM systems installed abroad to collect information. Notably, BIS cited Russia's "capability and intent to exploit Russian companies, like Kaspersky Lab, to collect and weaponize sensitive U.S. information". BIS found that Kaspersky posed an "unacceptable" risk to national security due to three factors: 1) the Russian government's jurisdiction over it — under which it must comply with requests for information that could enable access to sensitive information of customers using its software; 2) its access to sensitive US customer information; and 3) its capability to install malicious software or withhold critical updates.

Additionally, reporting from Russian news outlet RBC indicates Citadel is likely tied to Russian security services, specifically the Federal Security Service (FSB), with former FSB and Ministry of Internal Affairs (MVD) officials holding high-level positions at Citadel.[58] Further, ties between Citadel founder Anton Cherepennikov and oligarch Alisher Usmanov — a close associate of Russian President Vladimir Putin — as well as Cherepennikov's major role in the consolidation of the Russian SORM market, point to likely connections to the Russian government.[59] [60] [61] From 2005 to 2018, Cherepennikov consolidated at least five SORM providers and purchased Nexign (formerly Peter-Service), assessed to provide SORM solutions, in 2019 — moves he likely would not be able to make without at least the tacit approval of the Russian government, considering the importance of this industry.[62] In February 2023, the US Department of State identified Cherepennikov as Citadel's owner via his company ICS Holding, which he founded in 2018 to unite 23 companies in the information security and SORM space.[63]

[58] *https://www.rbc[.]ru/technology_and_media/21/08/2017/5997071c9a7947ba1404384d*
[59] *https://www.forbes[.]ru/tehnologii-photogallery/386387-14-biznesmenov-i-menedzherov-kotorye-sozdayut-rossiyskiy-kibersport*
[60] *https://tass[.]ru/ekonomika/18337251*
[61] *https://www.vedomosti[.]ru/technology/articles/2020/04/30/829371-iks-holding*
[62] *https://1sn[.]ru/glava-krupneisei-V-rossii-it-kompanii-skoncalsya-vo-vremya-modnoi-procedury*
[63] *https://www.kommersant[.]ru/doc/6122410*

Reflecting concerns regarding potential Russian access, the Kazakh National Security Council reportedly chose not to use certain Russia-made components of SORM-3 in favor of domestic equivalents, due to suspected backdoors. In November 2012, Radio Liberty's Kyrgyz Service reported that foreign intelligence services may have obtained access to Kyrgyzstan's Russia-produced SORM system, citing the 2010 publication of intercepted telephone conversations between Kyrgyz politicians. The Bishkek, Kyrgyzstan-based Civil Initiative of Internet Policy reported that Russian equipment manufacturers retained passwords used to access and operate SORM software. Specifically, Oniks-Line and Signatek were accused of maintaining access to their SORM equipment used in Kyrgyzstan.[64]

## Mitigations

Companies seeking to establish physical operations in, relocate employees in, or conduct business travel to, countries employing SORM-based systems should consider the following mitigation strategies.

- To mitigate the risk of interception, secure online communications with reputable privacy and encryption tools, such as encrypted messaging applications and VPNs — although users should avoid services based in these countries, which may be required to log user activity. Corporate legal teams should review country-specific laws around the legality of encrypted messaging applications and VPNs, as illegal use could result in detainment and criminal charges.
- If possible, avoid services on hosting providers with top-level domains of countries using SORM (for example, Russian hosting providers must install SORM equipment on their infrastructure).
- While traveling to these countries, consider limiting or removing employee access to corporate accounts or applications with sensitive data for the duration of travel.
- Corporate entities should conduct a comprehensive assessment of the country's state-run digital and physical surveillance capabilities, seeking evidence of those capabilities being used for malign purposes, such as against business travelers.
- Recorded Future customers can use Recorded Future's Country Risk feature, which includes regularly updated analysis of a country's data privacy and surveillance risk and can aid in the development of such assessments; Country Risk Scores for each country can be found on the country's Intelligence Card within the Recorded Future Intelligence Cloud.
- Customers can also consult Recorded Future's data privacy and surveillance risk mitigations for travelers.

Companies can use the following indicators to develop assessments of a country's surveillance capabilities and risk in the context of SORM. While none of the below factors alone is a guarantee that a country uses SORM, the presence of multiple indicators likely entails a higher state surveillance risk:

[64] Andrei Soldatov and Irina Borogan, *The Red Web: The Struggle Between Russia's Digital Dictators and the New Online Revolutionaries* (PublicAffairs, 2015), 375.

- Imports from known Russian providers of SORM hardware and software (see **Appendix A**)
- Legislation requiring telecommunications and internet service providers to install equipment facilitating interception of communications akin to SORM
- Press releases or news articles indicating joint telecommunications projects with Russian companies involved in the SORM supply chain
- High level of state control over telecommunications and internet infrastructure
- Reports indicating state access to telecommunications and internet communications, such as local media reporting or court cases regarding arrests or charges based on individuals' personal communications, especially of political dissidents, journalists, or activists
- Significant restrictions on encryption technologies that could protect against data interception

## Outlook

Based on marketing documents and regional subsidiary webpages of major SORM providers that advertise surveillance products outside Russia, as well as their participation in regional trade shows, the companies highlighted in this report will very likely continue to expand their operations abroad. For example, in January 2023, Citizen Lab reported that Iranian mobile network operator Ariantel corresponded with Protei regarding solutions for a legal intercept system. In particular, countries with close ties to Russia, especially those with a history of cybersecurity or intelligence cooperation or joint projects in the telecommunications sphere, will likely continue to source digital surveillance components from Russian providers. Deployment of SORM in these countries will almost certainly continue to present risks to the transmission of data security — exacerbated where judicial oversight does not present an effective check against government surveillance overreach.

More broadly, the export of Russian surveillance technologies will likely continue to offer Moscow opportunities to expand its influence, particularly in areas it deems to be under its traditional sphere of the "near abroad". The deployment of Russian interception solutions in the telecommunications infrastructure of a country will also likely continue to provide Moscow with intelligence collection capabilities, though the degree of its potential access to these systems is unclear.

# Appendix A: Russian SORM Providers

| Provider | Details |
|---|---|
| Analytical Business Solutions (Аналитические Бизнес Решения) | Analytical Business Solutions (Taxpayer Identification Number, TIN or Идентификационный номер налогоплательщика, ИНН: 7707524315) develops the "Semantic Archive" intelligence system, described as "a tool for creating an integrated storage of information".[65] [66] The Semantic Archive system reportedly supports SORM-3, specifically by providing an easily searchable database for the data logged from varied communications streams. |
| Citadel (Цитадель) | The Citadel group (TIN: 9701012339) incorporates several SORM manufacturers — Malvin Systems, MFI Soft, Osnova Lab, Signatek, and TekhArgos — as well as other telecommunications software providers.[67] [68] [69] A January 2023 archived version of Citadel's website identifies several of its companies as providing the following SORM components: MFI Soft (SORM 2–3), Osnova Lab (SORM 1), Malvin Systems (SORM 1), Garda Technologies, TekhArgos (SORM 2–3), Signatek (SORM control panel simulators), ADM Systems, and Bastion.[70]<br><br>Citadel's ownership information no longer appears in the public register of legal entities in Russia, very likely due to a September 2022 decree exempting sanctioned Russian companies from inclusion.[71] Following Anton Cherepennikov's death in July 2023, Citadel's ownership is unclear.[72] [73] |
| Iskra Technologies (Искра Технологии) | Iskra Technologies (TIN: 6660017837), formerly IskraUralTEL,[74] founded by Slovenian company Kontron (formerly Iskratel), is a "Russian manufacturer of communication equipment, digital platforms and automation systems, developer of specialized and applied software".[75] In 2013, Privacy International reported that IskraUralTEL produced at least three SORM components; while Iskra Technologies' website makes no mention of SORM or related technologies, a 2017 Iskratel document states that the company develops lawful interception solutions, including for SORM. |

[65] *https://www.org-info[.]com/company/72946*
[66] *http://old.anbr[.]ru/about/about/*
[67] *https://www.rbc[.]ru/technology_and_media/21/08/2017/5997071c9a7947ba1404384d*
[68] *http://mergers[.]ru/news/Struktury-sovladelca-Esforce-Antona-Cherepennikova-kupili-MFI-Soft-63311*
[69] *https://www.rusprofile[.]ru/id/10165631*
[70] https://web.archive.org/web/20230131195356/https://ctdl.ru/
[71] *http://publication.pravo.gov[.]ru/Document/View/0001202209200009*
[72] *https://www.interfax[.]ru/business/845596*
[73] *https://www.forbes[.]ru/tekhnologii/457797-usm-usmanova-prodast-it-gruppu-iks-holding*
[74] *https://www.iskratechno[.]ru/news/iskrauraltel-rastet-i-menyaet-imya-na-iskra-tekhnologii/*
[75] *https://www.rusprofile[.]ru/id/1146275*

| | |
|---|---|
| Malvin Systems (Малвин Системс; Citadel) | On an archived version of its website from October 2019, Malvin Systems (TIN: 7729557963) markets itself as a provider of "SORM solutions for manufacturers of telecommunications equipment".[76] [77] Specifically, it offers solutions for implementing SORM when using telecommunications equipment from Ericsson, Nokia, Dialogic, Huawei, and ZTE for fixed-line and mobile operator networks. While Malvin's current website is inaccessible, a May 2024 archived version states that Malvin Systems joined Citadel from March 2023, but "all company specialists continue to work as usual".[78] |
| MFI Soft (МФИ Софт; Citadel) | MFI Soft (TIN: 7710657509) is part of the Citadel group and, according to company sites, is known as "LLC Citadel" as of July 2023, although "all company specialists continue to work as usual".[79] [80] The company produces "a complete implementation of all three versions of SORM", including SORMovich, which is "scalable to a network of any size".[81] MFI Soft also manufactures IP SORM Yanvar for SORM-3, which facilitates interception of all phone calls, SMSs, and internet activity; geolocates users; can conduct 100 simultaneous searches; and stores intercepts for three years.[82]<br><br>MFI Soft is reportedly represented by Canada-based ALOE Systems (formerly known as MERA Systems and owned by Anton Cherepennikov) outside Russia. Specifically, ALOE Systems supplies MFI Soft products under the name "Netbeholder". |
| Network Solutions (Сетевые Решения) | Network Solutions (TIN: 77265520179) is a Russian software developer specializing in billing for telecommunications operators.[83] According to the company's website, it offers solutions for "transferring data to SORM" in addition to billing solutions. The website states that "it is possible to transfer data to SORM directly from certified billing", adding that data transferred to SORM includes "information about calls and payments of subscribers", "personal customer data", and "correct and complete addresses, passport details of individuals and details of legal entities".[84] Specifically, it integrates with technology from MFI Soft (Yanvar), Norsi-Trans (Yakhont), RTK NT (ELCOM-NT), Signatek (Visir), Special Technologies (Omega), TekhArgos, and VAS Experts. |

[76] *https://www.org-info.com/company/4437919*
[77] https://web.archive.org/web/20190215055723/http://www.malvinesystems.ru/
[78] https://web.archive.org/web/20240529041330/https://www.malvinesystems.ru/
[79] *https://www.mfisoft[.]ru/*
[80] *https://www.org-info[.]com/company/4536622*
[81] *https://www.mfisoft[.]ru/solutions/cormovich/*
[82] *https://www.mfisoft[.]ru/solutions/yanvar/*
[83] *https://www.org-info[.]com/company/755496*
[84] *https://www.lanbilling[.]ru/services/sorm/*

| | |
|---|---|
| Nexign/Peter-Service | Nexign (TIN: 7801019126), formerly Peter-Service, was founded in 1992 in St. Petersburg and provides business support systems for telecommunications operators.[85] According to WikiLeaks documents from September 2017, Peter-Service produced data retention and traffic analysis technology for SORM, although the company states it does not offer SORM products or access user data from telecommunications service providers. Nexign is part of Alisher Usmanov's USM Telecom holding.[86] |
| Nika-X (Ника-Х) (Citadel) | According to its website, Nika-X (TIN: 9731017006) "produces and performs a full cycle of work on the implementation of SORM for telecom operators, owners of autonomous systems and information dissemination organizers".[87] [88] Its products are part of the brand name "Vector" ("Вектор"). |
| Norsi-Trans (Норси-Транс) | Moscow-headquartered Norsi-Trans (TIN: 7118021939) is likely the second-largest SORM provider, accounting for approximately 20–40% of the Russian SORM market in 2019.[89] [90] Specifically, Norsi-Trans produces "Vitok" ("Виток") devices for SORM-2 and Yakhont ("Яхонт") for SORM-3.[91] [92] |
| Oniks-Line (Оникс-Лайн) | Oniks-Line (TIN: 7727682221), based in Moscow, has operated since 2009 and produces SORM equipment for the Ministry of Emergencies, the Federal District of Russia, and multiple telecommunications operators, according to its website.[93] [94] |
| Osnova Lab (Основа Лаб; Citadel) | Osnova Lab (TIN: 7701100976) operates under Citadel; on its website, it claims to be "the first company in Russia to develop and launch the SORM solution for IMS platforms".[95] [96] An archived version of its website states that its clients include "leading global manufacturers of telecommunications equipment". Osnova Lab markets SORM components under the brand "Olympus" ("Олимп"). |
| Protei (Научно-технический центр ПРОТЕЙ) | Protei (TIN: 7825483961) develops and sells SORM hardware and software for networks "in Russia and abroad".[97] Protei currently advertises at least ten SORM solutions. Specifically, in July 2024 |

[85] *https://www.rusprofile[.]ru/id/2705787*
[86] *https://www.cnews[.]ru/news/top/2022-02-09_byvshij_glava_mailru_budet_prismatrivat*
[87] *https://www.org-info[.]com/company/12050440*
[88] *https://nikasorm[.]ru/*
[89] *https://www.rbc[.]ru/technology_and_media/07/08/2019/5d49925e9a79473386b2d28d*
[90] *https://www.org-info[.]com/company/11698135*
[91] https://web.archive.org/web/20230609084217/https://norsi-trans.ru/catalog/paket-yarovoy/yakhont-golos374/
[92] *https://norsi-trans[.]com/wp-content/uploads/2018/07/Brochure_Yakhont_TLF.pdf*
[93] https://web.archive.org/web/20240701165255/http://www.onx-line.ru/
[94] *https://www.org-info[.]com/company/5746438*
[95] https://web.archive.org/web/20240525085836/https://osnovalab.ru/
[96] *https://www.org-info[.]com/company/8152473*
[97] *https://www.rusprofile[.]ru/id/3879268*

| | |
|---|---|
| | marketing documents, its subsidiary NEOS LLC (НЕОС, TIN: 7802700779)[98] advertises SORM solutions, including "passive interception systems for location and SMS", "technical solutions for SORM-2", and a "control panel simulator" for "checking the operability of SORM during implementation, delivery and certification".[99] [100] Protei also offers training, technical support, and "updating of SORM solutions to meet new legal requirements". |
| Signatek (Сигнатек; Citadel) | Novosibirsk-headquartered Signatek (TIN: 5408114571), acquired by Citadel in 2018, describes itself as "one of the leading Russian developers of professional equipment in the field of collection, distribution and processing of information for operational-search entities, as well as SORM solutions".[101] [102] It reportedly markets SORM systems under the brand name "Visir" ("Визирь").[103] |
| Special Technologies (Специальные Технологии) | Special Technologies (TIN: 7714343013), headquartered in Moscow, produces "all types of SORM systems from a leading Russian provider".[104] [105] Specifically, the company produces APK "Omega" (АПК "ОМЕГА"), advertised as a hardware and software complex designed to connect to data transmission networks and transfer information to SORM control panels. |
| TekhArgos (ТехАргос; Citadel) | TekhArgos (TIN: 7716856518), part of Citadel since 2018, "was established in 2009 as an organization engaged in the development, production and implementation" of SORM equipment on networks of Russian and CIS operators.[106] According to its website, TekhArgos is now part of "Garda Telekom" (Гарда Телеком), and its SORM activities were transferred to Citadel as of January 2023.[107] Per an archived website from December 2022, the company has completed over 300 projects in Russia and CIS countries.[108] |
| VAS Experts (ВАС Экспертс) | VAS Experts (TIN: 7841476577) provides SORM hardware and software systems for SORM-2 and -3, along with DPI technology, according to its website.[109] [110] Specifically, the company's SKAT DPI technology (СКАТ DPI) provides SORM support. VAS Experts serves customers in Azerbaijan, Kazakhstan, Lithuania, Nicaragua, and Uzbekistan. |

[98] *https://www.rusprofile.ru/id/11961279*
[99] http://archive.today/2024.08.26-232407/https://neo-s.ru/about.html
[100] *https://protei[.]ru/sites/default/files/2024-07/NeoS_presentation_Russia%202024.pdf*
[101] https://web.archive.org/web/20240225025952/https://www.signatec.ru/about
[102] *https://www.org-info[.]com/company/127516*
[103] *https://www.vedomosti[.]ru/technology/articles/2018/09/27/782237-partner-usmanova-prodolzhaet-skupat-zakona-yarovoi*
[104] https://web.archive.org/web/20240816100156/https://st-sorm.ru/
[105] *https://www.org-info[.]com/company/2359111*
[106] *https://www.org-info[.]com/company/9791468*
[107] https://web.archive.org/web/20240715200444/https://t-argos.ru/about/
[108] https://web.archive.org/web/20221205140610/https://t-argos.ru/about/
[109] https://web.archive.org/web/20240715000923/https://vasexperts.ru/products/sorm/
[110] *https://www.org-info[.]com/company/1592291*

# Appendix B: Known Telecommunications Customers of Russian SORM Providers

| Customer | Location | Details |
|---|---|---|
| Unet | Belarus | Client of VAS Experts[111] |
| Beeline Казахстан | Kazakhstan | Client of TekhArgos[112] |
| Kazakhtelecom | Kazakhstan | Client of MFI Soft[113], Analytical Business Solutions |
| Kcell | Kazakhstan | Client of TekhArgos[114] |
| Nursat | Kazakhstan | Client of Protei[115] |
| Tele2 | Kazakhstan | Client of TekhArgos[116] |
| TNS Plus | Kazakhstan | Client of TekhArgos[117] |
| X-COMMUNICATION | Kazakhstan | Client of VAS Experts[118] |
| 2Day Telecom | Kazakhstan | Client of TekhArgos[119] |
| Beeline Кыргызстан | Kyrgyzstan | Client of TekhArgos[120] |
| KyrgyzTelecom | Kyrgyzstan | Client of MFI Soft[121] |
| Uzbektelecom | Uzbekistan | Client of MFI Soft[122] |
| ETECSA | Cuba | Client of Protei[123] |
| Yota Nicaragua | Nicaragua | Client of VAS Experts[124] |

[111] https://web.archive.org/web/20240705044030/https://vasexperts.ru/about/reviews/
[112] https://web.archive.org/web/20221205152742/https://t-argos.ru/clients/
[113] https://web.archive.org/web/20180812203005/http://www.mfisoft.ru/company/clients/
[114] https://web.archive.org/web/20221205152742/https://t-argos.ru/clients/
[115] https://web.archive.org/web/20240224091251/https://www.protei.me/protei-building-ngn-networks-in-kazakhstan/
[116] https://web.archive.org/web/20221205152742/https://t-argos.ru/clients/
[117] https://web.archive.org/web/20221205152742/https://t-argos.ru/clients/
[118]https://web.archive.org/web/20220819210041/https://vasexperts.ru/resources/success-stories/xcom-bng-i-ipv6-dlya-prostogo-upravleniya-setyu/
[119] https://web.archive.org/web/20221205152742/https://t-argos.ru/clients/
[120] https://web.archive.org/web/20221205152742/https://t-argos.ru/clients/
[121] https://web.archive.org/web/20180812203005/http://www.mfisoft.ru/company/clients/
[122] https://web.archive.org/web/20180812203005/http://www.mfisoft.ru/company/clients/
[123] *https://esp.protei[.]com/sites/default/files/2022-04/PROTEI%20Company%20Profile%202022_0.pdf*
[124] https://web.archive.org/web/20240705044030/https://vasexperts.ru/about/reviews/

*Recorded Future reporting contains expressions of likelihood or probability consistent with US Intelligence Community Directive (ICD) 203: Analytic Standards (published January 2, 2015). Recorded Future reporting also uses confidence level standards employed by the US Intelligence Community to assess the quality and quantity of the source information supporting our analytic judgments.*

## *About Insikt Group®*

*Recorded Future's Insikt Group, the company's threat research division, comprises analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence that reduces risk for customers, enables tangible outcomes, and prevents business disruption.*

## *About Recorded Future®*

*Recorded Future is the world's largest threat intelligence company. Recorded Future's Intelligence Cloud provides end-to-end intelligence across adversaries, infrastructure, and targets. Indexing the internet across the open web, dark web, and technical sources, Recorded Future provides real-time visibility into an expanding attack surface and threat landscape, empowering customers to act with speed and confidence to reduce risk and securely drive business forward. Headquartered in Boston with offices and employees around the world, Recorded Future works with over 1,800 businesses and government organizations across more than 75 countries to provide real-time, unbiased, and actionable intelligence.*

*Learn more at recordedfuture.com*