Russian Federal Security Service (FSB) Internet Operations Against Ukraine

A TAIA GLOBAL REPORT

Russian Federal Security Service (FSB) Internet Operations Against Ukraine

On 31 March 2015, Ukrainian Security Service officials stated that their Internet monitoring component assessed that the Russian Federal Security Service's (RF FSB) 16th Center and 18th Center were behind Internet propaganda efforts directed at Ukraine[1]. The efforts included bogus social media postings generated by FSB controlled "trolls" and pseudo news postings from ostensibly Ukrainian news sites. According to the Ukrainians, the Ukrainian news sites were actually Russian controlled and coordinated with actions by Russian directed anti-Ukrainian activists. Ukrainian security officials stated that they had intercepted Internet communications between the activists and accounts attributed to Russian security services.

Taia Global research supports the Ukrainian official's assessment.

Political Background

In February 2015, Russian newspaper Novaya Gazeta published excerpts from a February 2014 Russian Presidential Administration planning document allegedly discussing plans for Russia's takeover of Eastern Ukraine[2]. The document concluded that then Ukrainian President Yanukovich would fall from power with unacceptable political and economic repercussions for Russia. The document provided a strategic outline for bringing eastern Ukraine under Russian influence. The outline stressed a concurrent PR campaign that depicted Russian actions as forced by the legitimate aspirations of pro-Russians in the south and east of Ukraine. The document stated that the campaign need include both Russian and Ukrainian media.

Russian implementation of the plan included supplementing ongoing political influence and traditional media operations with Internet operations directed against Ukraine[3]. The Internet operations include a significant effort to corrupt social media postings with controlled posting generated by hired Internet "trolls" almost certainly directed by Russian security services. While frequently stilted and transparent, the trolls postings create confusion and disrupt opposition efforts to use social media to generate political momentum. Former trolls have been interviewed by foreign media—including Radio Free Europe/Radio Liberty—and provided detailed accounts of troll operating methods and conditions. Russian media, working with former trolls, have identified the "trolls den" at 55 Savushkina Street in St. Petersburg and published both exterior and interior photos. The trolls are provided written guidance with their activities directed by "management" personnel[4].

Russian and Western media also identified several Internet news sites including the Kharkov News Agency, Neva News, novorus.info, newsdon.info, and newslava.info claiming to be Ukrainian news sites. The sites consistently provide a pro-separatist slant to their reporting. Media investigations found their claimed locations to be mostly bogus although Neva News was traced to the same location as the trolls den at 55 Savushkina Street. On 15 March 2015, Ukrainian security officials stated their Internet monitoring activities linked these sites to assets controlled by Russian security, specifically fingering the FSB's 16th and 18th Centers.

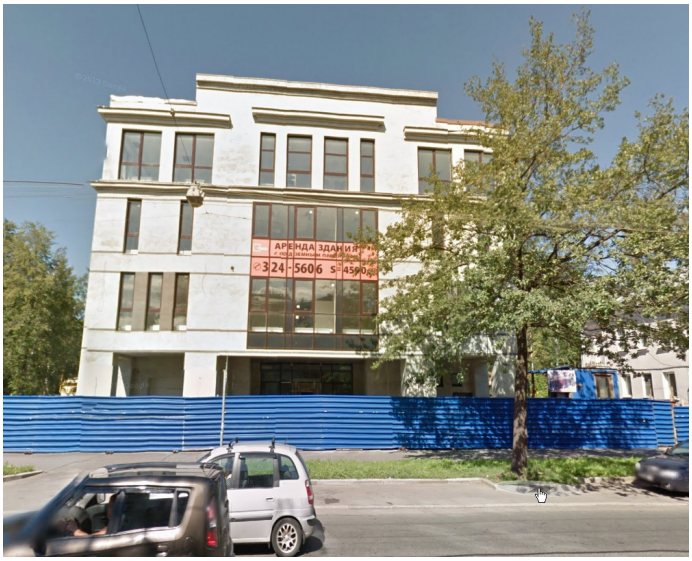
---

1 www.valuewalk.com/2015/03/russia-embarks-on-hybrid-war-in-ukraine/

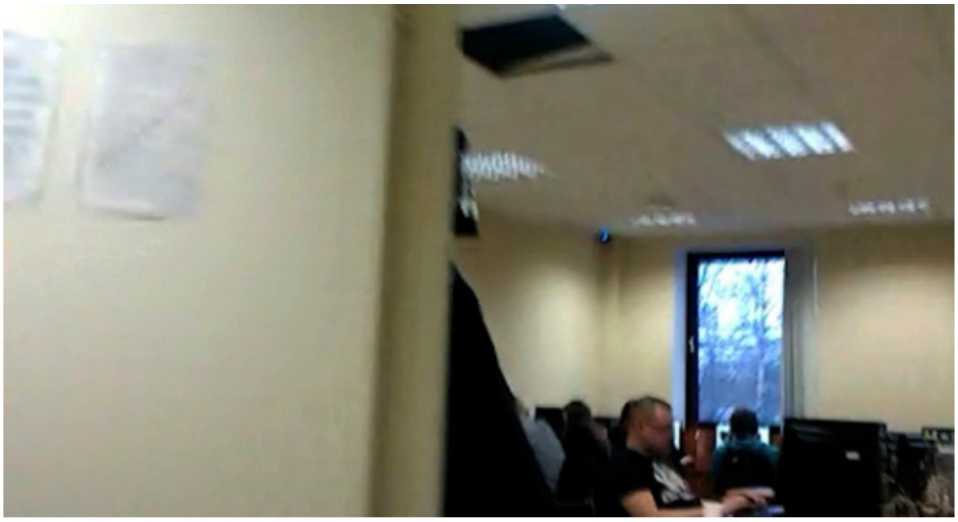
2 Moscow Novaya Gazeta Online in Russian 24 Feb 15

3 See *The Menace of Unreality: How the Kremlin Weaponizes Information, Culture, and Money* by Peter Pomerantsev and Michael Weiss for a full discussion modern Russian propaganda operations.

4 Security services frequently use the paradigm of directing a large number of uncleared personnel by a small cadre of cleared personnel to rapidly augment existing capabilities.



55 Savushkina Street, Yandex Maps



A rare glimpse [7] inside the "troll army headquarters" of Savushkina 55. Screencap from a video posted by Andrei Soshnikov to YouTube.

Globalvoiceonline.org

Internet Architecture and the 16th and 18th FSB Centers

The news sites Internet architecture supports the Ukrainian assessment. The domain name registrations for novorus.info, newsdon.info, and newslava.info were all obtained from Hong Kong based OnlineNIC with ownership protected. As of late April 2015, the sites were hosted at the same IP address on a server located in France. However, critical supporting architecture, such as the domain name servers (DNS), are located on AS 13238 the main enterprise network for the Russian search engine Yandex (see below). In short, the support architecture is located at the heart of the Russian Internet on servers closely monitored by Russian security services. The Russian can monitor anyone accessing the news sites and use their control of the DNS architecture to quickly relocate the sites if they are disrupted. Also, any attempt to attack the DNS supporting the sites would entail a conspicuous attack on Yandex with potentially serious effects that would affect ordinary Russians. The primary organization responsible for monitoring Yandex is the FSB 18th Center, the Information Security Center.

Records

Displays various information related to AS, BGP, Routes and Location.

Base	Record	Preference	Name	IP Number	Reverse	Routes	AS	Location
NOVORUS.INFO	A		NOVORUS.INFO	37.59.150.110	IP110.IP-37-59-150.EU	37.59.0.0/16 OVH ISP OVH Dedicated Servers	AS16276 OVH OVH SAS	France
	NS (primary)		DNS1.YANDEX.NET	2A02:6B8::213	DNS1.YANDEX.NET	2a02:6b8::/32 Yandex network	AS13238 Yandex Yandex LLC	
				213.180.204.213		213.180.204.0/24 Yandex enterprise network YANDEX-213-180-204 Yandex enterprise network		Russian Federation
	NS		DNS2.YANDEX.NET	2A02:6B8:0:1::213	DNS2.YANDEX.NET	2a02:6b8::/32 Yandex network		
				93.158.134.213		93.158.134.0/24 Yandex enterprise network YANDEX-93-158-134 Yandex enterprise network		Russian Federation
	MX	10	MX.YANDEX.NET	2A02:6B8::89	MX.YANDEX.RU	2a02:6b8::/32 Yandex network		
				77.88.21.89		77.88.21.0/24 Yandex enterprise network YANDEX-77-88-21 Yandex enterprise network		Russian Federation
				87.250.250.89		87.250.250.0/24 Yandex enterprise network YANDEX-87-250-250 Yandex enterprise network		
				93.158.134.89		93.158.134.0/24 Yandex enterprise network YANDEX-93-158-134 Yandex enterprise network		
				213.180.193.89		213.180.193.0/24 Yandex enterprise network YANDEX-213-180-193 Yandex enterprise network		
				213.180.204.89		213.180.204.0/24 Yandex enterprise network YANDEX-213-180-204 Yandex enterprise network		

Robtex Record 27 April 2015

The FSB's Information Security Center (FSB ISC)—also known as Military Unit (Vch) 64829—is the FSB's primary structure for counterintelligence operations involving Russia's internet infrastructure. FSB ISC operations include monitoring the Russian Internet—RuNET—and analyzing Internet content to identify threats.

The FSB's Information Security Center was formed in 2002 when then FSB Director Nikolay Patrushev re-organized the Department of Computer and Information Security inherited from the Federal Agency for Government Communications and Information (FAPSI). The re-organization split some administrative and developmental functions transferring them to other FSB components—including the Center for Communications Security; the Center for Licensing, Certification, and Protection of State Secrets; and the Scientific Technical Center—while focusing FSB ISC on counterintelligence operations on the Russian Internet. According to archived directives posted on the FSB web site (www.fsb.ru), FSB ISC is also designated as an FSB expert investigative center performing forensic investigations for criminal prosecution. Russian Law authorizes FSB ISC to conduct legal investigations and take action against Russian citizens. FSB ISC works closely with the Russian Ministry of the Interior Directorate K responsible for cyber crime.

The FSB ISC headquarters is located on Butchers Street adjacent to main FSB headquarters on the Lubyanka. The Russian security services monitor Internet traffic using hardware and software installed at Russian Internet Service Providers (ISP), Internet access points, and Internet exchanges. The Internet monitoring system--known as SORM—was first established in the 1990s. Despite some complaints by Russian ISPs, the system has evolved with RuNET and cooperation is mandated by Russian Law.

FSB ISC HQ (Street View) Butchers Street No. 6/3 Google Earth

According to Russian government tender documents and press reports, the FSB ISC began a major upgrade with contracts let during 2007 and 2008. The upgrade enhanced FSB ISC's ability to task the Internet monitoring system remotely and analyze collected information offline in a dedicated center located at the FSB ISC building on Butchers Street. The upgrade also enhanced FSB ISC non-attributable Internet operations.

According to the Russian tender document, the new FSB ISC monitoring/analytic center was funded as part of the ongoing Electronic Russian Government project. The center incorporated the best technology available to achieve several tasks:

- ensure the information needs of concerned departments and organizations seeking necessary information in the Russian segment of the Internet;
- construct distributed systems to identify individuals carrying out terrorist activity or other events under the competence of the Federal Security Service of Russia;
- monitor information situation in the Russian segment of the Internet;
- identify key trends, and those other events of interest to users of the Russian-speaking Internet segment;
- provide retrospective and predictive analysis of information, events, fact-based content analysis

of Russian-speaking Internet segment;
- coordinate system development with information systems, located with the analytic divisions of the Russian FSB.

The tender stated that the system would build on the existing monitoring and analytic systems installed at Russian ISPs with new equipment installed as needed. The center would exploit information from existing Russian search engines. The tender's language implied that access to search histories, site indexing and other data associated with search engines is already in place. The list included a reference to "other" unspecified sources that, in a security service context, normally refers to information obtained through covert intelligence collection.

The tender specified that the center would include remote, and non-attributable, tasking of monitoring sensors. The center desired extensive automated initial processing and classification—including geo-location—of detected data for transfer to offline databases for further processing. The tender included detailed specification of the desired equipment by specifying that performance would at least equal the performance of well know western technical systems and software. In sum, the project would provide FSB ISC with a state-of-the-art monitoring/analytic center operating on the Russian Internet without attribution.

In sum, any Internet operation originating in Russia are almost certainly monitored and probably overseen by the FSB ISC. Current Russian press covers Russian intentions to implement further restrictions on RuNet to counter foreign attempts to wage "information warfare" against Russian and ideologically subvert the Russian population. Whatever final form the new restrictions take, the FSB ISC will be heavily involved.

The FSB 16th Center is the primary structure for Internet operations outside Russia. The Russia Federal Security Service (FSB) Center for Electronic Surveillance of Communications (TSRRSS) is responsible for the interception, decryption, and processing of electronic communications. The Center —also known as the 16th Center (Directorate) FSB and Military Unit (Vch) 71330—is directly subordinate to the FSB Director.

According to a 2004 unclassified history, the Soviet Committee for State Security (KGB) consolidated existing signals intelligence (SIGINT) activity in the KGB 16th Directorate in 1969. The 16th Directorate responsibilities included:

- Interception of foreign communications—both legal and illegal—inside the USSR;
- Location of foreign communication systems—both legal and illegal—inside the USSR;
- Decryption of intercepted communications;
- Technical penetration of foreign embassies and facilities both in the USSR and abroad;
- Interception of foreign government and military communications aboard;
- Clandestine audio surveillance aboard.

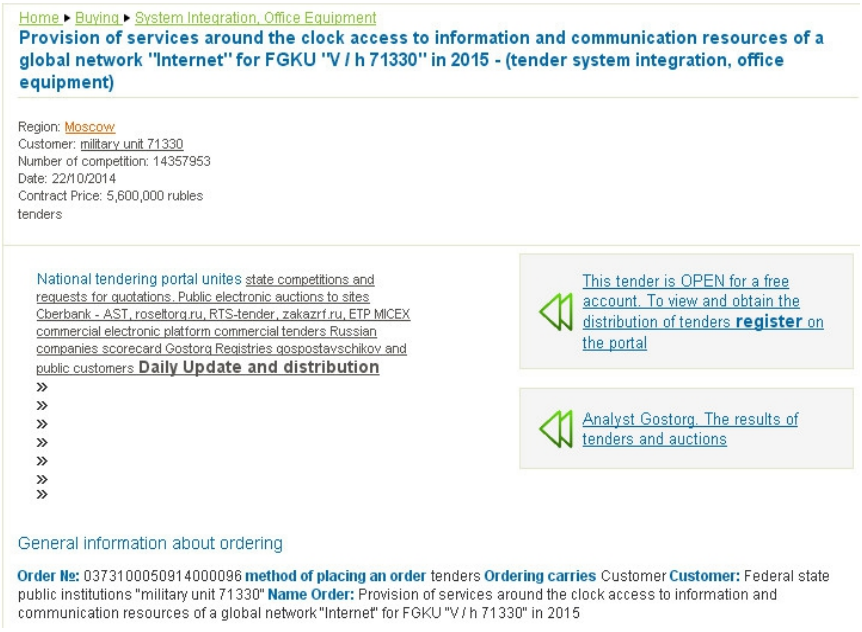
In 1991, Russian President Yeltsin broke up the KGB transferring the 16th Directorate to the Federal Agency of Government Communications and Information (FAPSI) where it became the Main Directorate for Communications Systems Signals Intelligence (GURRSS). The KGB's 8th Main Directorate—responsible for communications security —also went to FAPSI, already responsible for running government communication networks.

In 2003, Russian President Putin disestablished FAPSI with many communications security and intercept functions going to the FSB. Responsibility for running government communication networks went to the re-organized Federal Protection Service (FSO). Currently named the FSB Center for Electronic Surveillance of Communications (TSRRSS), the Center is also called the 16th Center (Directorate) reflecting the Center's bureaucratic heritage. For cover purposes, the Center is Military Unit (Vch) 71330.

The FSB 16th Center—Vch 71330--operations are increasingly focused on the Internet as communications that formerly moved through the air shift to wired digital networks. Vch 71330 is registered with the European Internet authority RIPE as holding a block of IP numbers. The block is located on Autonomous System Number 12695 (AS12695) registered to a Russian Closed Joint Stock Company (JSC) Digital Network (www.di-net.ru/www.msm.ru). According to the RIPE database, JSC Digital Network is a major service provider hosting networks for an extensive list of government and private entities. JSC Digital Network also maintains a block of IP numbers for Vch 43753, the FSB Communications Security Center.

RIPE registration data for JSC Digital Network lists their Network Operations Center (NOC) at Yaroslavskaya Street Number 13A. The contact information from the JSC Digital Network web site also lists that address. Taia Global mapped the address using Google and Yandex maps checking the address in English and Cyrillic. They both agreed on the location and agreed with the map on the JSC Digital Network web site. The building at that location, however, is not capable of supporting a NOC for a major Internet Service Provider (the building is across the street from the Alekseevskii Cathedral). The address could be the NOC's administrative office. The location of the NOC is unknown. Taia Global estimates that the NOC is actually at one of the major Moscow area data-centers.

Russian government contract tender postings[5] show Vch 71330 seeking additional Internet access through commercial vendors. A Google translation of the initial posting is shown below.



Home ▸ Buying ▸ System Integration, Office Equipment

Provision of services around the clock access to information and communication resources of a global network "Internet" for FGKU "V / h 71330" in 2015 - (tender system integration, office equipment)

Region: Moscow
Customer: military unit 71330
Number of competition: 14357953
Date: 22/10/2014
Contract Price: 5,600,000 rubles
tenders

National tendering portal unites state competitions and requests for quotations. Public electronic auctions to sites Cberbank - AST, roseltorg.ru, RTS-tender, zakazrf.ru, ETP MICEX commercial electronic platform commercial tenders Russian companies scorecard Gostorg Registries gospostavschikov and public customers **Daily Update and distribution**

» » » » » » »

This tender is OPEN for a free account. To view and obtain the distribution of tenders **register** on the portal

Analyst Gostorg. The results of tenders and auctions

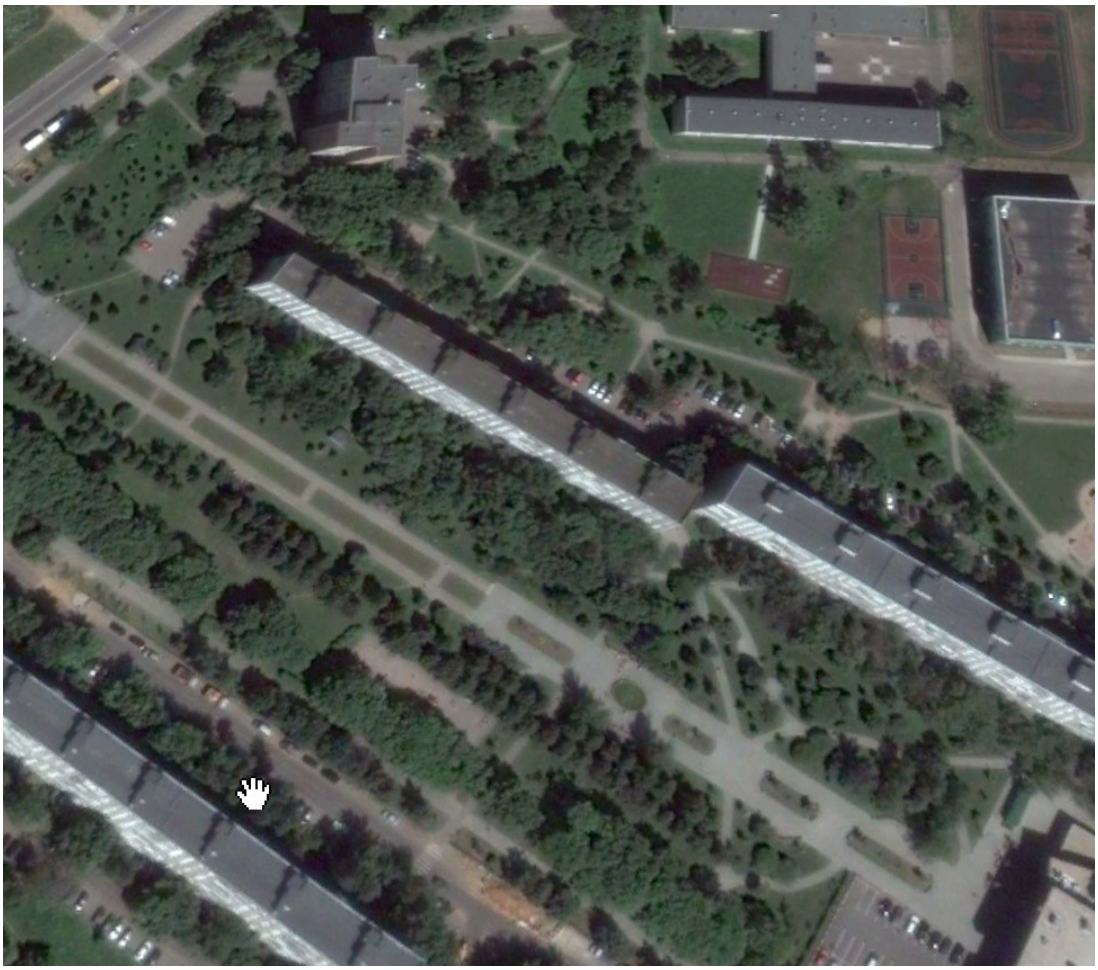
General information about ordering

Order №: 0373100050914000096 **method of placing an order** tenders **Ordering carries** Customer **Customer:** Federal state public institutions "military unit 71330" **Name Order:** Provision of services around the clock access to information and communication resources of a global network "Internet" for FGKU "V / h 71330" in 2015

The Vch 71330 contract was awarded to a small limited liability company NEO Print in Mytischi

5 http://zakupki.gov.ru/epz/contract/printForm/view.html?contractInfoId=19087186

northeast of Moscow. NEO Print's address tracks to a large apartment building in Mytischi[6] northeast of Moscow, an area long associated with Russian defense industry. Taia Global doubts Vch 71330 Internet service are run through an apartment building and assesses that the contract is probably a cover mechanism.



OOO NEO Print, Mytischi, Summer Street, d 24, Bldg 3 – Google Earth

While the FSB 16th and 18th Centers run Internet operation outside and inside Russia respectively, overall FSB operations against Ukraine are almost certainly run by the FSB Fifth Directorate. The Fifth Directorate's acknowledged role is preparing analytic reports for Russia's President and managing FSB relations with foreign intelligence services. However, Russian and foreign press articles allege that the Fifth Directorate's Department of Operational Information conducts intelligence gathering and influence operations in the "near abroad."[7] Russian press, however, shows Fifth Directorate leaders attending memorial services for Fifth Directorate personnel killed in "counter-terrorist" operations indicating that the directorate's role includes more aggressive options. Ukrainian press shows the Ukrainians seeking to interview Colonel-General Beseda regarding FSB involvement in violent attempts to suppress the Maydan movement[8].

6 The address was plotted in both Yandex and Google Maps. Some of the tender posts linked to the same map location.

7 The near abroad is Russia's term for those neighboring countries that, though now independent, formerly comprised the Union of Soviet Socialist Republics (USSR). Russia intelligence activities in the near abroad are conducted by the FSB, the Russian internal security service. Russian intelligence activities beyond the near abroad are conducted by the Foreign Intelligence Service (SVR).

8 Moscow Yezhednevnyy Zhurnal 13 Apr 14