Florida International University

FIU Digital Commons

Research Publications

Fall 9-27-2024

How Russian Surveillance Tech is Reshaping Latin America

Doug Farah

Follow this and additional works at: https://digitalcommons.fiu.edu/jgi_research

Part of the International Relations Commons

This work is brought to you for free and open access by FIU Digital Commons. It has been accepted for inclusion in Research Publications by an authorized administrator of FIU Digital Commons. For more information, please contact dcc@fiu.edu.

JACK D. GORDON INSTITUTE
FOR PUBLIC POLICY

HOW RUSSIAN SURVEILLANCE TECH

IS RESHAPING LATIN AMERICA

AUTHOR
DOUGLAS FARAH

SEPTEMBER 2024

The Jack D. Gordon Institute for Public Policy, part of FIU's Steven J. Green School for International & Public Affairs was founded in 1985 to establish, promote, and advance the study of public policy and national security studies. The Gordon Institute serves as the forefront of public policy discourse by leading, integrating, and delivering exceptional multidisciplinary education and research while improving the competitiveness and diversity of students and professionals entering the workforce. The Gordon Institute is centered on four pillars: Academics, Professional Education, Research, and Community Outreach, each serving the mission of shaping public policy and national security solutions in the 21st century.

Disclaimer: This product is part of the Florida International University—United States Southern Command Academic Partnership. United States Southern Command provides funding to support this series as part of its analytic outreach efforts. Analytic outreach is intended to support United States Southern Command with new ideas, outside perspectives, and spark candid discussions. The views expressed in this report are those of the author and do not necessarily reflect the official policy or position of the United States Government, United States Southern Command, Florida International University, or any other affiliated institutions.

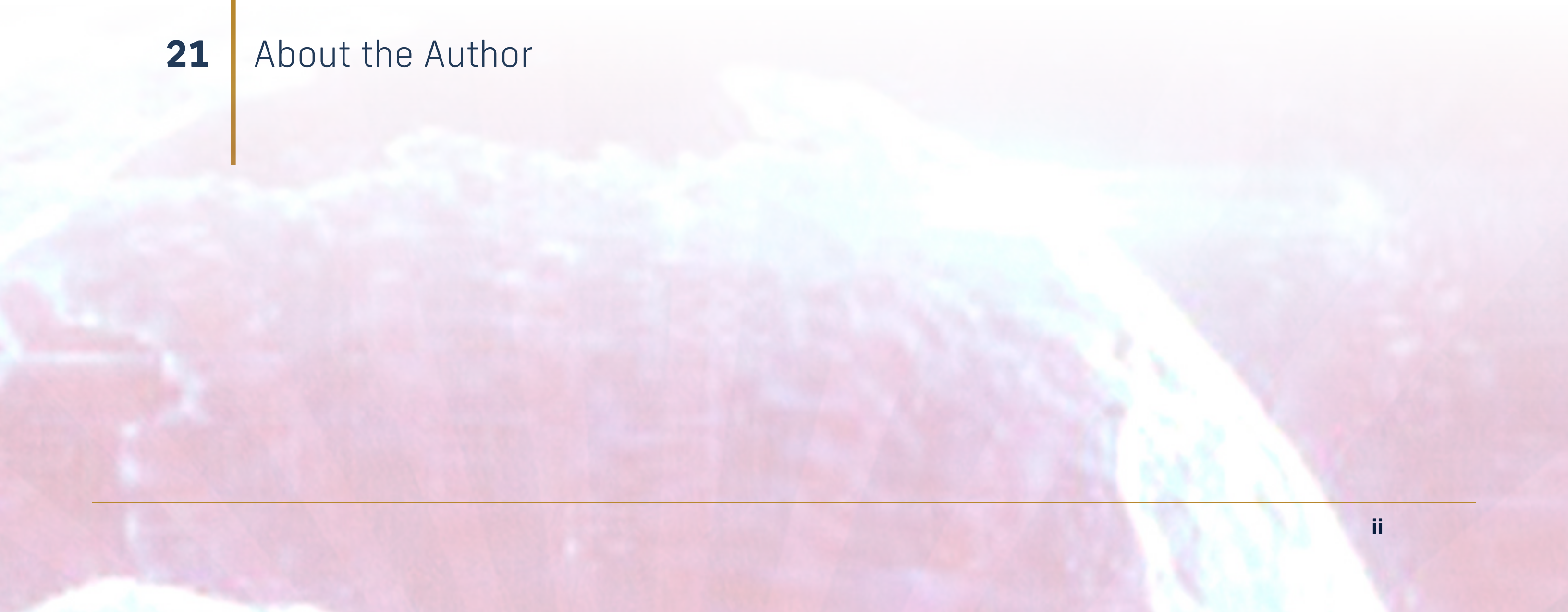
Permission Statement: No part of this work may be reproduced in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system without the permission of the Jack D. Gordon Institute for Public Policy.

Requests for permission should include the following information:

- The title of the document for which permission to copy material is desired.
- A description of the material for which permission to copy is desired.
- The purpose for which the copied material will be used and the manner in which it will be used.
- Your name, title, company or organization name, telephone number, e-mail address and mailing address.

Please send all requests for permission to jgi@fiu.edu.

TABLE OF CONTENTS



EXECUTIVE SUMMARY

Over the past decade, Russian-based companies have provided sophisticated surveillance technology to several Latin American countries. These technologies are critical to the survival of the repressive regimes in Venezuela, Nicaragua, and Cuba, and possibly criminal nonstate actors that weaken democracy and threaten U.S. national security.

The transfer of surveillance technologies and other cyber activities, often run by Russian intelligence officials directly tied to Russia's state cyber structures, goes beyond traditionally understood gray zone activities. While these technologies empower the region's most repressive regimes and criminal threat networks, they also give Russia access to key military, law enforcement, and financial data in multiple countries in the Western Hemisphere.

Multiple platforms in Latin America now operate the most sophisticated of these malicious cyber activities under direct Russian state security supervision. These include a high-security military complex in Cerro Mokorón, Nicaragua; the Maduro regime fortress of Fuerte Tiuna, Venezuela; and corporate spaces in Chile. Transnational criminal organizations are also acquiring Russian surveillance technology, some of which are advertised on Russian state websites.

The heart of the systems provided by the Russians for surveillance activities is the System for Operative-Investigative Activities (SORM-3), capable of gathering information and data from all communications media and creating mobile block points to immediately intercept and record the operator's digital traffic and monitor credit card transactions.

Our research identified three primary ways Russia is expanding its digital presence in the hemisphere: (1) direct placement and control of technology on the ground, (2) through state and parastate groups that present themselves as private partnerships affiliated with Russian cyber defense, and (3) through companies less visibly linked to the Russian state but led by longtime senior intelligence operatives from the days of the Soviet Union and the fall of the Berlin Wall.

The first step in countering Russian cyber networks and outreach in Latin America is to make understanding the scope and methodologies of the adversary a higher policy priority. With a baseline understanding, the United States, through its embassies and selected outreach, should develop an outreach and education program to blunt the progress of Russia's cyber actors.

The lack of understanding of Russian strategic interests in this sphere is compounded by the lack of Russian-language speakers. An important step to counter Russian strategic advances would be to have a small group of Russian-language experts with cyber experience available to allied governments seeking to address these vulnerabilities within their administrations.

Finally, the U.S. government should help form public-private partnerships with groups of trusted U.S. cyber experts with knowledge of Russia who could help the business communities and local IT providers understand and address the strategic challenges raised by Russia's actions.

INTRODUCTION

Over the past decade, Russia waged a successful but little-noticed irregular warfare campaign to provide its Latin American allies with sophisticated Russian state-designed and controlled surveillance technology. These surveillance technologies are critical to the survival of the repressive regimes of Nicolás Maduro in Venezuela, Daniel Ortega in Nicaragua, Miguel Díaz-Canel in Cuba, and possibly criminal nonstate actors that weaken democracy and threaten U.S. national security.

Gen. Laura Richardson, commander of U.S. Southern Command (SOUTHCOM), acknowledged in her 2024 Posture Statement that:

> Russia employs a host of malign activities within the gray zone, including malicious cyber activities, disinformation campaigns, and periodic high-level visits and military force projection. Moscow and affiliated cybercriminal groups seek to destabilize democracies by targeting public institutions and sensitive government frameworks, disrupting critical infrastructure, and stealing information.[1]

The transfer of surveillance technologies and other cyber activities, often run by Russian intelligence officials directly tied to Russia's state cryptology and surveillance structures, goes beyond traditionally understood gray zone activities. These activities directly aid authoritarian regimes to further repress their people. While these technologies significantly empower the region's most repressive regimes and criminal threat networks, they also give Russia access to key military, law enforcement, and financial data in multiple countries in the Western Hemisphere.

Many of the Russian groups involved in Latin America today were active in the region during the Soviet and early post-Soviet eras. One of the main groups, the National Committee for Economic Cooperation with Latin American Countries (CN CEPLA), was founded in 1998 in Chile and led for decades by a former KGB general. Today, Russian surveillance and cyber espionage activities are broader than traditional malicious cyber activities[2] and Russia's massive information operations in Latin America, although the various spheres overlap.[3]

The surveillance and electronic interception technologies provided by Russia in Latin America are among the most sophisticated in the world. Russia provides these same systems to other repressive regimes in Belarus, Iran, Kazakhstan, Tajikistan, Turkmenistan, and Uzbekistan.[4]

The expansion of Russia's cyber activities in Latin America and around the globe falls within Moscow's foundational national defense framework, the Primakov Doctrine, articulated in 1996 by the one-time prime minister, foreign minister, and head of the Russian Foreign Intelligence Service, Yevgeny Primakov. It remains in place under Putin.[5]

This doctrine includes among its five pillars that Russia must be an indispensable actor on the world stage, a unipolar world dominated by the United States is unacceptable, and Russia must have the capabilities to simultaneously wage war across multiple domains, including cyber and technology, to protect Russian strategic interests.[6] China and Iran also share a multipolar world and great power competition vision within their national interests but we found no evidence of technological cooperation among them in these cyber activities.

In 2013, General Valery Gerasimov, chief of Russia's general staff and now commander of Russia's operations in Ukraine, adapted the Primakov doctrine for modern hybrid warfare as Russia prepared for its annexation of Crimea in 2014, defining the war domains to include military, diplomatic, economic, information, and technological.

Gerasimov argued that permanent conflict with the West is inevitable and necessitates a hybrid or nonlinear response. This includes a changing combination of multiple, largely offensive forms of fighting, including technological warfare, cyber warfare, information operations, and trade, arguing that "new challenges require rethinking the forms and modes of warfare" that are highly adaptable to the circumstances.[7]

This study examines how the expansion of cyber surveillance technology is being conducted through case studies of the three main methodologies observed. The research included a review of open-source literature in Russian, Spanish, and English; a review of Russian government and technology websites by a native Russian language speaker, and field research conducting 14 interviews during field research trips in Argentina, Uruguay, Paraguay, and Chile from June 2022 to June 2024.

While our research confirmed the use of the most invasive surveillance systems in Venezuela, Cuba, and Nicaragua, we focus on Nicaragua in this study, as it is the least explored in existing research and the U.S. policy community. We also remain concerned about Russian malign influence operations in other countries across Latin America that are not part of this study.

Given the senior level of officials within the Russian state that are leading the effort, and the direct ties of the cyber corporations to Russian state intelligence services, the expansion is properly viewed as a significant Russian strategic line of effort in the hemisphere.

Russia's willingness to provide this technology at low cost or as part of aid packages to friendly criminalized regimes has been key to the ability of Maduro, Ortega, Diaz-Canel, and other authoritarian regimes around the world to quickly identify, locate, and neutralize opponents or suspected opponents, and maintain their iron grip on power as their public support shrinks and these leaders become more repressive autocrats.

RUSSIA'S IMPACT IN LATIN AMERICA

In Latin America, the rulers of the deeply criminalized states allied with Russia are also strategically allied with transnational criminal organizations, including the Sinaloa Cartel, the *Cartel Jalisco Nueva Generación*, Colombian-based cartels, the Italian 'Ndrangheta, and others.[8] These regimes not only stifle democracy in their countries but form part of an alliance with Iran, North Korea, and China that directly challenges strategic U.S. interests in the hemisphere and globally.[9]

In recent years, Russia expanded its state-sanctioned operations by successfully partnering with local technology companies to acquire direct access to strategic information nodes of multiple countries in Latin America.

Multiple platforms in Latin America now operate the most sophisticated of these malicious cyber activities under direct Russian state security supervision. They include a high-security military complex in Cerro Mokorón on the outskirts of Managua, Nicaragua[10] to the Maduro regime fortress of Fuerte Tiuna in Caracas, Venezuela to the genteel corporate spaces in Santiago, Chile.

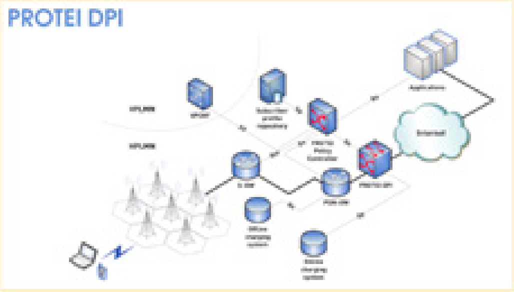
There are credible reports of Latin American criminal groups—including transnational criminal organizations based in Paraguay and Honduras, as well as the main Mexican cartels—acquiring Russian surveillance technology, some of which is advertised on Russian state websites.[11]

In Chile, the Russian state affiliated *Comité Nacional para la Cooperación Económica con los Países Latinoamericanos* (CN CEPLA in Spanish, translated in English as "Russian National Committee for the Promotion of Economic Trade with Countries of Latin America,") is among the most active. [For consistency and brevity, the Spanish acronym CN CEPLA is used throughout this paper when discussing this group.]

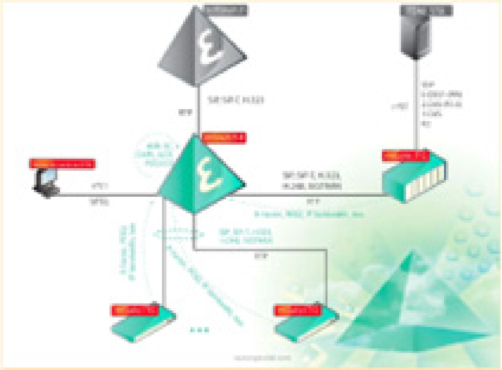
One of CN CEPLA's important roles is to facilitate the expansion of Russia's premier cybersecurity firm, PROTEI ST Cybersecurity and Surveillance Company, a subsidiary of NTC PROTEI, which has contracted with Russian military and intelligence agencies to provide them with cybersecurity and surveillance websites. PROTEI I is the largest but not the sole provider of technology using the Russian government-mandated state "back door" to monitor most communications on Russian-controlled systems.[12] A sample of the PROETI products offered for sale on the CN CEPLA site can be seen below.[13]

Examples of the dozens of types of PROTEI technology for sale on the CN CEPLA website. Though often opaque in their descriptions, most products have clear surveillance or monitoring capacities.

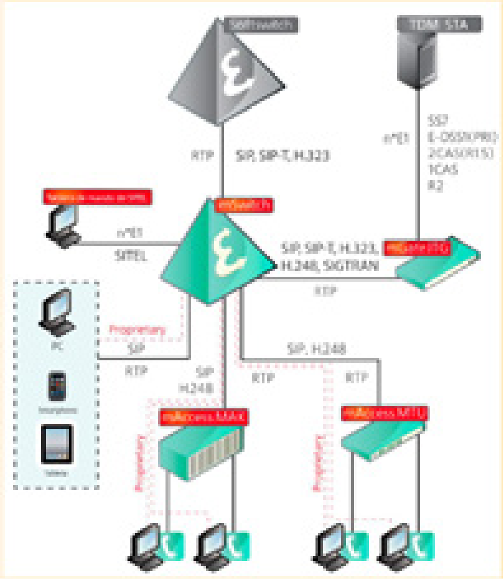
- PROTEI DPI: Advertised as technology that "controls service policy through data flows," allowing data to by analyzed "through distinct or static platforms."

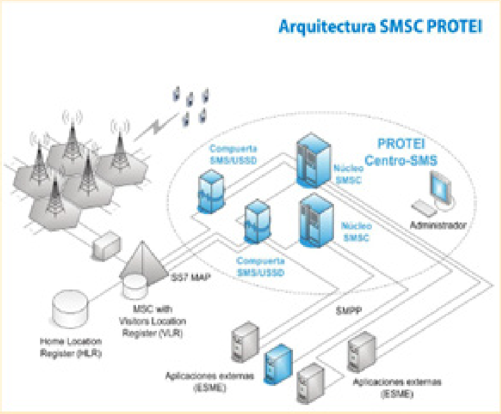


- PROTEI SE imSwitch5: Advertised as an "affordable solution" scalable for use in offices to citywide networks. It offers access to "Triple Play" services, and specifically lists "legal [electronic] interception" among its services.



- PROTEI imSwitch Complex for Zonal Communications: Advertised as a "potent system for collection and analysis" with "use of certificates of interception" and "active monitoring of equipment, detailed collection of data about calls, and "detailed tracing of calls."




Arquitectura SMSC PROTEI
Compuerta SMS/USSD
PROTEI Centro-SMS
Núcleo SMSC
Núcleo SMSC
Administrador
Compuerta SMS/USSD
SS7 MAP
SMPP
MSC with Visitors Location Register (VLR)
Home Location Register (HLR)
Aplicaciones externas (ESME)
Aplicaciones externas (ESME)

THE SORM SYSTEMS: PREFERRED BY DICTATORS

The heart of Russia's surveillance systems is the System for Operative-Investigative Activities (SORM), which began as a Soviet KGB program in 1986 to intercept telephone landlines. It is now capable of surveilling specific individuals across digital, internet, and telephone communications. Russia produces SORM-1, SORM-2, and SORM-3, each with added layers of sophistication.

The most advanced program, SORM-3, gathers information from all communications media and creates mobile block points to immediately intercept and record the operator's digital traffic and monitor credit card transactions.[14] The Federal Security Service of the Russian Federation (FSB is its English acronym) is the principal agency in charge of communications surveillance. Seven other Russian security agencies can access SORM if needed.[15]

One study of Russian surveillance technology found that

> By 2015, an updated version—SORM-3—would encompass all communications. Under Russian law, internet service providers and telecom providers are required to install SORM equipment, providing the Russian FSB with access to all data shared online without the companies' knowledge or control of which data are being shared and with whom. SORM works by basically copying all data flows on internet and telecom networks—sending one copy to the government and the other to the intended destination. SORM is the FSB's "backdoor" to Russia's internet.[16]

In February 2023, the U.S. Department of State sanctioned multiple Russian companies and individuals for their production or use of SORM, which "enables Russia's domestic and foreign intelligence collection, monitoring, and suppression of dissent." Among the entities sanctioned was Company Citadel, which has widespread operations in Latin America and is associated with several of the groups discussed below.[17]

The risk of SORM interception is significant enough that in June 2024, the U.S. Department of State warned U.S. citizens traveling to Russia that SORM "legally permits authorities to monitor and record all data that traverses Russia's networks. Telephone and electronic communications are subject to surveillance at any time and without advisory, which may compromise sensitive personal or business-related information."[18]

In August 2024, the Nicaraguan digital investigative medium *Confidencial* found that in the Mokorón surveillance center just outside of Managua, Russian intelligence had added the SORM-3 software "to spy and listen to the communications of their 'targets,' as well as the so-called "internal enemies" of Daniel Ortega's dictatorship," according to *Confidencial.*[19]

To further its strategic objectives of penetrating cyber infrastructure in the region, in September 2021, the Kremlin formally approved the creation of an institute of "digital ambassadors" or digital attachés, operating out of Russian embassies to support Russian IT companies and encourage foreign IT companies to transition to Russian technology and jurisdiction.

A Russian online recruitment site for the attachés under the direction of the state-run Russian Foundation for the Development of Information Technologies noted that "the main task of the 'digital attachés' is to increase the volume of exports of Russian goods and services in the field of IT (software and electronic products)."[20]

The attaches are now officially stationed in 16 countries, including Argentina, Brazil, Cuba, and Peru, in Latin America. The Russian Ministry for Digital Development oversees the selection of personnel for the postings.[21]

The attachés were visible when several attended an October 2022 technology exposition in Santiago, Chile, where they identified themselves and actively pursued Chilean and regional defense officials to sell a new Russian technology from Dialog LLC.[22] The product is actively offered across Latin America, including sales at high-profile technology expositions.

Figure 1: Dialog booth in Santiago, Chile, October 2022 (IBI Consultants)

The FSB intelligence service authorized Dialog and is the developer of the Dialog secure messaging app. The company was founded in 2016 and has belonged to the Sberbank Group since 2018.[23] Sberbank was sanctioned by the U.S. Department of the Treasury following the 2022 invasion of Ukraine, saying the bank was "uniquely important to the Russian economy" and majority-owned by the government of Russia.[24] The secure, encrypted app allows organizations to manage internal communications as well as integrate or mirror communications from other apps. Dialog also provides its clients with the capacity to create bots capable of carrying out routine operations or chats with customers.[25]

THE PRIMARY PENETRATION METHODOLOGIES

Our research identified three primary ways Russia is expanding its digital presence in the hemisphere. Each show how deeply enmeshed state, para-state and "private" entities are with the Russian state cybersecurity and information technology:

- The first is through direct placement and control of technology on the ground, as in Cerro Mokorón in Nicaragua and Fuerte Tiuna in Venezuela. In these spaces, the Russians not only have autonomy of action, control of locations without host government oversight, and multiple interests of their own but also provide services to the host country. These are under the rubric of official state-to-state relations.
- The second is through state and para-state groups such as the SearchInform consortium that form part of multiple Russian state entities and officially present their efforts as private partnerships affiliated with Russian cyber defense and warfare intelligence centers.
- The third is through less visibly state-linked groups like the CN CEPLA family of organizations, which are state-sponsored but not officially part of the Russian state cyber architecture. This group is perhaps the most influential, and its leadership comes from the ranks of senior intelligence officials of the Soviet Union at the end of the Cold War and the early days of the Russian state after the fall of the Berlin Wall in 1989.

Nicaragua, the State-to-State Model

Our research shows Nicaragua is the most visible center of Russian surveillance under the Ortega regime's unconditional support for Putin and long-standing historical ties to the former Soviet Union. This trust and Ortega's increasingly repressive and isolated regime form the basis for the ties that are the focus of this section.

While Venezuela and Cuba also follow the state-to-state model, Nicaragua remains the least studied Russian partner in the region. Numerous published accounts report a Russian military presence co-located in Venezuelan military installations. One former head of Venezuelan intelligence detailed the presence in the military headquarters of Fuerte Tiuna as being for "communications and intelligence exploration."[26]

As noted, Cerro Mokorón in Nicaragua is reportedly the hub of information processing for eight identified Russian electronic surveillance and espionage stations operating in that country that are operationally accessible to Russians or under direct Russian control. The Ortega regime's Directorate of Military Intelligence and Counterintelligence, known as Unit 502, operates the Mokorón base, and only Russian officials are allowed to operate the system and access the information gathered.[27]

This hub, which compiled surveillance and electronic data from eight Nicaraguan military listening centers to which Russia has unfettered access, began operations in 2017 and has since expanded. This capability has been key in allowing the Ortega regime to identify and eliminate suspected regime opponents while constantly attempting to penetrate U.S. and NATO classified communications.[28]

The then-newly provided SORM system was reportedly key to the Ortega regime's ability to quickly identify student protest leaders during civil unrest in 2018. It was the strongest challenge to date to the Ortega regime, which responded by killing more than 350 protesters,[29] often identified via Russian technology used to identify key WhatsApp information nodes.[30]

In addition to the Mokorón center, multiple concurrent cyber developments seem to have the shared goal of granting Russian intelligence services greater access to Latin American data through the Ortega regime. The headquarters of the Russian state geolocation tracking GLONASS (Global Navigation Satellite System), is located near the Nejapa Lagoon and is banned in the United States and much of Europe for its dual use in intelligence gathering.[31] According to reporting from Nicaragua, Brazil, and Chile, the GLONASS installations are far more sophisticated than required for similar geolocation systems, raising the possibility that they could be used for other purposes.[32]

Another opaque espionage center is the Russian Ministry of Interior "training center" in Managua, which is under the command of Russian Police Lt. Col. Oleg Surov. The center was officially opened in 2014 as a regional counternarcotics training center and inaugurated again on October 16, 2017, as a training facility for law enforcement officials.[33] The center's first course was given in November 2017, and several other courses have been held since.[34]

As of June 2019, at least 270 security officers were reportedly trained in the center, suggesting there were more courses than those publicly announced.[35] In February 2020, the center held two courses on drug trafficking and money laundering for 40 Nicaraguan federal police officers and one unnamed Brazilian individual.[36]

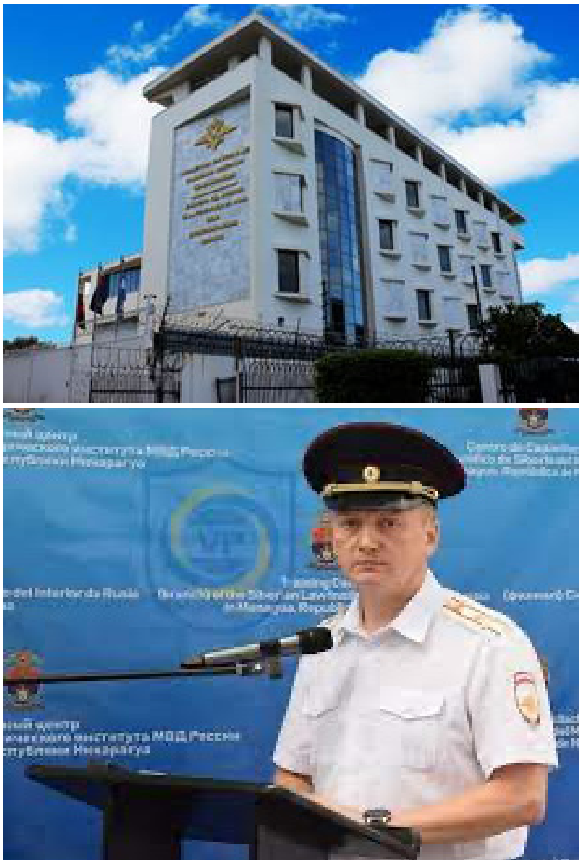


Figure 2: Russian Ministry of Interior building in downtown Managua (Top, IBI Consultants) and Lt. Col. Oleg Surov (Bottom,Nicaraguan National Police)

What is striking about the center is that the building is the official property of the Russian Ministry of the Interior with special privileges to operate in the country, a fact stated on a brass plaque on the side of the building in Russian and Spanish, identifying the building as "belonging to" the Russian state; the center is listed as an extension of the Russian Embassy. Russian officers control facility access.[37]

Author sources with direct knowledge of events said that when protests against the Ortega regime broke out in 2018, Surov was tasked with providing special training classes to a select group of Nicaraguan police to eliminate the protest movement and its leaders.

The course was titled "Modern Means and Methods to Combat Extremism and Terrorism." It provided digital and electronic surveillance techniques that enhanced the Ortega regime's capacity to repress and control civil society. In 2021, the Russian Ministry of Internal Affairs taught a follow-up course for 20 officers titled "The Fight Against Computer Information."

In September 2023, Ortega conferred a special military medal on Russian Col. Gen. Oleg Plokhoi and, for the first time, publicly acknowledged the training center was used to "better fight the *golpistas*" his regime faces and said the Medal of Honor for Police Friendship was "recognition of the invaluable support and cooperation provided to our National Police."[38]

Figure 3: Nicaraguan President Daniel Ortega presenting medal to Russian Police Col. Gen. Oleg Plokhoi in September 2023. (Confidencial)

STATE AND PARA-STATE BUSINESS: SEARCHINFORM

The Russian state built a multilayered symbiotic relationship between the state and loyal semiautonomous companies that operate both for profit and the expansion of Russian intelligence and cyber penetration within the hemisphere.

While portraying themselves to be private enterprises, these companies play a key role in building Russia's cyber platforms and security structure at home and abroad and are tied directly to Russian state surveillance architecture.

Among the primary Russian cyber actors in Latin America is the state-sponsored company SearchInform LLC, with headquarters in Buenos Aires, Argentina. SearchInform operates under the umbrella of Russoft, the Russian government's interdisciplinary and ministerial committees that facilitate relations with different parts of the Russian state and provide regulatory guidance.

SearchInform, one of Russia's premiere cyber companies, has access to sell and use SORM surveillance technology licensed out by the FSB.[39] SearchInform's Chairman, Lev Matveev, is a key player and leader in multiple Russian state technology consortiums.

Due to the nature of the services provided and the clientele in Russia and internationally, the company has a variety of licenses and certifications posted on its website in Russian, including the ones associated with "confidential information provider" and "technical protection of information," along with "certification and protection of the state secrets" and "development and production of means of protecting confidential information," which indicates the company's legal and procedural compliance and cooperation with the Russian law enforcement and government.[40]

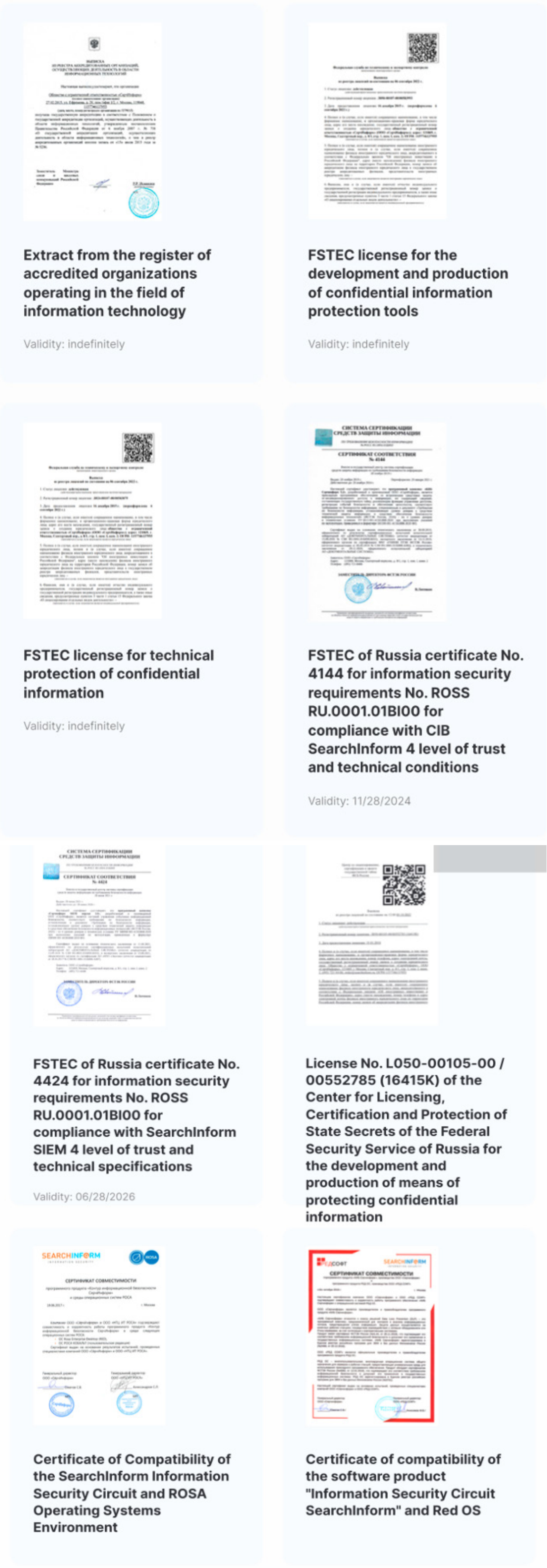
According to SearchInform's website,[41] the group began operations in Latin America in 2017, forming alliances with local IT providers with existing government contracts to provide "cyber security services."

Fieldwork in Paraguay and Argentina found that SearchInform had direct access to police databases, the ministries of finance and justice, and other strategic information by accessing dozens of sensitive government cybersecurity contracts held by three local partners (one in Paraguay, two in Argentina).

One confidential source with direct knowledge of SearchInform's activities in the region said having access to government IT contracts was a prerequisite for partnering with SearchInform and, having used the SearchInform platform for criminal investigations, said the system was designed to extract information rather than enhance information sharing among government entities.[42]

SearchInform now lists on its website subsidiaries in Argentina (3); Bolivia, Chile and Colombia (2); Brazil (5); as well as one each in Paraguay, Costa Rica, Ecuador, Mexico, Peru, and Uruguay. The Russian company likely has significant access to government cyber infrastructure in each country where it operates.

To expand its business, the company has held a series of SearchInform Road Shows since 2018, in which its leaders host a series of events to demonstrate and advertise its information security products to potential clients across Latin America and build relationships with tech companies.



Extract from the register of accredited organizations operating in the field of information technology

Validity: indefinitely

FSTEC license for the development and production of confidential information protection tools

Validity: indefinitely

FSTEC license for technical protection of confidential information

Validity: indefinitely

FSTEC of Russia certificate No. 4144 for information security requirements No. ROSS RU.0001.01BI00 for compliance with CIB SearchInform 4 level of trust and technical conditions

Validity: 11/28/2024

FSTEC of Russia certificate No. 4424 for information security requirements No. ROSS RU.0001.01BI00 for compliance with SearchInform SIEM 4 level of trust and technical specifications

Validity: 06/28/2026

License No. L050-00105-00 / 00552785 (16415K) of the Center for Licensing, Certification and Protection of State Secrets of the Federal Security Service of Russia for the development and production of means of protecting confidential information

Certificate of Compatibility of the SearchInform Information Security Circuit and ROSA Operating Systems Environment

Certificate of compatibility of the software product "Information Security Circuit SearchInform" and Red OS

Figure 4: Certificates and translations provided by a native Russian speaker and security analyst.

SEARCHINFORM IN THE RUSSIAN CYBER INTELLIGENCE ECOSYSTEM

To fully appreciate the importance of SearchInform's presence in the region, it is necessary to understand how it fits into the overall complex and multi-layered Russian state IT structure.

Founded in 2009 as a successor to the SoftInform technology company, SearchInform began training work for the National Research Technology University in Russia[43] and, in 2015, was granted prized real estate for its offices in the Skolkovo Innovation Center (a Russian Silicon Valley complex for modern science and technology).[44]

SearchInform CEO Lev Matveev is a member of the board of Russoft, which is composed of 247 IT companies and represents the IT industry. Russoft reports to the prime minister of the Russian Federation's Ministry of Digital Development and Mass Media. Matveez is also a partner or board member of other major Russian state organizations involved in promoting Russian IT services in Latin America.

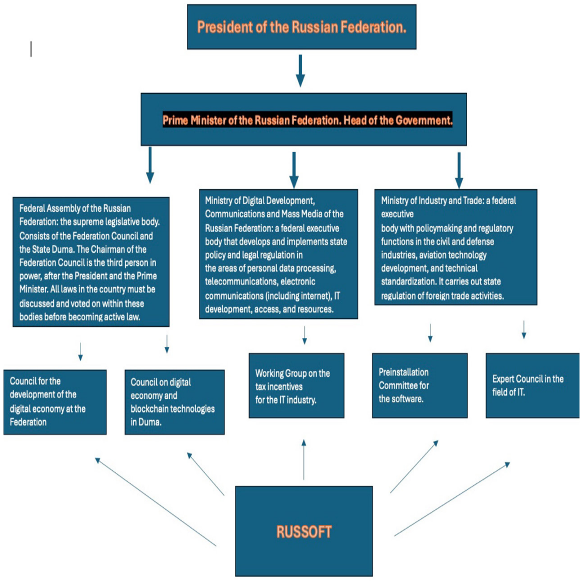

President of the Russian Federation.
Prime Minister of the Russian Federation. Head of the Government.
Federal Assembly of the Russian Federation: the supreme legislative body. Consists of the Federation Council and the State Duma. The Chairman of the Federation Council is the third person in power, after the President and the Prime Minister. All laws in the country must be discussed and voted on within these bodies before becoming active law.
Ministry of Digital Development, Communications and Mass Media of the Russian Federation: a federal executive body that develops and implements state policy and legal regulation in the areas of personal data processing, telecommunications, electronic communications (including internet), IT development, access, and resources.
Ministry of Industry and Trade: a federal executive body with policymaking and regulatory functions in the civil and defense industries, aviation technology development, and technical standardization. It carries out state regulation of foreign trade activities.
Council for the development of the digital economy at the Federation
Council on digital economy and blockchain technologies in Duma.
Working Group on the tax incentives for the IT industry.
Preinstallation Committee for the software.
Expert Council in the field of IT.
RUSSOFT

Figure 5: Russoft, the umbrella organization under which SearchInform operates in the Russian cyber hierarchy.

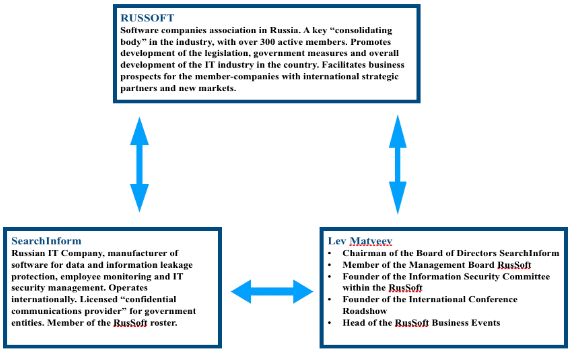

RUSSOFT
Software companies association in Russia. A key "consolidating body" in the industry, with over 300 active members. Promotes development of the legislation, government measures and overall development of the IT industry in the country. Facilitates business prospects for the member-companies with international strategic partners and new markets.
SearchInform
Russian IT Company, manufacturer of software for data and information leakage protection, employee monitoring and IT security management. Operates internationally. Licensed "confidential communications provider" for government entities. Member of the RusSoft roster.
Lev Matveev
Chairman of the Board of Directors SearchInform
Member of the Management Board RusSoft
Founder of the Information Security Committee within the RusSoft
Founder of the International Conference Roadshow
Head of the RusSoft Business Events

Figure 6: Relationship among Russoft, SearchInform, and Director Matveev

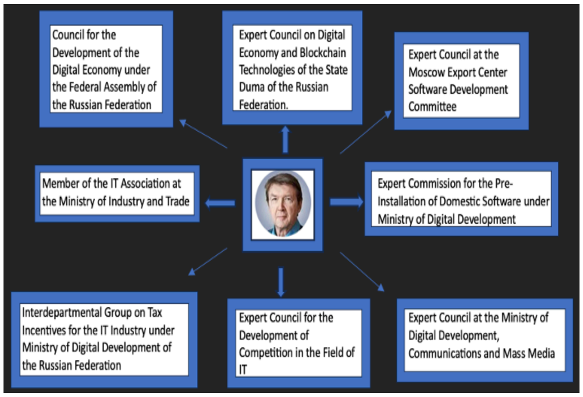

Council for the Development of the Digital Economy under the Federal Assembly of the Russian Federation
Expert Council on Digital Economy and Blockchain Technologies of the State Duma of the Russian Federation.
Expert Council at the Moscow Export Center Software Development Committee
Member of the IT Association at the Ministry of Industry and Trade
Expert Commission for the Pre-Installation of Domestic Software under Ministry of Digital Development
Interdepartmental Group on Tax Incentives for the IT Industry under Ministry of Digital Development of the Russian Federation
Expert Council for the Development of Competition in the Field of IT
Expert Council at the Ministry of Digital Development, Communications and Mass Media

Figure 7: The multiple roles of Matveev in the Russian cybersecurity architecture

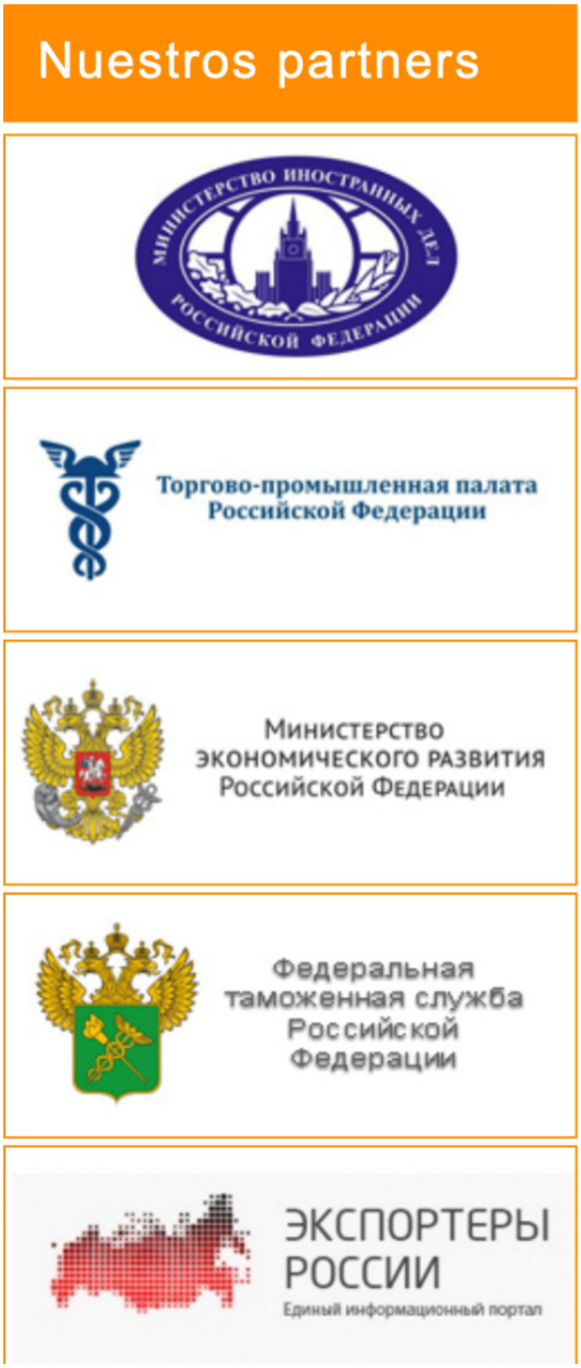
Cementing its leadership role in Russian cybersecurity exports, SearchInform, along with several other Russian firms, including SORM provider MFI Soft, formed a consortium of "information security" companies known as the Group Citadel. Its main specialization is providing SORM programs to Latin American customers.[45] Citadel was sanctioned by the U.S. Department of State in 2023.

THE CN CEPLA CONSORTIUM

Since 1998, the CN CEPLA group, formally established by the office of the Russian presidency and operating under the direction of a former KGB general, has been one of Russia's most active networks in Latin America, offering an array of surveillance and intelligence equipment through online sales, technology fairs, and state-to-state sales or donations. The following information was obtained through open-source research in conjunction with C4ADS, a nonprofit organization specializing in data analysis and retrieval, with Russian language capabilities.

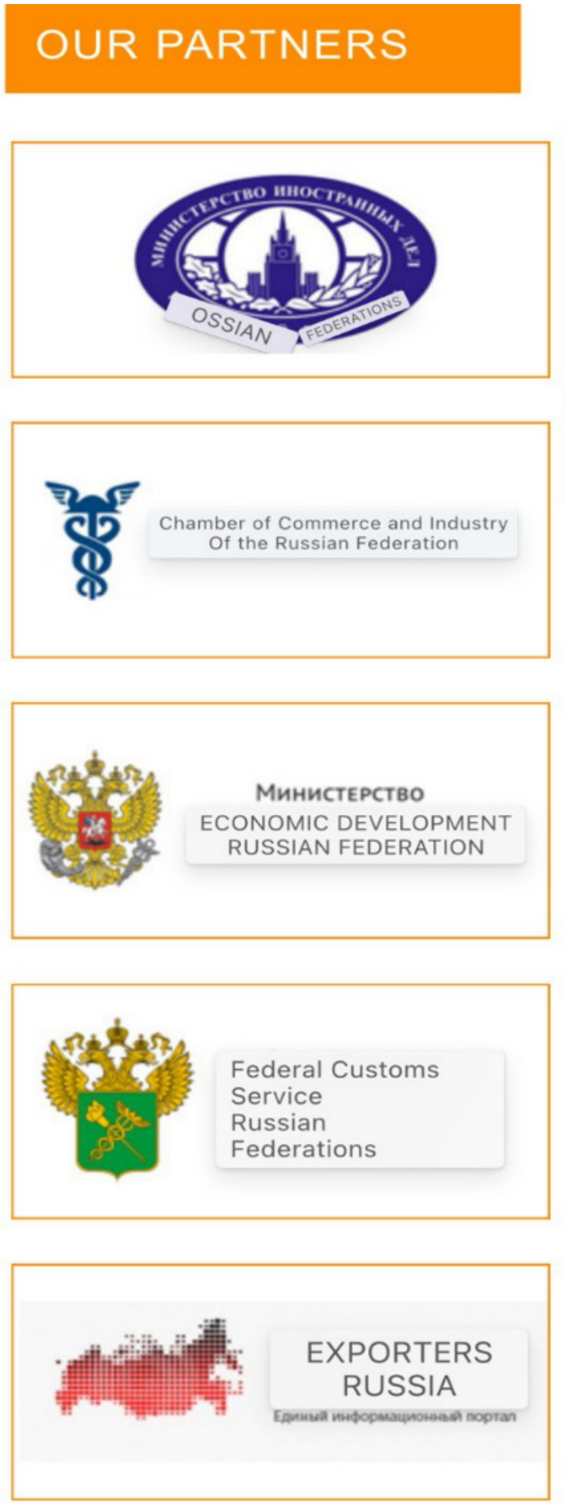
Headquartered in Santiago, Chile, the para-state enterprise has numerous former senior intelligence officials in CN CEPLA leadership positions. Many of these officials began their careers in the state cryptology enterprises before and during the years following the collapse of the Soviet Union.

The cluster of organizations, which calls itself a noncommercial partnership, is among the most public of a group of Russian enterprises in the consortium with overlapping directorships and state sponsors. The group and the leadership of that organization within the group are also prominent public conduits for articulating Russian intelligence and foreign policy in Latin America.[46] The network leadership regularly hosts visiting Latin American presidents and senior leaders in Moscow and, prior to the invasion of Ukraine, hosted frequent conferences in Latin America.



Nuestros partners

МИНИСТЕРСТВО ИНОСТРАННЫХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ
Торгово-промышленная палата Российской Федерации
Министерство экономического развития Российской Федерации
Федеральная таможенная служба Российской Федерации
ЭКСПОРТЕРЫ РОССИИ
Единый информационный портал



OUR PARTNERS

OSSIAN FEDERATIONS

Chamber of Commerce and Industry
Of the Russian Federation

Министерство
ECONOMIC DEVELOPMENT
RUSSIAN FEDERATION

Federal Customs
Service
Russian
Federations

EXPORTERS
RUSSIA
Единый информационный портал

Figure 8: Partial list of CN CEPLA Russian state partners listed on its website (left) and translations (right).47

The CN CEPLA leadership also serves as the directors of multiple other Russian state cyber warfare entities. Because of the leaders' seniority and documents authorizing the entity to act on behalf of Russian intelligence services and the Russian military, this network's primary purpose is likely connected to its roots in electronic intelligence, cryptology, and surveillance. Its most visible work includes hosting conferences and training programs for Latin American businesspeople to attend in Russia.[48]

THE KEY ROLE OF KGB GENERAL STAROVOITOV

The importance of the CN CEPLA is seen in its longtime leader and its formal partnerships with Russian state entities, including the Ministries of Foreign Affairs and Economic Development, the Institute of Latin America of the Russian Academy of Sciences, and the state cybersecurity structures.[49]

While the consortium has multiple leaders tied to former Soviet and Russian state cyber operations, the role of the longtime leader offers the clearest example of the overlap of Russian state interests in cyber technology, business, and diplomacy.

Alexandr (cq) Starovoitov, a former general in the Soviet KGB, founded CN CEPLA in 1998 and led the company until his death in 2021. His publicly identified specialties included electronic communications technology and cryptography. Starovoitov, who was also a colonel in the Soviet military, was a pioneering figure in Russia's cyber technology field. When he died in May 2021, he was buried as a "hero of the Russian State."

Given his multiple roles over several decades, Starovoitov was at the center of a nexus of Russian state intelligence and business worlds. The companies he led are some of the most important cyber and defense initiatives of the Russian government.

In addition to serving as president of CN CEPLA, Starovoitov was listed as director general of the International Center of Informatics and Electronics (Inter EVM is the Russian acronym). The center posted certificates from the FSB and Russian military authorizing it to use "information constituting state secrets, advanced cryptographic information systems" and "activities in the field of information tools."[50]

The Science and Technology and Information Consortium is part of the Inter EVM Center. Its responsibility is to "jointly solve the problems of the creation and development of advanced information technology, computer hardware and microelectronics." The center is listed as a member of CN CEPLA on the group's website.

Starovoitov was also director of the Center for Informational Technology Systems of the Executive Branch Organs (TsITIS is the Russian acronym), a secretive government agency specializing in signals intelligence and code breaking. In 2014, Putin charged the company with the core strategic task of building a multibillion-dollar integrated, secure communications network for the Russian military. The network is to help detect and deter cyberattacks.[51]

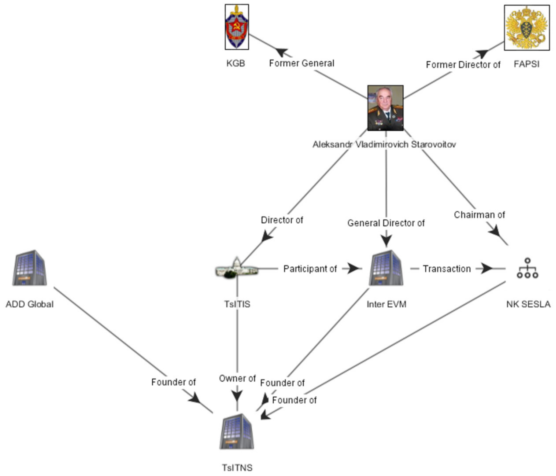


Figure 9: Figure developed by C4ADS based on Russian language research.

According to his biography on the CN CEPLA site and his official obituary, Starovoitov also served as director of the Cryptology Academy of the Russian Federation and served on Russia's Security Council from 1998-1999.

In 1986, Starovoitov was named the vice director technical supply for the KGB's Directorate of Government Communications. That same year, he received the rank of major general in the KGB. In 1991, as the Soviet Union collapsed, he was named director of the Federal Agency of Government Communications and Information of the Russian Federation (FAPSI), roughly the equivalent of the NSA, a post he held for eight years.

During that time, he was responsible for his nation's "signals intelligence, cryptography, cryptology, and secret government communications." FAPSI was dissolved in 2003 and folded into the FSB.[52]

Starovoitov's obituary, published in numerous Russian media outlets and on the CN CEPLA website, cited him for his work in "developing cooperation with Latin American countries, especially in the promotion of sophisticated Russian technologies in the region."[53]

Starovoitov's official successor is Tatiana Mashkova, his deputy since 2009, who was named CN CEPLA director and has become a spokesperson for Russia on Latin American issues. Her biography on the CN CEPLA website highlights her multiple jobs across the Russian state bureaucracy.[54] She primarily operates out of Moscow but travels in Latin America.

An indicator of her importance came in February 2022, when she met separately with former Argentine President Alberto Fernández and then-Brazilian President Jair Bolsonaro during their trips to Moscow on the eve of the invasion of Ukraine. The two presidents' meetings with Mashkova at the CN CEPLA Moscow headquarters were the only meetings they attended outside of their summits with Putin that were publicly reported on state media.[55]

Since then, Mashkova has hosted dozens of business seminars across the region to tout Russian technologies and equipment, sponsored scores of tours by Latin American business leaders to Russia, and made trips to Panama and Cuba. The organization is quite active and has 91 members.[56] CN CEPLA also serves as a mouthpiece for pro-Russian propaganda. Since the invasion of Ukraine, its website has been a repository of dozens of pro-Russia articles and disinformation, relating to Ukraine, as well as alliances with Cuba and Venezuela.

Figure 10: Tatiana Mashkova at a meeting in Havana, Cuba, 2023 (Sputnik Mundo)

OTHER ACTORS

While Starovoitov had the most illustrious career within Soviet and Russian intelligence structures, several other leaders of the network also had long ties to Russian state structures. The most notable, in addition to Mashkova, is Vyacheslav Vasyagin, a director of Inter EVM along with Starovoitov and key liaison with the Ortega regime in Nicaragua.

Like Starovoitov, Vasyagin was a former Soviet military officer who was in various "divisions of external economic links of the Committee of People's Control" of the USSR. After the fall of the Berlin Wall, he served in multiple intelligence services, including as the deputy director of Russia's notorious tax police, the FSPN, from 2000 to 2003.[57]

During that time, the FSPN was part of the Russian state intelligence structure used to monitor the financial flows of those deemed possible enemies of the state, including the newly emerging oligarchs and former dissidents. The FSPN was then incorporated into the FSB, the civilian intelligence structure that still operates. According to his now-defunct Facebook page, he is a member of Orthodox Russia, an ultra-conservative group of the Russian Orthodox Church close to the Kremlin.[58]

Figure 11: Vasyagin meets in 2014 with Luis Molina Cuadra, Nicaraguan vice minister for foreign affairs (Sputnik Mundo).

Vasyagin has publicly led numerous delegations to Nicaragua, El Salvador, and Guatemala and often acts as a translator for visiting Russian delegations. In 2014, he presented a medal in Managua, Nicaragua, on behalf of the Russian state to Luis Molina Cuadra, who served for years as Ortega's ambassador to Moscow. Vasyagin, according to the Inter EVM website, is also an "active state advisor of the first class" to the Russian Federation, the highest rank a person can obtain in the Russian civil service and one bestowed by the president.[59]

RECOMMENDATIONS

The first step in countering Russian cyber networks and outreach in Latin America is to understand the scope and methodologies of the adversary, which is a significant knowledge gap across the U.S. government.

Equally important, the U.S. national security community must make addressing the malign influence operations by Russia and other authoritarian regimes advancing a multipolar agenda to weaken democracies in Latin America and elsewhere a higher defense, law enforcement, and foreign policy priority.

Russia's recent cyber activities in Latin America are not a high strategic priority for the U.S. Department of State, SOUTHCOM, or the intelligence community. Yet, given the high level of Russian operatives involved in the efforts, cyberspace is clearly a strategic priority for Russia in the hemisphere and a primary tool used by strategic adversaries to retain power, undermine democratic norms and the rule of law, and attack U.S. strategic interests.

With a baseline understanding of the Russian lines of effort and entry points, the United States, through its embassies and selected outreach to trusted media, should develop an outreach and education program to blunt the progress of Russia's cyber actors and weaken, if not break, ties of local subsidiaries with their Russian partners.

For example, none of the government sources interviewed by the author over the past year were aware of U.S. sanctions against companies providing SORM technology, including those linked to SearchInform. Nor were the government officials aware that local cybersecurity companies under contract with their governments had ties to Russian companies, even though the Russian companies posted information on the relationships on their websites.

The lack of understanding of Russian strategic interests in this sphere is further compounded by the lack of Russian-language speakers, a severe handicap given how much of the information contained in this report and available overall is only available in Russian and on Russian websites.

An important step to counter Russian strategic advances would be to have a small group of Russian-language experts with cyber experience available to allied governments seeking to address these vulnerabilities within their administrations.

Finally, at a relatively low cost, the U.S. government could help form public-private partnerships with groups of trusted U.S. cyber experts with knowledge of Russia to help the business communities and local IT providers understand and address the strategic challenges raised by Russia's actions.

CONCLUSIONS

The Russian state and para-state cyber penetration of much of Latin America is far broader, deeper, and more successful than is generally understood. The case studies and overview presented in this report are a small sampling of a much larger Russian state-sponsored network carrying out a coordinated campaign across Latin America and fomenting chaos, insecurity, democratic backsliding, violence, and criminality. Despite this study's limited time, resources, and access to Russian language expertise, we found an alarming amount of Russian activity and believe a full regional study that could look more broadly at the issues raised would have significant value.

The groups interact extensively with each other, co-hosting events, speaking at each other's conferences, and cross-referencing each other on their websites. Despite the influence the groups wield individually and collectively, they are seldom the focus of U.S. policy interests in the region, which remain focused almost exclusively on Russia's historic state-to-state strategic relationships with Venezuela, Cuba, and Nicaragua.

At the same time, the local and regional law enforcement and intelligence across the region remain dangerously uninformed and unaware of Russia's strategic corruption and malign influence operations in their countries and do not usually link Russian cyber activities to broader Russian strategic campaigns.[60]

At the same time, the CN CEPLA group and its current director, Mashkova, have become a more visible part of the Kremlin's diplomatic arsenal in the hemisphere, especially for Spanish-language countries, where they publicly meet with most high-level Latin American delegations and issue formal statements on behalf of the Kremlin.

Given the large number of certificates of authorization from different Russian state entities posted by each group, including permission to work with state secrets and military technology, as well as a review of the leadership posts held by the directors of the different groups, these groups are undoubtedly directly tied to the highest levels of the Russian government.

The campaign has four identifiable goals:

(1) To enhance the surveillance capacity of the region's most repressive regimes—all Russian allies—and undermine democratic norms and the rule of law while providing tools to root out and eliminate perceived enemies.

(2) To position the Russian state to have persistent access to the most sensitive information in those nations where they gain a foothold, as they have in Paraguay and Argentina, and likely in multiple other countries, many of them historically important allies of the United States and mostly unaware of the existing vulnerabilities and penetration.

(3) To position Russian cyber and electronic capabilities and monitoring capacities under the direct control of Russian state security operatives, as closely located to the United States as possible, as shown in the Mokorón base in Nicaragua.

(4) To leverage and converge with other Russian malign influence operations, including sowing disinformation by covertly promoting AI-generated false narratives across the digital world and on social media.

Despite the 2022 invasion of Ukraine, Latin American nations have remained largely engaged in "active neutrality" and unwilling to condemn Russian aggression or impose sanctions on Moscow. Costa Rica was the only government to join in U.S. and EU economic pressure.[61] This has allowed the Russian cyber expansion to continue its advance, especially for those groups that maintain a façade of nonstate independence.

Given the overall lack of awareness of the ties of groups like SearchInform and CN CEPLA to the Russian state in host nations, as well as the diminished U.S. presence in the region and reduced embassy personnel, the Russian advances in their cyber campaigns are likely to continue as the U.S. Department of Justice underscored in several indictments related to Russian influence operations made public in September 2024.[62] It is a relatively low cost but effective way for Russia to support its nondemocratic allies, gain access to strategic information, and create more robust platforms from which to monitor U.S. activities and intelligence.

ENDNOTES

1. Government of the United States, Statement of General Laura J. Richardson, United States Southern Command, before the 118th Congress, House Armed Services Committee, March 12, 2024, https://www.southcom.mil/Portals/7/Documents/Posture%20Statements/2024%20SOUTHCOM%20Posture%20Statement%20FINAL.pdf?ver=Iwci9nu-nOJkQjxIWpo9Rg%3D%3D.

2. Douglas Farah and Marianne Richardson, "Dangerous Alliances: Russia's Strategic Inroads in Latin America," Institute for National Strategic Studies, National Defense University, Strategic Perspectives no. 41, December 2022, https://inss.ndu.edu/Portals/68/Documents/stratperspective/inss/strategic-perspectives-41.pdf.

3. Douglas Farah and Román Ortiz, "Russian Influence Campaigns in Latin America," United States Institute of Peace, October 17, 2023, https://www.usip.org/publications/2023/10/russian-influence-campaigns-latin-america.

4. Peter Bourgelais, "Commonwealth of Surveillance States: On the Export and Resale of Russian Surveillance Technology to Post-Soviet Central Asia," Access Now, 2013, https://www.accessnow.org/wp-content/uploads/archive/docs/Commonwealth_of_Surveillance_States_ENG_1.pdf; and Gary Miller et. al., "You Move, The Follow: Uncovering Iran's Mobile Legal Intercept System," Citizen Lab, January 16, 2023, https://citizenlab.ca/2023/01/uncovering-irans-mobile-legal-intercept-system/.

5. Primakov spoke fluent Spanish and had deep ties to Latin America. In 2010, he was awarded the Orden de Solidaridad by the Cuban government. See "Otorgan a Primakov Orden de Solidaridad con Cuba," Granma, January 22, 2010, https://www.granma.cu/granmad/2010/01/22/interna/artic23.html.

6. Eugene Rumer, "The Primakov (Not Gerasimov) Doctrine in Action," Carnegie Endowment for International Peace, June 05, 2019, https://carnegieendowment.org/2019/06/05/primakov-not-gerasimov-doctrine-in-action-pub-79254.

7. Valery Gerasimov, "The value of science in foresight: New challenges require rethinking the forms and methods of warfare, Military-Industrial Courier, February 26, 2013, https://archive.ph/gHt9q.

8. Douglas Farah, "Fourth Transnational Criminal Wave: New Extra Regional Actor and Shifting Markets Transform Latin America's Illicit Alliances and Transnational Organized Crime Alliances," Florida International University, June 2024, https://digitalcommons.fiu.edu/cgi/viewcontent.cgi?article=1063&context=jgi_research.

9. For a more complete look at criminalized states in Latin America, see Douglas Farah, "Transnational Organized Crime, Terrorism, and Criminalized States in Latin America: An Emerging Tier-One National Security Threat," Strategic Studies Institute, US Army War College, working paper, https://ssi.armywarcollege.edu/pdffiles/PUB1117.pdf.

10. "Centro de espionaje ruso opera en base militar de Mokorón en Managua," Confidencial, August 25, 2024, https://confidencial.digital/politica/el-centro-de-espionaje-de-rusia-en-el-cerro-mokoron-de-nicaragua/.

11. Farah and Richardson, "Dangerous Alliances."

12. Farah and Richardson, "Dangerous Alliances."

13. The information and drawings were taken from the main CN CEPLA website, https://cncepla.ru/es/. However, many of the pages have been taken down since the invasion of Ukraine, and the group's English-language page has been removed.

14. Bourgelais, "Commonwealth of Surveillance States."

15. James Andrew Lewis, "Reference Note on Russian Communications Surveillance," Center for Strategic and International Studies, April 18, 2014, http://csis.org/publication/reference-note-russian-communications-surveillance.

16. Alina Polyakova and Chris Meserole, "Exporting digital authoritarianism: The Russian and Chinese models," Foreign Policy Brief, Brookings Institution, August 18, 2019, https://www.brookings.edu/

wp-content/uploads/2019/08/FP_20190827_digital_authoritarianism_polyakova_meserole.pdf.

17. Government of the United States, Fact Sheet, “The United States Takes Sweeping Actions on the One Year Anniversary of Russia’s War Against Ukraine,” U.S. Department of State, February 24, 2023, https://www.state.gov/the-united-states-takes-sweeping-actions-on-the-one-year-anniversary-of-russias-war-against-ukraine/.
18. Government of the United States, “Security Alert: U.S. Embassy Moscow, Russia: Mobile Device Monitoring,” U.S. Department of State, June 06, 2024, https://ru.usembassy.gov/security-alert-u-s-embassy-moscow-russia-mobile-device-monitoring-june-6-2022/.
19. “Russian Espionage Center Operates at Mokoron Military Base in Managua,” *Confidencial*, August 27, 2024, https://confidencial.digital/english/russian-espionage-center-operates-at-mokoron-military-base-in-managua/.
20. RFRIT, “Digital Attaché Service,” https://rfrit.ru/sluzhba_tcifrovoi_attashe?ysclid=lj5pe884q0245214491.
21. “Comnews: ‘Digital Attachés” Will Fly Around the World,” Reksoft, September 02, 2022, https://www.reksoft.ru/blog/2022/02/09/comnews-digital-attaches/?ysclid=lxj9kw2pn6715833389.
22. Author interviews with Expo attendees from Chile and Colombia, December 2022.
23. https://dlg.im/en/government/. (access can lead to malware tracking)
24. Government of the United States, “U.S. Treasury Announces Unprecedented & Expansive Sanctions Against Russia, Impose Swift and Severe Economic Costs,” U.S. Department of the Treasury, February 22, 2022, https://home.treasury.gov/news/press-releases/jy0608.
25. 25 BC Game, website, https://dlg.im/en/integrations/, accessed August 16, 2024.
26. 26 Tony Frangie Mawad, “Venezuela is just one more card in Russia’s geopolitical game,” *Caracas Chronicles*, March 04, 2022, https://www.caracaschronicles.com/2022/03/04/venezuela-is-just-one-more-card-in-russias-geopolitical-game/.
27. “Russian Espionage Center Operates at Mokoron Military Base in Managua,” *Confidencial*.
28. Author interviews with exiled Nicaraguan military officials and cyber investigators, January to March 2024.
29. “Instilling terror: From lethal force to persecution in Nicaragua,” Amnesty International, October 18, 2018, https://www.amnestyusa.org/reports/nicaragua-authorities-stepped-up-strategy-for-repression-committing-grave-human-rights-violations-during-clean-up-operation/.
30. Author interviews with regional law enforcement, technology, and intelligence sources in Central America, February 2020.
31. “Russian Espionage Center Operates at Mokoron Military Base in Managua,” *Confidencial*.
32. For further information see Joshua Paltrow, “The Soviet Union Fought the Cold War in Nicaragua. Now Putin’s Russia is Back,” *Washington Post*, April 08, 2017, https://www.washingtonpost.com/world/the_americas/the-soviet-union-fought-the-cold-war-in-nicaragua-now-putins-russia-is-back/2017/04/08/b43039b0-0d8b-11e7-aa57-2ca1b05c41b8_story.html.
33. Carlos Fernando Álvarez, “Inaugurado el Centro de Capacitación Anti Narcóticos Rusia-Nicaragua,” *El 19 Digital*, October 16, 2017, https://www.el19digital.com/articulos/ver/titulo:62553-inaugurado-el-centro-de-capacitacion-anti-narcoticos-rusianicaragua-.
34. Lesbia Umaña, “Entregan diplomas a oficiales de la Policía que recibieron primer curso antinarcótico,” *El 19 Digital*, November 10, 2017, https://www.el19digital.com/articulos/ver/titulo:63445-entregan-diplomas-a-oficiales-de-la-policia-que-recibieron-primer-curso-antinarcotico.
35. Mabel Calero, “Esta es la propiedad que Daniel Ortega le ‘donó’ a Rusia en Managua,” *La Prensa*, June 30, 2019, https://www.laprensa.com.ni/2019/06/30/nacionales/2565282-esta-es-la-propiedad-que-daniel-ortega-le-dono-rusia-en-managua.
36. Tatiana Rodríguez Vargas, “Centro de capacitación ruso inicia su año lectivo 2019,” *Policía Nacional*,

January 28, 2019, https://www.policia.gob.ni/?p=28542

37. In addition to a brass plaque on the wall stating it, the Russian Embassy's official website makes this relationship unambiguous. See https://nicaragua.mid.ru/web/nicaragua_es/centro-de-capacitacion-del-ministerio-del-interior-de-rusia. Recent attempts to access the site shows it has been removed.

38. "Ortega admite que centro ruso en Nicaragua funciona 'para enfrentar golpistas'," *Confidencial*, September 12, 2023, https://confidencial.digital/nacion/ortega-admite-que-centro-ruso-en-nicaragua-funciona-para-enfrentar-a-los-golpistas/.

39. Pierluigi Paganini, "How Russia Controls the Internet," INFOSEC, July 01, 2014, http://resources.infosecinstitute.com/russia-controls-internet/.

40. https://searchinform.ru/docs/ Russian-language website

41. https://searchinform.ru/docs/ ; https://searchinform.ru/press/about-us/ SearchInform International, X (formerly known as Twitter), https://twitter.com/searchinformi?lang=en, accessed August 16, 2024.

42. Author field research in Paraguay and Argentina, June 2023, where the contracts with the local partners of SearchInform had dozens of contracts with the countries' security forces, justice ministry, intelligence services and other strategic sectors. A source involved with the company said this was replicated in each country where SearchInform worked. Having or acquiring such contracts was a condition of forming the partnership.

43. https://misis.ru/

44. https://old.sk.ru/foundation/about/ (no longer accessible)

45. Maria Kolomoychenko, "Usmanov's partner will hire generals to create wiretket systems," *Archive Today*, https://archive.ph/ByzTv, accessed August 16, 2024.

46. Farah and Richardson, "Dangerous Alliances."

47. http://www.cepla.ru/es/about/.

48. While much of the information has been taken down since the invasion of Ukraine, the author monitored the site over seven years and captured much of the content, including the certificates at the time of authorization from the FSB, valid from 2013 to 2018, the Ministry of Defense (2014-2019), and the sales operations. See Farah and Richardson, "Dangerous Alliances."

49. This information was taken from the CN CEPLA website, http://www.cepla.ru/es/about/, accessed August 23, 2024.

50. This information was taken from the Center website: https://www.inevm.ru/index.php, accessed August 23, 2024.

51. "Russian FSB mulls unified secure communications net," *Flash Critic Cyber Threat News*, August 21, 2013, http://flashcritic.com/russian-fsb-mulls-unified-secure-communications-net/.

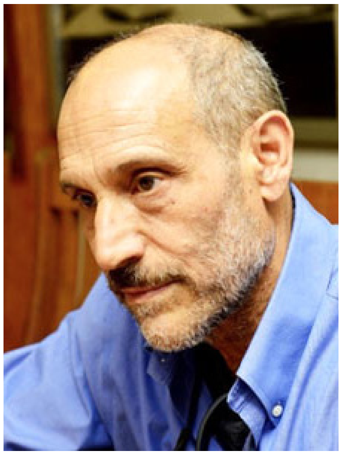
52. Much of the information on Starovoitov is taken from his biography on the CN CEPLA website: http://www.cepla.ru/es/about/president.php. For his time as director of FAPSI, see Mojmi Babacek, "The Threat of Information, Electronic, Electromagnetic and Psychtronic Warfare," Global Research, September 29, 2005, http://www. globalresearch.ca/the-threat-of-information-electromagnetic-and-psychtronic-warfare/1016?print=1; Additional information was found on the following Russian-language websites: http://www.agentura.ru/dossier/russia/people/ starovoitov/; and http://www.compromat.ru/page_11454.htm.

53. "Hero of Russia Alexander Staroviotov dies at 81," RT, July 17, 2021, https://russian.rt.com/russia/news/886328-geroi-rossii-aleksandr-starovoitov and https://cncepla.ru/es/press-center/news/79381/?PAGEN_2=25

54. http://cncepla.ru/es/about/staff.php.

55. Víctor Ternovsky, "Rusia y Latinoamérica con 'buena voluntad' y 'optimismo' para superar las trabas de su comercio," *Sputnik Mundo*, April 28, 2022, https://mundo.sputniknews.com/20220428/rusia-y-latinoamerica-con-buena-voluntad-y-optimismo-para-superar-las-trabas-a-su-comercio-1124942897.html.
56. http://www.cepla.ru/es/about/.
57. Much of the information accessed on Vasyagin in the initial research in 2017 and translated by C4ADS has been removed from original websites and is no longer available. For an overview of the ties of the Russian Orthodox Church, Orthodox Russia, and Vladimir Putin, see Geraldine Fagan, "How the Russian Orthodox Church Is Helping Drive Putin's War in Ukraine," *Time*, April 15, 2022, https://time.com/6167332/putin-russian-orthodox-church-war-ukraine.
58. Argentura.ru website, specializing in dossiers on Russian leaders, http://www.agentura.ru/english/dosie/fsnp/, accessed August 23, 2024.
59. For a brief official biography of Vasyagin containing information on his service in the USSR and Russian governments and first found in other sources, see "Vasyagin, Vyacheslav Petrovich," Bolshaya Biograficheskaya Enciklopediaya [Bolshaya Biographical Encyclopedia], http://my-dict.ru/dic/bolshaya-biograficheskaya-enciklopediya/1453992-vasyagin-vyacheslav-petrovich, accessed August 16, 2024.
60. This conclusion is based on numerous conversations the author has had with officials in Chile, Argentina, Paraguay, Colombia, Ecuador, and Uruguay during field research in the region from 2020 to 2024.
61. Farah and Ortiz, "Russian Influence Campaigns in Latin America."
62. Sarah N. Lynch, Andrew Gousdsward and Christopher Bing, "US charges employees of Russia's RT network in crackdown on election influence efforts," Reuters, September 4, 2024, https://www.reuters.com/world/us/us-accuse-russia-effort-influence-2024-election-cnn-2024-09-04/

ABOUT THE AUTHOR



DOUGLAS FARAH

Douglas Farah is the president of IBI Consultants and a senior advisor for Latin America for the International Coalition Against Illicit Economies (ICAIE). From 2014 to 2022, he was a Senior Visiting Fellow at National Defense University's Center for Strategic Research. From 1987 to 2004, Douglas was a foreign correspondent and investigative reporter for the *Washington Post* and other publications covering Latin America, West Africa, and transnational organized crime. After leaving the *Washington Post*, he founded IBI Consultants in December 2005.

Farah spent his first two decades in Bolivia and, in 1985, graduated with honors from the University of Kansas (a B.A. in Latin American Studies and a B.S. in Journalism). He was named UPI bureau chief in El Salvador and covered the region's civil wars. In 1987, he left UPI, and in 1988, he won the Sigma Delta Chi Distinguished Service Award for Foreign Correspondence for a *Washington Post* series on right-wing death squads in El Salvador.

In 1990, the *Washington Post* assigned him to Bogotá, Colombia, where he covered the exploding drug war in the Andean region and chronicled the rise and fall of Pablo Escobar and the Medellin cartel and other drug cartels. In 1992, the *Washington Post* named him bureau chief for Central America and the Caribbean. In 1995, Columbia University awarded him the Maria Moor Cabot Prize for outstanding coverage of Latin America.

In 1997, Farah returned to Washington as an international investigative reporter covering drug trafficking and organized crime. In the same year, he was honored by Johns Hopkins University for a *Washington Post* magazine article on how the Cali cocaine cartel bought the 1994 presidential elections in Colombia.

In March 2000, Farah was named the *Washington Post's* West Africa bureau chief. There, he covered the brutal civil wars in Sierra Leone and Liberia and the conflict diamond trade. In November 2001, Farah broke the story of al-Qaida's ties to those diamond and weapons networks.

He left the *Washington Post* in January 2004 after two years on the investigative staff.

Farah is the author of two books: *Blood from Stones: The Secret Financial Network of Terror* (Broadway, 2004) and *Merchant of Death: Money, Guns, Planes and the Man Who Makes War Possible* (with Stephen Braun, Wiley, 2007). He has published dozens of peer-reviewed academic papers, as well as chapters in six books. Farah appears regularly in regional media outlets.

FIU | Steven J. Green School of International & Public Affairs
FLORIDA INTERNATIONAL UNIVERSITY

SEPTEMBER 2024