# Mission Plan – Moscow, Russia

Theresa E. Elam
CSci384 – Information Warfare
April 21, 2004

## Executive Summary

**Target city**: Moscow, Russia.
**Primary target infrastructure(s)**: Oil and natural gas pipeline systems, electricity grids.
**Support target infrastructure**: Internet security.
**Goal**: Significant and prolonged disruption of the Russian economy via a progressive, multi-level attack culminating with widespread manipulation of the country's export pipeline system for oil and natural gas. An attack on these systems designed to prevent normal export operations for more than 30 days will have a devastating effect not only on the Russian economy, but Eastern and Western Europe, as well. The weakened economic condition of the country will leave it vulnerable to hostile operations of either a military or political nature. Such control over Russia, with the world's largest natural gas reserves and second largest oil reserves, could prove invaluable.

**Summary:**

- Timing – We have planned our attack for winter. Specifically, Russia's Constitution Day, which is Dec. 12. Advantages of this timing:
    - The weather – The average winter temperatures for Russia are well below freezing. Successful attacks on the energy sectors will be far more severe when mass public exposure to the elements is of concern to the government. Not only will emergency services, hospitals and community services be more burdened, but overall transportation will be more difficult, causing even more problems.
    - The three-day weekend – Russia's Constitution Day is celebrated with a three-day weekend. With the holiday, the government response is likely to be slower. In addition, there might be some parades or events to help to assist with Phase I of our plan (see below).

- Phase I
    - Goal of phase – Major traffic congestion on the streets of Moscow via multiple traffic incidents in strategic and planned areas. No major malicious intent here, more to study how the city and government responds to a "crisis" (specifically, any action that EMERCOM may take). It is reported that the bureaucracy of the government can

render emergency services ineffective. Is this true? If so, in what ways and how can we exploit this for further phases. In addition, we hope to tax the emergency services of the city in some ways.
    - Timing (in relation to Constitution Day) – Starting the day before the three-day weekend and continuing throughout.
- Phase II
    - Goal of phase – Large-scale disruption of power services in Russia. As with Phase I, the goal here is to learn how the government responds to crises in addition to further taxing emergency services and causing general panic within the city. Given that major power outages are not terribly uncommon in Russia, we hope to not raise too many alarms that our attack is a planned effort rather than weaknesses in the system.
    - Timing (in relation to Constitution Day) – 2-4 weeks after.
- Phase III
    - Goal of phase – Large-scale infiltration and control of the oil and natural gas pipeline systems. The goal is to cause the shutdown of major export trunk lines via misinformation fed to the monitoring systems by our insiders.
    - Timing (in relation to Constitution Day) – 8-12 weeks out.

## Political and Economic Climate

Russia is a study in contradictions. The largest country in the world in terms of area, yet it lacks access to major sea-lanes and ninety-four percent of its land is unavailable for agricultural use. Home to the world's first largest reserve of natural gas and the second largest of oil, yet the country ranks sixty-fifth in the World Economic Forum's Global Competitiveness Report. Since the 1991 dissolution of the USSR, Russia has been working to build a democratic political system and market economy, yet the majority of the Russian people feel the real power in the country is in the hands of big-business "oligarchs" and organized crime syndicates. The contradictory state of Russia is prevalent in almost every aspect of the country's make-up.

While unfortunate for the Russian people, the splintered nature of Russia makes it an ideal target for hostile operations. Specifically in support of our mission plan, four factors are paramount:

**Commodities vs. Transportation** – The general structure in Russian is that the commodities (e.g., oil, natural gas, electricity) are owed by private sector corporations and the state owns and controls the transportation systems (e.g., pipelines and power grids) that deliver those commodities to the consumer. This is interesting for our purposes for, while the private companies may be able to spend money to protect and secure the production of their goods, they have no control over the systems that transport their products to important consumer markets and in fact, a vast majority of these transportation systems are in a state of serious disrepair. These transportation systems are thus highly vulnerable to an outside attack.

**Corruption and organized crime** – Corruption and organized crime are rampant in Russian. In fact, in January of this year, President Vladimir Putin vowed to address the problem of corruption and held the first session of the Council Under the President for the Fight Against Corruption. In his address to the country regarding the new council, Putin cited bribery and government favors for high-profile businessmen as the two most common forms of corruption. In addition, a recent Interfax poll revealed that nineteen percent of the Russian people feel that their country is run by organized crime. This may not seem like a high percentage, but compared to the fact that only fifteen percent

believe President Putin is in charge and four percent feel power resides in the lower house of parliament, nineteen percent is quite significant. For the purposes of our mission plan, this political climate supports many ways to infiltrate government entities as well as access to sensitive information, infrastructure components, and computer systems.

**Formal vs. informal sources of power** – The above Interfax poll found that thirty-seven percent of Russians believe the power of their country rests in the hands of big-business "oligarchs". During the years following the break-up of the USSR while Russia was transitioning to a market economy, corporation stocks could be had for pennies and those in a position to do so took advantage of these opportunities. Today these stocks, mainly in the oil and natural gas industries, have made their owners billionaires. These businessmen, along with their contacts in government institutions have created an informal structure of power within Russia that is often more influential than the state itself. The formal government has recognized this and wants to reclaim its power. This has taken various forms from Putin's council on corruption to the imprisonment of a few of these businessmen following Kremlin initiated inquires (See Appendix A). This in fighting is relevant to our goals for while this power struggle continues to dominate the political and economic arenas, little is being done to modernize and protect the infrastructures that are our targets. In fact, little can be done. The government does not have the resources to modernize the commodity transportation systems and the corporations cannot modernize that which they do not control (and are being prevented from building new, private infrastructure).

**Export reliance** – Eighty percent of Russia's exports are tied to oil, natural gas, metals and timber. Fifty-five percent of the revenue from these exports is tied to the energy exports of oil, natural gas and electricity. The steady four to five percent GDP growth rate Russia has experienced in the last few years has mainly been fueled by high oil prices. In fact, in May of 2003, responding to President Putin's challenge to double the Russian GDP within ten years, the Russian government designated the energy sector as the primary engine for economic growth. At the same time, government subsidies and chronic domestic consumer non-payment issues have all but rendered the domestic market sterile for the country's natural resources. Thus, in order for Russian energy companies to remain profitable, they turn to external markets. To do this, they must rely

on the transportation systems controlled by the state. This combination of factors makes the commodities transportation systems *paramount* to the economic health of Russia and, at the same time, a very viable and attractive target for our purposes.

## Infrastructure Details – Oil and Natural Gas Pipeline Systems

**Infrastructure description** – As mentioned above, Russia is home to the world's largest natural gas reserves and the second largest oil reserves. Controlling the pipeline systems for these resources are Transneft for oil and Gazprom for natural gas. Both companies are state controlled and run. The following is a general overview of these companies and the systems they manage:

Transneft – The pipeline system that Transneft controls is a technological marvel. It comprises 46,800 km of trunk pipelines, 395 oil pumping stations, 868 storage facilities and has a carrying capacity of approximately 12.7 million cubic meters. The average length of the transcontinental routes is 3,500-4,000 km with future routes planned that may be as long as 9,000 km. The average pipeline diameter is 860 mm, which is almost twice that of the international average. However, it is estimated that roughly 20 percent – approximately 10,000 km – is in need of repair. The pipeline systems is also segmented into systems that serve domestic and external markets. The key export pipeline system is the Baltic Pipeline System (BPS), which carries oil from Russia's West Siberian and Timan-Pechora oil provinces to the port of Primorsk in the Russian Gulf of Finland. A major project is underway to construct another pipeline from the same region to Murmansk on the Barents Sea. The project is expected to be completed in 2007. In addition, several pipeline reversal projects are in the works as well as developing pipelines to the Far East.

Russian oil production in the near-term is being constrained by the country's export capacity. In 2002, the Transneft export pipelines had a maximum capacity of roughly 3.5 million bbl/d. However, the Russian oil producers turned out approximately 5 million bbl/d. Therefore, deficiencies in the pipeline system resulted in a 1.5 million bbl/d deficit. Producers tried to make up for the deficit by using alternative shipping methods such as rail and river barges, but these methods are far more expensive that transport via pipelines. The Russian government recognizes this issue and is taking steps to improve the state's export infrastructure via new pipelines, enhancements to existing pipelines and the reversal of existing pipelines to flow to external markets.

In order to monitor and protect its vast pipeline system, Transneft created the OJSC Diascan Center for Technical Diagnostics (CTD Diascan). This organization is a subsidiary of the parent company and was chartered in 1991 to address the dilapidated state of the pipeline system and create and support emergency response policy and procedures for Transneft. Appendix B is an article about CTD Diascan and contains some very useful information on technologies used by Transneft to monitor its pipelines. In a more general sense however, the existence of CTD Diascan is an important lead to discovering vulnerabilities in the Transneft system. A successful infiltration or compromise of this organization would be invaluable to our attack.

Gazprom – Like Transneft, the size of Gazprom is staggering. Gazprom controls nearly one-third of the world's natural gas reserves. It produces 90% of Russia's natural gas as well as running the pipeline grid for transportation. Gazprom is also Russia's largest earner of hard currency and the company's tax payments account for around 25% of federal tax reserves. At the same time, the company is severely hindered by governmental regulation in terms of the domestic market. The Russian Gas Law of 1999 forces Gazprom to sell gas to domestic users at government-regulated prices. Currently, those prices have Gazprom selling to the domestic market at below cost and at a price nearly one-tenth of the export price. These regulations, combined with chronic non-payment by consumers has left Gazprom in a weak financial position and has stunted the company's ability to invest in new projects. In addition, many oil companies are sitting on large natural gas reserves that they refuse to develop due to lack of lucrative export markets as Gazprom keeps firm control of the nation's pipeline network.

Development of a sound export infrastructure would be key to Gazprom and the Russian economy. Russia continues to export significant amounts of natural gas to the Commonwealth of Independent States (CIS), Europe, as well as Japan and other Asian countries. As with the oil sector and Transneft, development of new export pipelines and the refurbishing of existing systems are top priority for Gazprom. The Blue Stream system (From Russia to Turkey) is the major export

pipeline, with projects such as the North Trans-Gas Pipeline and Shakhalin I-III in the works.

Also like Transneft, Gazprom also has an in-house monitoring and security division for its pipelines. The United Gas Transmission System (UGTS) is responsible for reliably delivering Gazprom products to distributors and end-consumers. Not as much information was available about UGTS, but as with CTD Diascan, its existence provides us with a valuable target in which to exploit.

Russian pipeline systems are at a critical juncture – to exploit the vast natural resources of the country, they must find a way to get those resources to lucrative export markets. However, financial instability, government regulation and the daunting nature of upgrading such a large and antiquated system leaves the system vulnerable to attack with devastating consequences.

**Cascading** – Obviously the energy sector touches almost every aspect of daily life within a country and damaging the transportation infrastructure of this sector will have widespread effects. Specifically in regards to the Russian oil and natural gas pipeline infrastructure, our main goal is to disable the Russian economy via the ripple effect of damaging its existing export pipeline system and impacting the large revenues these sectors generate.

However, another ripple effect that cannot be ignored will be the impact on the countries that rely on Russian for oil and natural gas. For the oil market, the effect could be felt not from the lack of oil, but rather in the increased dependence on oil from the countries that are members of the Organization of Petroleum Exporting Countries (OPEC). This organization has a history of keeping oil prices artificially high by controlling market supply. Russia has taken advantage of this by offering an alternative to OPEC oil. A significant disruption of Russia's ability to export oil could disrupt this balance.

For the natural gas market, the impact would be greatest on those countries that export large amounts of Russian natural gas. For example, Slovakia and Belarus export over 90% of their domestic consumption of natural gas from Russia and for Italy, France and Germany, the numbers are around 30%. In his written statement to the Special Senate

Committee on the Year 200 Technology Problem, Lawrence K. Gershwin estimated that Western Europe could survive for 30 days if Gazprom was unable to deliver natural gas. This would especially be true in the winter, where natural gas is a common source for heating and cooking. Our attack is planned for December to take maximum benefit of this situation.

**Technology reliance and open source intelligence** – Modern pipelines systems rely on two general types of technology. They are:

- Supervisory Control & Data Acquisition System (SCADA) – As the name implies, these systems are responsible for acquiring data to facilitate the control over a system. For pipeline systems, with their vast geographical spread, the usefulness of such systems is obvious. These systems are mainly built to monitor the pumping stations and tank farms along the pipelines. Raw data, graphs and even warning alarms are collected and sent back to a main repository for analysis. In addition, system managers can use a SCADA to actually control portions of the system they monitor.
- Intelligent "pigs" – Pipeline "pigs" are used mainly to clean and monitor the health of pipelines. Ranging from simple scrubbers to sophisticated tools with more than 300 sensors, pigs are automated pieces of machinery that travel pipelines and send information back to be analyzed.

The exploitation possibilities of the above technologies are extensive and the effects quite powerful. Controlling such systems would allow us to not only shutdown portions of the pipelines, but, more covertly, we could cause the companies themselves to shutdown by causing false reports of damages or systems errors in key places. The key is using the infrastructure of the pipelines themselves to our advantage. Exploiting the systems above will allow us to cause damage (or reports of damage) that may be hundreds, if not thousands of kilometers away from the services needed to repair it. The time and resources it will take to respond to such damage will be significant. Enough false alarms could cause monitoring systems to be shut down completely, exposing the pipelines to potential physical attacks.

For the most part, the software for the SCADA systems and pigs used for the Russian pipelines run on Microsoft Windows and use TCP/IP to transmit data back to

management. In the course of our research, we found two companies that provide SCADA and intelligent pig technologies to Transneft and Gazprom. Iconics, Inc. is a company located in Foxborough, Massachusetts and provides the world's largest PC based SCADA and dispatch system to Transneft. According to the press release (see Appendix C), the Iconics system runs on Microsoft Windows 2000 and NT and has an ActiveX web-enable thin client/server architecture. Volgasoft, a company from Saratov, Russia provides the embedded programs used by the intelligent pigs that travel the Gazprom pipeline system. They also provide the analysis software for the gathering and processing of the information the sensors gather. The case study (see Appendix D) provides details on operating systems (various Windows versions), languages the software was written in as well as screen shots of the information the system provides.

**Physical mapping** – High-quality pipeline maps will be vital to the success of our mission. There are several companies (e.g., Pennwell MapSearch out of Houston, Texas) that sell these types of maps and they are quite expensive. However, for maximum damage, it would be critical to obtain such information so that the best possible targets could be identified.

There are high-level pipeline maps available on-line. Some examples can be found in Appendix E.

## Infrastructure Details – Electricity

**Infrastructure description** – Russia depends greatly on its strong electrical power industry, which evolved and grew after the soviet era. In 1992 Russia established the Russian joint-stock electricity and electrification company, RAO UES (Unified Energy Systems or UES) of Russia (see Figure 2 below). RAO UES oversees the daily operations of large thermal power plants with capacities of 1000 MW or higher, hydroelectric power plants with capacities of 500 MW or higher, high voltage trunk lines that form the single power grid of the Russian Federation, central and regional dispatching offices, and Research and Development institutions. RAO UES owns wholly or in part 73 of the 75 regional joint-stock energy and electrification companies (AO Energos). RAO UES is responsible for much of the generation, transmission, and distribution of electricity in Russia. They own 2.6 million kilometers of transmission and distribution lines or more than 96% of all transmission and distribution in Russia. Two regional energy systems did not form part of UES, OAO Irkutskenergo and POEE Tatenergo. Thirty power stations were incorporated as independent power stations or AO-Electrostations. All AO-Energos are part of seven integrated power systems (IPSs) of which six work in parallel (the Center, Middle Volga, Urals, Northwest, North Caucasus, and Siberia IPSs) and the East IPS, which operates separately from the Siberia IPS.

The Russian Power Grid is the world's largest highly automated grid. It is also very complex to generate, transmit, and distribute electric power. Because of the complexity, Russia's power grid is also difficult to control and monitor on a daily basis. The power grid can be controlled from a single center, although it is a complex network of power plants and mains, which all have the same operating mode and centralized dispatching control. UES zonal enterprise operates the high-tension transmission lines that make up the core system network of the power grid. The length of these mains equal a distance of 153,400 km and the total length of the electric mains in the Russian Federation is 2,647,800 km. There are 432 public power plants that create the engineering base of the Russian power industry.

The current state of the power sector of Russia can be characterized by the following. The power sector of Russia has a high level of monopolization, with one organizational

structure that has been given the responsibility of joining together both monopolist and potentially competitive activities. There is no free market (neither wholesale and retail) for power and generating capacities. State regulation of power tariffs exist with a tendency that tariff growth rates stay behind the general inflation index. There is a low profitability of power and heat production due to low tariffs and the general low production efficiency that is insufficient to compensate for investment risk.

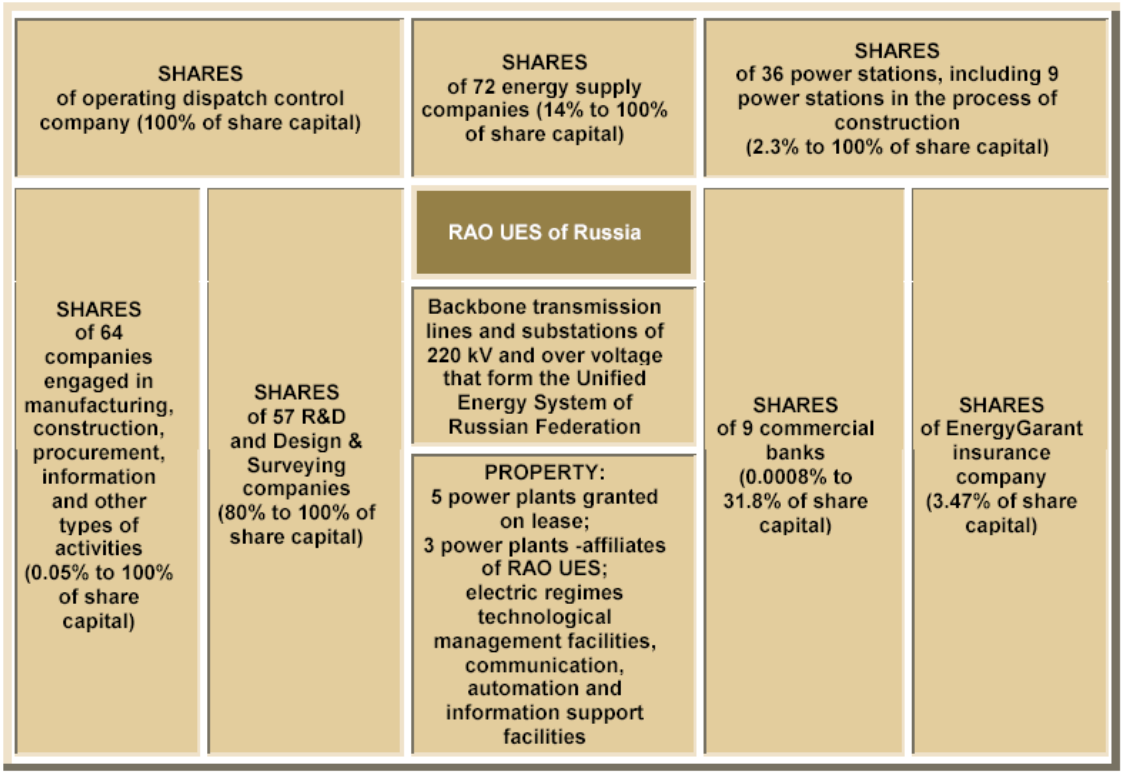



Figure 5: RAO UES Ownership Structure

Figure 2: RAO UES Ownership Structure

**Cascading** – Once the electrical power infrastructure is damaged, the financial infrastructure will be greatly damaged also, because of the already unstable financial climate of UES. UES is selling electricity to retail consumers at very low prices, about 1.2c per kWh. UES makes a profit only because the industrial price of electricity is considerably higher. The industrial sector is subsidizing the retail sector. Retail prices would have to increase by two to three times for the system to approach a reasonable structure. Power to various communications centers, nuclear power plants, hydroelectric power plants, and thermal power plants will be interrupted as well which will slow

Russia's export industry causing a substantial reductions in production and export. Transportation will be affected as power to the trains that run on electricity is interrupted. Russia relies greatly on trains for mass transit and for the delivery of crucial supplies to power utility stations. More blackouts would occur as a result. With part of the trains system out of operation, major traffic delays will occur along with blackouts spread throughout. This should cause mass confusion leading to panic.

The Russian Federation's Ministry of Civil Defense, Emergencies and the Elimination of the Consequences of Natural Disasters (EMERCOM) is responsible for managing catastrophic situations in Russia caused by either neglect on the part of man, uncontrollable acts of nature, or the consequences of accidents. EMERCOM will be Russia's first line of defense and therefore they will be notified once the attacks on the electricity begin. Hence we must also attack EMERCOM and prevent their corrective actions by disrupting communications between the electricity sector and them. Therefore as the electricity team is initiating blackouts throughout Russia and causing other calamitous events, another team will implant themselves in the EMERCOM network at the Command and Control Center. They will block legitimate incoming and outgoing communications by initiating a pipe flood to incapacitate the network and a port/service flood to disable EMERCOM's key services. The team will also modify data to send incorrect instructions and directions, false information regarding supplies and resources needed, and false information regarding the actual reason for requesting the assistance of EMERCOM. These actions are not aimed at totally stopping EMERCOM's actions but rather to slow and hinder its otherwise quick response. Dispatched units will respond much slower to the blackouts, massive traffic jams, multiple power plant's loss of electricity, and other planned disasters. As a result the damaging effects of the planned disasters will be much more intense.

**Technology reliance and open source intelligence** – UES who manages the Russian national power grid uses Industrial and Financial Systems (IFS) Applications for the maintenance, technical development, and supervision of power lines and network objects in the high voltage transmission infrastructure. Due to the dispersed infrastructure of the grid UES uses this software to streamline the networks and corporate processes. IFS's Enterprise Asset Management System (EAM) handles

project management, document management, and procurement. Corporate Financial System (CFS) is the IFS distributor in Russia. IFS develops and supplies component-based business applications for medium and large enterprises and organizations. It is based on web and portal technology. The software solution is used in manufacturing, supply chain management, service provision, financial management, product development, maintenance and human resource administration.

IFS applications are based on component architecture that features open interfaces and web services to enable extended connectivity and coexistence with other applications. The web technology runs on Windows IIS and Apache Web servers in addition to special solutions from IBM and SUN. The web interface was designed with standard HTML and JavaScript. IFS software also allows the user to link from IFS applications to information on the Internet and on the Intranet. IFS also allows the user to ink from the Intranet directly to activities, data, queries, and reports in IFS Applications.

The portals are role-based and tailored for each user. Intranet, Extranet, and Internet information can be integrated directly into the portal. However with these amenities comes the need for increased security and bandwidth and network delays to overcome. IFS applications allows up to 5 concurrently active users per 56 kbps connection. IFS supports Microsoft Internet Explorer and Netscape. It provides access from standard Java Server Pages (JSP) and Servlets, as well as Microsoft Active Server Pages (ASP).

Vulnerabilities of the above infrastructure include:

- Technically advanced relays can be programmed over a telephone modem connection after typing in an eight-digit password.
- Weak network links between the European part of Russia and Siberia and between Siberia and the Russian Far East
- Dispersed infrastructure of grid
- Low electricity and heat tariffs established by regulatory bodies led to under investment in the power industry with respect to replacement of production facilities. As a result there is much wear and tear of production equipment.
- Network and corporate processes not streamlined
- Degrading power lines

- Embedded systems used to monitor, control, and assess system. These systems are received from a vendor who has added the requested software prior to shipping. However the vendor receives part of the product from sub vendor who adds a layer of functionality before shipping.
- Switches and monitoring equipment programmed remotely with software. Therefore there will be vulnerable connections to a computer network.
- Weak grid designs and configurations
- Microsoft IIS is inherently not secure.
- Apache web server is inherently not secure.

**Physical mapping** – High-quality electric grid maps will be vital to the success of our mission. On-line searches revealed very little in terms of publicly available maps. Therefore, we feel the best way to obtain such maps would be via the reconnaissance phase of our plan when we would have teams in Russia to obtain this information.

We were able to find some surveillance photos of power lines and graphs relating to the structure of the Russian power industry. These can be found in Appendix F.

## Infrastructure Details – Internet Security

**Infrastructure description** – On December 9, 2000, President Putin signed the "Information Security Doctrine of the Russian Federation". This was the first major step towards a national information security policy within Russia. The policy ties Internet security with four major "national interests", which are:

- The respect of the constitutional rights and freedoms of man and citizen in obtaining and using information,
- Information support of the state policy of the Russian Federation,
- The development of modern information technologies and a domestic information industry, and
- Protection of information resources against unauthorized access

This information is key to the success of our mission plan because, unlike other industrialized nations, the Russian government has tried to keep control over what technologies provide Internet security within the country. To further this goal, the country has set up the following two regulatory agencies:

- Federal Agency of Governmental Communications and Information (FASPI) - This agency is responsible the licensing of all encryption technologies within Russia.
- State Technical Commission (GosTekhComissiya) – This agency is responsible for certifying all authentication/identification, access control and audit logging technologies within Russia.

The existence of a national Internet security policy and regulatory system is important for two main reasons. The first is that the difficulty of obtaining the needed licenses and certificates from the above agencies has actually made Russian networks l*ess* secure. The added cost of obtaining these documents is such that many companies do without or use vastly inferior protection solutions that rely on one technology only. Secondly, according to Russian legislation, state enterprises and organizations working with sensitive information are liable to use only local products that have received the appropriate documentation from FASPI and the GosTekhComissiya. This requirement greatly reduces the number of possible security solutions that an organization may utilize and makes finding vulnerabilities in said systems dramatically easier.

**Cascading** – The impact of a weak Internet security infrastructure impacts all organizations and entities connected to the Internet. In the case of our mission plan, this is especially relevant with respect to those organizations connected to our targets. The gas/oil pipeline systems and electrical infrastructure may be relatively more secure in that they are government controlled, however, the businesses that are connected to our targets are less so. In addition, the fact that are targets are government institutions and subject to the above regulation gives us a far narrower scope of technologies in which to research in order to find vulnerabilities.

**Technology reliance and open source intelligence** – Although there is evidence of the use of *nix-based operating systems, for the most part, Russian Internet security infrastructure relies on DOS/Windows technologies (see the "Open Source Intelligence" section below for more details). In terms of encryption, 256 bits is the standard and the algorithms are under the complete control of FAPSI. A main exception to the FAPSI control of encryption is that foreign-owned companies may use software products with non-FAPSI certified encryption to communicate with their Russian subsidiaries. However, the encryption must be built into the software package and not an add-on.

Fortunately for this project, there is a publicly available list of the Internet security products (including version numbers) certified by the Russian government. It can be found on-line at http://www.jetinfo.ru/annexes/3/annex-3.html. Unfortunately, it is in Russian. A mechanical translation of the list revealed the following names:

- Cisco Pix
- Zastava-Jet
- AltaVista Firewall
- CyberGuard
- Gauntlet
- Bay Networks
- SecretNet
- Ship

Several of these names resulted in numerous hits from the CERT vulnerability database. To fully exploit this information a full translation would be needed, which would be very easy to obtain.

In addition, the Moscow International Safety and Security Trade Show is an annual event and is the premier event that showcases a wide range of security (both for physical and Internet security) products used within Russia. Attending this trade show would be invaluable to learn more information about what products are being used in which organizations. Information on the event can be found at http://www.buyusa.gov/russia/en/113.html.

**Physical mapping** – While mapping of the Russian Internet security infrastructure is not a commonly available resource, maps of Russia networks are. Figure 1 below is the Internet infrastructure of Golden Telecom, one of the major ISPs in Russia. While the map is quite high-level, there are others, usually available for a fee, which are quite detailed. Sources of such information include:

- Traceroute, DNS queries and whois information – See Appendix G for output using these tools against our oil and natural gas pipeline targets as well as some key players in the oil and natural gas industries. We now have IP address ranges, possible hosting locations and contact information. In addition, searches for the contacts listed in the whois queries were performed using the Google Group search. The results were in Russian, but could be easily translated.
- http://www.rocich.ru/georunetica/rumaps.php - A source for maps of Russian ISPs. In Russian, but easily translated.
- http://www.telegeography.com/ - A company headquartered in both the United States and the United Kingdom. Detailed information on network geography and usage for more that one hundred countries. Average price of the information is around $3000, however, the cost is worth it compared to the time it would save in compiling the information by hand.
- http://www.cybergeography.org/atlas/atlas.html - An “atlas of cyberspaces”. Information regarding many projects that map the Internet in various ways.

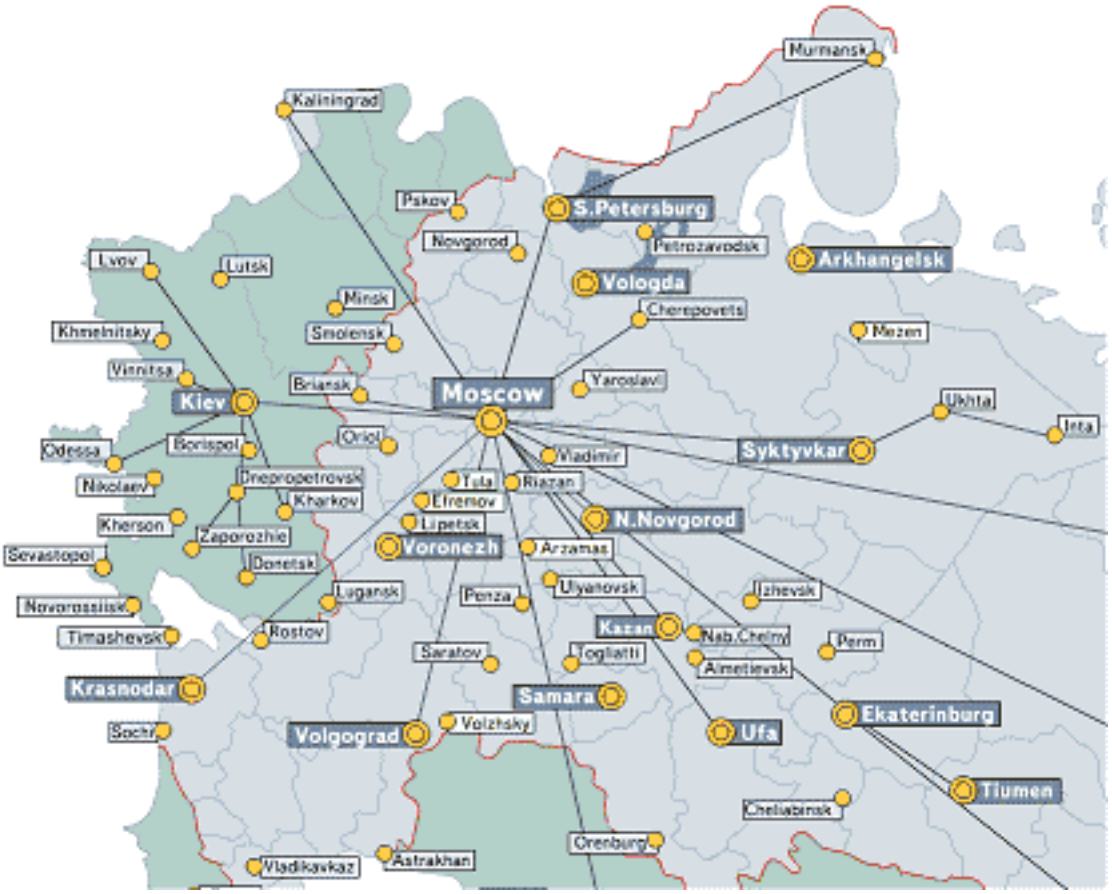



**Figure 1:The Internet infrastructure of Golden Telecom in Russia.**

## Mission Plan

**Target city**: Moscow, Russia.
**Primary target infrastructure(s)**: Oil and natural gas pipeline systems, electricity grids.
**Support target infrastructure**: Internet security.
**Goal**: Significant and prolonged disruption of the Russian economy via a progressive, multi-level attack culminating with widespread manipulation of the country's export pipeline system for oil and natural gas. An attack on these systems designed to prevent normal export operations for more than 30 days will have a devastating effect not only on the Russian economy, but Eastern and Western Europe, as well. The weakened economic condition of the country will leave it vulnerable to hostile operations of either a military or political nature. Such control over Russia, with the world's largest natural gas reserves and second largest oil reserves, could prove invaluable.

There are several strategic reasons we chose a more "passive" type of attack on Russia. Granted, it is difficult to characterize any attack as "passive", however, we are trying to differentiate our approach of exploiting systematic weaknesses in the country to that of 9/11-type destructive attack. Our reasons are:

- Long-term effects – While the 9/11-type attack certainly disrupts daily life of a target, it is for a relatively short period of time. It is true that changes to daily life may continue for some time (e.g., increase security lines at airports, etc.), but we would argue that as being a disruption. The target continues to operate and move forward. Our goal is long-term disruption in the sense that Russia is no longer able to support the organizations and services needed to run the country and we feel the best way to do this is to attack the economy which, fortunately for us, is unstable to begin with.
- Lessen the effects of martyrdom. With 9/11-type attacks, the target is given a common enemy to rally against. Patriotism within the target is fueled as well as sympathies from other countries that do not wish to be the next target. If done correctly, our attack will not appear as an outside attack, but a consequence of Russia's fragile economy and weakened state-controlled infrastructure. In this situation aid from other countries will certainly still be offered, but for different reasons and certainly with more strings attached. These strings will further weaken Russia's control over its own country.

- Ripple effects to other countries – As mentioned earlier, the disruption of Russian oil and natural gas exports will have effects on other countries. Looking for more stable supplies of energy, these countries have two main options. First, they could look to other sources of energy. This helps our overall goal by reducing supply for Russian energy and further damaging the economy. Given Russia's vast energy reserves however, this is unlikely. Rather, countries are more than likely to exert pressure on Russia to relinquish the state-monopolies on its energy sectors and to modernize its political and economic structure. Is this a "bad" thing? From the perspective of the Russian government, yes, which furthers our overall goal.
- Harder to prevent and apply countermeasures. If done correctly, the type of attack we have planned will be very hard to prevent against. By exploiting systematic weaknesses in our target, we essentially use the country against itself. These systematic flaws often have very few countermeasures and if they do, they take years, even decades to implement.

**Plan**: The following is a summary of our plan. It is a three-phased attack in addition to a reconnaissance phase.

- Timing – We have planned our attack for winter. Specifically, Russia's Constitution Day, which is Dec. 12. Advantages of this timing:
    - The weather – The average winter temperatures for Russia are well below freezing. Successful attacks on the energy sectors will be far more severe when mass public exposure to the elements is of concern to the government. Not only will emergency services, hospitals and community services be more burdened, but overall transportation will be more difficult, causing even more problems.
    - The three-day weekend – Russia's Constitution Day is celebrated with a three-day weekend. With the holiday, the government response is likely to be slower. In addition, there might be some parades or events to help to assist with Phase I of our plan (see below).
- Reconnaissance phase
    - Goal of phase – Gather information in support of the phases of our plan and to setup needed infrastructure.
    - Timing (in relation to Constitution Day) – 12-18 months out.
    - Resources needed

- All phases – Russian speakers and/or translators. Study corruption and organized crime within the country. Identify sources of power and methodologies by which sensitive information can be obtained.
- Phase I – Study geography of Moscow. A river splits the city, how can we use this to our advantage? Send 2-3 people to Moscow to study its public transportation systems and general traffic patterns. Best way to do this would be to plant people as bus drivers, taxi drivers and couriers. In addition, procure detailed maps and system details for study.
- Phase II – At least 1 year before compromising any systems, subjects will be planted in UES, IFS Russia, and CFS. These subjects will learn how daily operations are conducted, establish contacts, learn the technology and software used, and find vulnerabilities and weaknesses in the technical side and human side. They will also identify critical nodes and their interdependencies and calculate the consequences of a power failure. The subjects will also identify the physical limitations and uncertainties. To do this, we will need to identify positions within UES, IFS Russia, and CFS where we can place people. In addition, identify contractors, service provider and partners that might also have positions available.
- Phase III - At least 1 year before compromising any systems, subjects will be planted in Tansneft's CDT Diascan and Gazprom's UGTS. These subjects will learn how daily operations are conducted, establish contacts, learn the technology and software used, and find vulnerabilities and weaknesses in the technical side and human side. They will also identify the best locations for pipeline failures and study emergency response systems and procedures. To do this, we will need to identify positions within Transneft and Gazprom where we can place people. In addition, identify contractors, service provider and partners that might also have positions available.

- Phase I
    - Goal of phase – Major traffic congestion on the streets of Moscow via multiple traffic incidents in strategic and planned areas. No major malicious intent here, more to study how the city and government responds to a "crisis" (specifically, any action that EMERCOM may take). It is reported that the bureaucracy of the government can render emergency services ineffective. Is this true? If so, in what ways and how can we exploit this for further phases. In addition, we hope to tax the emergency services of the city in some ways.
    - Timing (in relation to Constitution Day) – Starting the day before the three-day weekend and continuing throughout.
    - Resources needed – Using the information from the reconnaissance phase, we will need the people and vehicles needed to cause the traffic incidents.
    - Details – Traffic in Moscow is horrendous. The Institute for Traffic Care was commissioned by the government to implement the Moscow Urban Traffic Project to relieve the city of its major traffic headaches. Using this and the geography of the city to our advantage, the plan is to cause major traffic congestion for several days in a row via a series of small, strategically planned incidents.
    - More information needed – As mentioned above, detailed maps of Moscow as well as information about traffic flows will be needed.
- Phase II
    - Goal of phase – Large-scale disruption of power services in Russia. As with Phase I, the goal here is to learn how the government responds to crises in addition to further taxing emergency services and causing general panic within the city. Given that major power outages are not terribly uncommon in Russia, we hope to not raise too many alarms that our attack is a planned effort rather than weaknesses in the system.
    - Timing (in relation to Constitution Day) – 2-4 weeks after.
    - Resources needed – Inside contacts from Reconnaissance phase. Mobile team to help disrupt EMERCOM services.
    - Details

- Exploit component reliability and parameter uncertainties by triggering system interruptions, changes in the frequency, disruptions in transmission and generation, and by triggering simultaneous faults.
- Change settings to trigger cascading blackouts. We want the outages to cause demand to suddenly outweigh supply, putting a strain on the grid and possibly cause more power losses.
- Implant a worm similar to Blaster or a tiny piece of corrupted data to totally block communications between computers used to monitor the power grid. It would block commands that operate power utilities. The worm would hinder the response to multiple power line failures. The goal would be to crash the crucial computerized control device that is installed in all of the grid substations. To help mask our activities, this worm should be released into the "wild" as well.
- Exploit Microsoft IIS and Apache web server vulnerabilities to gain root access and take control of the remote terminal unit and command it to trip breakers. Next change the settings on substations' programmable circuit breakers. The team will lower settings on some breakers (i.e., 500 to 200) and raise settings on others (i.e., 500 to 900). Normal power usage could trip the 200 amp breakers and take those lines out of service, diverting power to other lines with the breakers set to 900. These breakers are set too high to trip the overload. As a result, the transformers and other critical equipment on these lines would have a meltdown. Major repairs would have to be performed on this equipment costing much money, time, and resources that are already limited in Russia.
- Exploit the relays on telephone modem connections. Use the most efficient password-cracking tool to crack the passwords. Find substation phone lines that connect to these relays with war dialers.

        - Further damage power lines to the point that they no longer transmit electricity.
    - More information needed – Best systems within the power infrastructure to exploit and more detailed analysis of computer systems that run the infrastructure.
- Phase III
    - Goal of phase – Large-scale infiltration and control of the oil and natural gas pipeline systems. The goal is to cause the shutdown of major export trunk lines via misinformation fed to the monitoring systems by our insiders.
    - Timing (in relation to Constitution Day) – 8-12 weeks out.
    - Resources needed – Inside contacts from Reconnaissance phase. People who have skills not only related to system software and operating systems, but who are familiar with the oil and natural gas industries and the technologies that are used in pipeline monitoring, diagnostics and control.
    - Details – The goal is to cause the companies themselves to shutdown the pipelines in response to events within our control. To do this effectively, we will need detailed information on the emergency and incident response procedures within each company in addition to control over the SCADA and intelligent pig systems.
        - Control of computer systems – This can happen in several ways and the best method would be determined at attack time. Options available are control via our insider's direct access to the systems, network attacks based on vulnerabilities in the networks supporting information collection and dissemination and attacks on the platforms on which the system software run. In both the Oil and Natural Gas Pipeline Systems and Internet Security Infrastructure Details sections, there are details as to what operating systems, software, and security measures we could exploit.
        - Emergency and incident response procedures – This information would be mainly available via our inside contacts.

        - Combination of the elements – With information of the above, we can design a series of events that would cause the companies to shutdown portions of their pipelines. For example, if we know the level of distress at which a joint welding is considered too dangerous for pipeline operations, we can configure the system to generate such a warning. Or, if we know that the pipeline is shutdown in response to malfunctions in the monitoring systems, we can generate the appropriate events necessary to cause such a reaction. We want to use the companies' emergency and incident responses against them. Also, given the vast nature of the pipeline systems, the time needed to check out problems can be a few days or more. If we create multiple events, spaced apart in terms of time and geography, we can significantly degrade the carrying capacity of the export pipeline systems. As with the attack on the power grids, our goal would be to appear coincidental rather than planned and overt.
    - More information needed – Detailed information on the emergency and incident response policies and procedures of both Transneft and Gazprom.

General issues to consider: Below are some issues to be considered in terms of the entire plan, not any specific phase.

- Illegitimate sources of information and access – Currently, our plan calls for mostly "legitimate" means of gathering information and obtaining access to systems. By "legitimate" we mean that as far as our targets are concerned, our people have a right to be where they are and have access to systems and information. However, it would be shortsighted of us not to use the vast illegitimate resources also available in Russia. Corruption and organized crime are prevalent within Russia and we should not ignore these sources of information.
- Redundancy – This is a key component to our plan. We are relying heavily on planted insiders. If a person changes their mind, it could be devastating to the entire plan. To this end we need to build redundancy into out teams and only tell each person what they are required to know. As few people as

possible should know the entire plan.  This will help protect the plan not only in the case of a double agent, but also if one of our team is discovered.

- Communications within the teams and to leaders – Plan for as little communication as possible once plan is in motion.  The more communication between team members, the more chances for discovery and the more evidence of a coordinated effort.

## Prevention and Countermeasures

**General** – One of the overall themes of our project was to use *systematic* weaknesses in Russia against the country itself. In addition to being very effective, this type of attack has the benefit of being very hard to prevent. For example, a major defense against our attack would be for Russia not to have a fragile economy that is reliant on its energy exports. It would also help if the country were not plagued by corruption and organized crime. Releasing the governmental control over Internet security and allowing companies to design systems that best suit their needs would be a huge help. However, all these situations do exist and to correct them will take a long time and a lot of resource effort on Russia's part. Our plan also relies on the use of insiders which, if done well, is difficult to detect and impossible to prevent. At the same time, there are things that our individual targets can do to help prevent the type of attack we have planned and described. They are listed below.

**Estimated cost of damage** – Taking an average price of $35 a barrel, if our plan could cut the carrying capacity of the oil export pipelines by 25%, we would cost Russia $40 million per *day* during the attack. Additionally, decreased consumer confidence which could result in loss of major customers which would increase those numbers. For natural gas and electricity, the numbers are harder to calculate (due to the differences in units in which the commodity is delivered and priced). However, our goal is to destabilize the Russian economy, which is very hard to put a price on.

**Phase I** – As mentioned above, traffic in Moscow is a nightmare and is another systematic problem of the city itself. In order to truly prevent an attack such as ours the city would have to either change the geography of the city (the river, the narrow, disorganized streets) or implement a public transportation system to relieve the congestion. The city is working on a public transportation system, but it will not be in effect for years to come. However, there are some things the city can have in place to prevent the impact of seemingly minor traffic accidents with the most important being policies and procedures in place to deal with such events. Response teams with highly trained personnel to attend to public safety and have traffic flowing normally as soon as possible will also help. The teams would need to be trained in the geography of the city

and know best how to reroute traffic.  Possible assistance from helicopters with a bird's eye view of the situation would also help.

**Phase II** –

Power Grid Operations

- Evaluate probabilistically how the grid responds to perturbations.
- Optimize grid designs and configurations to account for component reliability, parameter uncertainties, and cost/benefit trade-offs.
- Develop and implement analytical tools, hardware, and secure control software for a decentralized grid.
- Devise a plan to treat possible changes in the frequency and duration of disruption of generation or transmission.
- Identify of critical nodes and consequences and their interdependencies.
- Devise accurate models and tools of the power grid.
- Conduct research and development on robust, secure applications for electric power operations (including supervisory control and data acquisition systems and tools to detect and protect against malicious interference and disruptions)
- Develop a system to exchange important incident warnings.
- Assure service to critical facilities, such as nuclear power plants, medical facilities, and communication centers, while repairs or restructuring occurs.
- Understand accurately and fully the physical limitations and uncertainties of this multi-faceted and changing network.
- Conduct reliability assessments and simulations to maintain continuous and adequate flow of electricity from generation to distribution.
- Conduct security assessments to maintain the stability of the system following disturbances, such as multiple, simultaneous faults.
- Construct models and plans to take into account complex issues involving interactions between the electric grid and other infrastructures, such as banking, oil and gas, and telecommunications.
- Perform a cost and benefit analysis of security and protection options.
- Examine the interdependencies between the electric power grid and other infrastructures.

General

- Develop and review operational plans and procedures and ensure they are up-to-date, to include:
    A. Security, Threat, Disaster Recovery, and Fail-Over plans
    B. Other Operation Plans as appropriate, i.e., transmission control procedures
    C. Availability of additional security personnel
    D. Availability of medical emergency personnel
- Review all data and voice communications channels to assure operability, user familiarity, and backups function as designed
- Review fuel source requirements
- Ensure all gates, security doors, and security monitors are in working order and visitor, contractor, and employee access control are enforced.
- Create a relationship, assign a liaison, and establish frequent communications to law enforcement, medical emergency services, and other utility organizations.
- Develop emergency utility operations procedures.
- Ensure all personnel are fully briefed on emergency procedures.

Computer Security

- Develop an emergency plan for IT operations.
- Ensure all business critical information and information systems (including applications and databases) and their operational importance are identified.
- Ensure all points of access and their operational necessity are identified.
- Conduct education and training for users, administrators, and management.
- Ensure an effective password management program is in place.
- Conduct periodic internal security reviews and external vulnerability assessments.
- Conduct normal auditing, review, and file back-up procedures.
- Ensure effective virus protection scanning processes are in place.

- Confirm the existence of newly identified vulnerabilities and test and install patches as available.
- Periodically review and test security and operational plans and procedures and ensure they are up-to-date.
- Conduct internal security review on all critical systems.
- Review intrusion detection and firewall logs.
- Check cyber security communications for software vulnerabilities.
- Determine staffing availability for backup operations and provide notice.
- Consider increasing physical access restrictions to computer rooms, communications closets, and critical operations areas.
- Consider 7/24 emergency tech support staffing.
- Implement continuous 7/24 monitoring of intrusion detection and firewall logs.
- Implement continuous 7/24 monitoring of cyber security communications for latest vulnerability information. Contact software vendors for status of software patches and updates.
- Reconfiguring information systems to minimize access points and increase security.
- Reroute mission-critical communications through unaffected system.
- Disconnect non-essential network access.
- Have in place alternative modes of communication and disseminate new contact information, as appropriate.

**Phase III** – To protect themselves from an insider type attack like the one described in this document, the oil and natural gas companies can do several things. Protecting against insiders or bribed employees is very difficult, if not impossible. However, the company can mitigate its risks via several means. First of all, control the information that is to be published about sensitive systems. We were able to find press releases, case studies and whitepapers pertaining to the technology that monitors and maintains the pipeline systems of our target. If Transneft or Gazprom had stipulated (as part of the contract) that such detailed information not be published, our task would have been more difficult. In addition, both targets and their subcontractors publish job openings on their Web sites and it is easy to predict the kind of hardware and software the companies use based on the skills they are looking for in employees. Using a hiring agency instead

and not publicly publishing this information would have mitigated this risk. Inside the company, making sure that access to sensitive data and systems requires multiple people and authentication is a good idea. If it takes more than one person to access sensitive systems, it makes an illegitimate insider's job much more difficult for he or she cannot do anything without another employee watching.

## Appendix A:

"A New Twist in Russia's Yukos Oil Affair", The New York Times

---

Note: This article was found on-line and cannot be easily included in the electronic version of this document (it is, however, included in the hard copy). If you have received this document electronically and would like to view the article, it can be found at: http://www.nytimes.com/2004/04/16/business/worldbusiness/161ebedev.html.

## Appendix B:

Center for Technical Diagnostics, OJSC Transneft

---

Note: This article was found on-line and cannot be easily included in the electronic version of this document (it is, however, included in the hard copy). If you have received this document electronically and would like to view the article, it can be found at: http://www.transneft.ru/About/Subsidiaries/Article.asp?LANG=EN&ID=211.

## Appendix C:

Iconics Press Release

---

Note: This press release was found on-line and cannot be easily included in the electronic version of this document (it is, however, included in the hard copy). If you have received this document electronically and would like to view the press release, it can be found at: http://www.iconics.com/.

## **Appendix D:**
Volgasoft Case Study

---

Note: This case study was found on-line and cannot be easily included in the electronic version of this document (it is, however, included in the hard copy). If you have received this document electronically and would like to view the case study, it can be found at: http://www.volgasoft.com/case_studies/gas_pipelines/.

**Appendix E:**

Russian Oil and Natural Gas Industry Information: Pipeline Maps and Company Information


Oil and natural gas basins in Russia


Export pipelines, oil


Existing and planned export pipelines, natural gas

# Transneft Company Information

**President**
Simon M. Vainshtock
Chairman of the Administration, member of the Board of Directors, President of OJSC AK Transneft

**Board of Directors**
Simon M. Vainshtock,
Chairman of the Administration, member of the Board of Directors, President of OJSC AK Transneft

Anton V. Danilov-Danilyan,
Head of Economic Department of the Russian Federation President

Yuri M. Medvedev,
First Deputy Minister of the Russian Federation Ministry for Property Relations

Vladimir S. Stanev,
Deputy of the Russian Federation Energy Ministry.

Alexander V. Tikhonov,
Deputy Head of State Property Department of the Fuel and Energy Complex of the Russian Federation Ministry for Property Relation

Leonid A. Tropko,
First Deputy Minister of the Russian Federation Energy Ministry

Viktor B. Christenko,
Deputy Prime Minister of the Russian Federation

Andrei V. Sharonov,
First Deputy Minister for trade and economic development of the Russian Federation

Igor K Yusufov,
Minister of Energy of Russion Federation

**Contact information**:

Postal address**:** Russia, 119180, Moscow, Bolshaya Polyanka str., 57.
Telephones**:** (095) 950 81 78, 950 81 35.
Fax-server**:** (095) 950 89 00, 953 55 25.
e-mail**:** transneft@transneft.ru

# Gazprom Company Information

**Board of Directors**
Medvedev Dmitry Anatolievich
Chairman of the Board of Directors, Head of the Presidential Administration of the Russian Federation

Miller Alexey Borisovich
Deputy Chairman of the Board of Directors, Chairman of Gazprom's Management Committee

Ananenkov Alexander Georgievich
Deputy Chairman, Gazprom Management Committee

Bergmann Bruckhard
Chairman of the Management Committee of Ruhrgas AG

Gazizullin Farit Rafikovich
Member, Board of Directors

Gref German Oskarovich
The Russian Federation Minister for Economic Development and Trade

Levitskaya Alexandra Yurievna
First Deputy Head of the Administration of the Government of the Russian Federation

Sereda Mikhail Leonidovich
Head of Administration of Gazprom's Management Committee

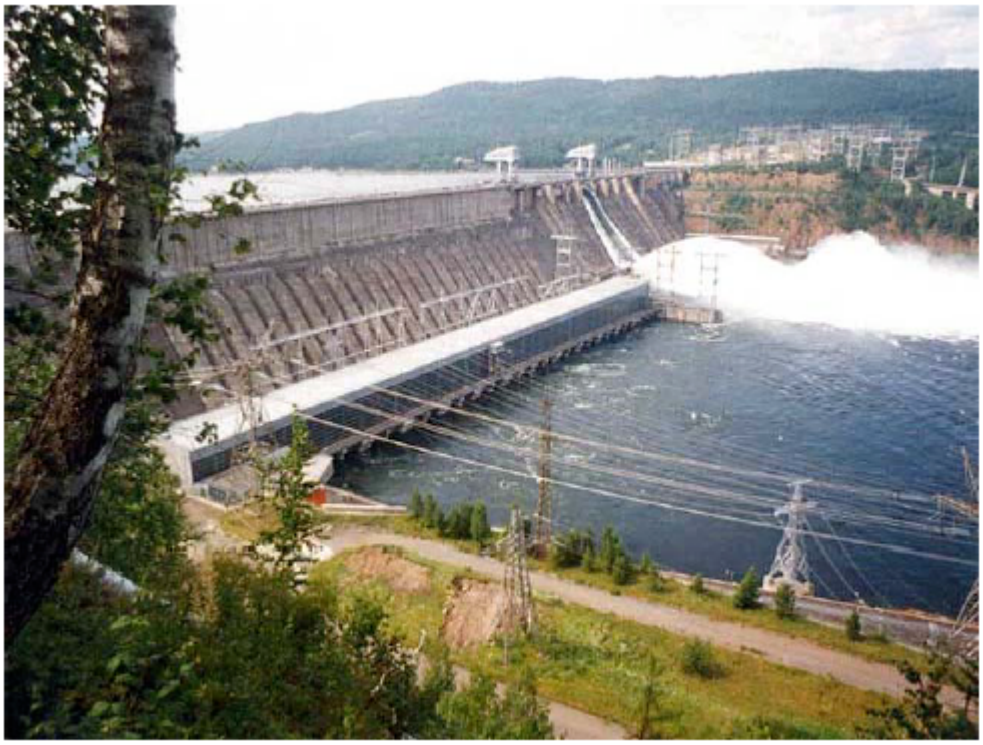
Fedorov Boris Grigorievich
Gazprom's Shareholder

Khristenko Viktor Borisovich
The Russian Federation Minister for industry and energy

**Contact information**

Mail address**:** 16 Nametkina St., 117997, Moscow, V-420, GSP-7
Tel**.:** +7 (095) 719-30-01 (for references)
Fax**:** +7 (095) 719-83-33, 719-83-35
Certificate of entry into the Unified State Register of Legal Entities:
Issued by the Moscow Department of the Ministry of Taxes and Fees of the Russian Federation on 07.08.2002; No. 1027700070518
INN**:** 7736050003
E-mail**: gazprom@gazprom.ru**

**Appendix F:**
Russian Electricity Industry Information: Charts, Photos, RAO UES Company Information



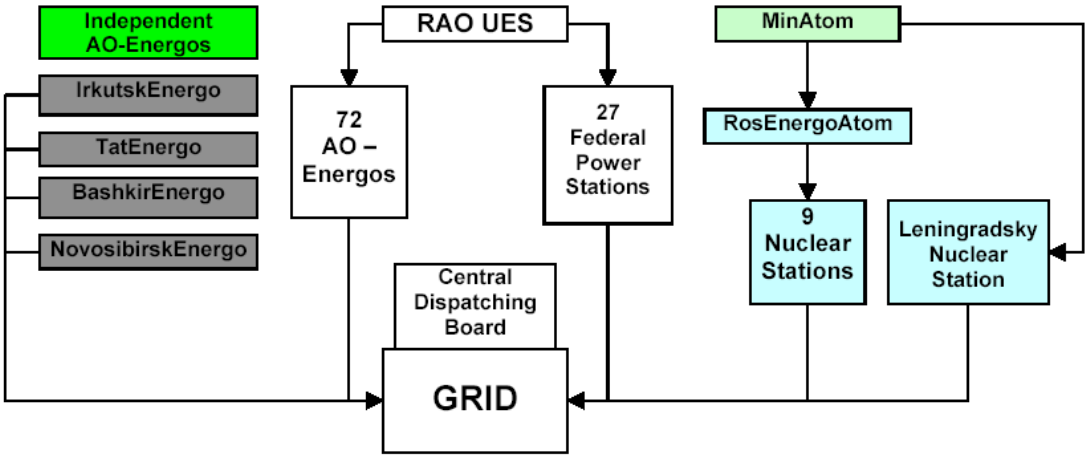



Figure 10: Organization Structure of Russian Power Sector

# RAO-UES Company Information

**Chairman of the Supervisory Board**: Alexander Stalievich Voloshin
**Chairman of the Management Board**: Anatoly Borisovich Chubais
**Deputy Chairman of the Management Board, Business and Economy**: Yakov Urinson
**Presiden**t: Leonid Viktorov

Trifonovsky tupik, 3
129272 Moscow
RUSSIA
Telephone: +7 095 788 0770
Fax: +7 095 788 0770

**Distributors:**
COMPULINK USP
Udaltsova str., 85, build.2
117607 Moscow
RUSSIA
Telephone: + 7 095 737 8866
Fax: +7 095 932 9853

FORS-SPb
Alexander Nevsky Str., 6, office 401
193167 St. Petersburg
RUSSIA
Telephone: +7 812 274 5747
Fax: +7 812 274 7098

Fors Holding
Trifonovsky tupik, 3
129272 Moscow
RUSSIA
Telephone: +7 095 787 7040
Fax: +7 095 787 7047

Infotrans
Polevaya Str., 47
443001 Samara
RUSSIA
Telephone: +7 8462 33 4979
Fax: +7 8462 32 3166

Microtest
Savvinskaya Embankment, 15
119435 Moscow
RUSSIA
Telephone: +7 095 787 2058
Fax: +7 095 787 2056
Bevalex

Partizansky prospect, 14a
220040 Minsk
BELARUS
Telephone: +7 017 249 9078
Fax: +7 017 249 4051
IBA
Bogdanovich Str, 155
220040 Minsk
BELARUS
Telephone: +7 017 210 1268

## Appendix G:

Tranceroute, DNS and whois Query Outputs

```
traceroute to www.gazprom.com (217.151.130.37), 30 hops
max, 38 byte packets
 1  leng (10.0.0.171)  0.538 ms  0.397 ms  0.353 ms
 2  er1.sea1.speakeasy.net (64.81.31.1)  13.251 ms  13.033
ms  11.398 ms
 3  210.ge-0-1-0.cr1.sea1.speakeasy.net (69.17.83.237)
11.177 ms  9.288 ms  9.554 ms
 4  border25s.g3-3.speakeasy-42.sea.pnap.net
(206.253.193.137)  9.497 ms  9.526 ms  10.076 ms
 5  core2.ge3-0-bbnet2.sea.pnap.net (206.253.192.194)
9.560 ms  9.377 ms  8.984 ms
 6  12.124.173.37 (12.124.173.37)  9.838 ms  11.071 ms
10.033 ms
 7  gbr1-p60.st6wa.ip.att.net (12.123.44.114)  9.594 ms
9.602 ms  10.040 ms
 8  tbr1-p012501.st6wa.ip.att.net (12.122.12.157)  12.358
ms  11.362 ms  13.875 ms
 9  tbr2-cl1.sffca.ip.att.net (12.122.12.113)  45.557 ms
72.457 ms  147.705 ms
10  ggr1-p3100.sffca.ip.att.net (12.122.11.230)  270.580 ms
28.335 ms  24.694 ms
11  sjo-bb1-pos0-3-3.telia.net (213.248.86.61)  29.204 ms
28.919 ms  29.332 ms
12  chi-bb1-pos3-2-0.telia.net (213.248.80.1)  75.778 ms
76.069 ms  76.815 ms
13  nyk-bb1-pos0-3-0.telia.net (213.248.80.154)  85.065 ms
85.210 ms  85.946 ms
14  kbn-bb1-pos2-1-0.telia.net (213.248.64.21)  164.840 ms
*  165.241 ms
15  s-bb1-pos7-0-0.telia.net (213.248.65.26)  179.884 ms
180.050 ms  180.425 ms
16  s-b4-pos12-0.telia.net (213.248.66.6)  179.890 ms
180.316 ms  179.363 ms
17  teliasonera-01842-s-b4.c.telia.net (213.248.78.246)
180.521 ms  180.446 ms  179.965 ms
18  192.130.130.145 (192.130.130.145)  189.871 ms  187.312
ms  187.353 ms
19  193.227.225.162 (193.227.225.162)  195.001 ms  195.575
ms  195.140 ms
20  spb1-p500.sonera.ru (217.74.128.214)  193.909 ms
193.932 ms  194.692 ms
21  mow1-000.sonera.ru (217.74.128.122)  206.434 ms
204.836 ms  204.746 ms
22  vxr.gazsvyaz.ru (217.74.128.30)  208.045 ms  207.622 ms
209.909 ms
23  * *
```

```
Trying "www.gazprom.com"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 25884
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 3,
ADDITIONAL: 3

;; QUESTION SECTION:
;www.gazprom.com.        IN   ANY

;; ANSWER SECTION:
www.gazprom.com.    86176     IN   A    217.151.130.37

;; AUTHORITY SECTION:
gazprom.com.        86176     IN   NS   ns1.gazsvyaz.ru.
gazprom.com.        86176     IN   NS   ns2.gazsvyaz.ru.
gazprom.com.        86176     IN   NS   ns.gazprom.ru.

;; ADDITIONAL SECTION:
ns.gazprom.ru.      86176     IN   A    217.151.130.34
ns1.gazsvyaz.ru.    86176     IN   A    217.151.128.34
ns2.gazsvyaz.ru.    86176     IN   A    217.151.128.35

Received 169 bytes from 127.0.0.1#53 in 1 ms



% This is the RIPE Whois server.
% The objects are in RPSL format.
%
% Rights restricted by copyright.
% See http://www.ripe.net/ripencc/pub-
services/db/copyright.html

inetnum:      217.151.128.0 - 217.151.131.255
netname:      GAZSVYAZ-MSK
descr:        Gazsvyaz Ltd
descr:        16, Namyotkina street
descr:        117884,Moscow, V-420
descr:        Russia
country:      RU
admin-c:      AS6100-RIPE
tech-c:       AP164-RIPE
tech-c:       II286-RIPE
status:       ASSIGNED PA
notify:       registry@gazsvyaz.ru
mnt-by:       GAZSVYAZ-RIPE-MNT
changed:      izotov@gazprom.ru 20030605
source:       RIPE
```

```
route:          217.151.128.0/20
descr:          Gazsvyaz Ltd
descr:          16, Namyotkina street
descr:          117884, Moscow, V-420
descr:          Russia
origin:         AS20576
notify:         registry@gazsvyaz.ru
mnt-by:         GAZSVYAZ-RIPE-MNT
changed:        izotov@gazprom.ru 20010702
source:         RIPE

person:         Anatoly Stepanov
address:        Gazsvyaz Ltd
address:        16, Namyotkina Street
address:        117884, Moscow, V-420
address:        Russia
phone:          + 7 095 719 35 88
fax-no:         + 7 095 719 34 44
e-mail:         A.Stepanov@gazprom.ru
nic-hdl:        AS6100-RIPE
mnt-by:         GAZSVYAZ-RIPE-MNT
changed:        izotov@gazprom.ru 20030605
source:         RIPE

person:         Ilya V Izotov
address:        Gazsvyaz Ltd
address:        16, Namyotkina Street
address:        117884, Moscow, V-420
address:        Russia
phone:          +7 095 719 35 60
fax-no:         +7 095 719 34 44
e-mail:         izotov@gazprom.ru
nic-hdl:        II286-RIPE
notify:         izotov@gazprom.ru
mnt-by:         GAZSVYAZ-RIPE-MNT
changed:        izotov@gazprom.ru 20010303
source:         RIPE

person:         Alexey A Polyakov
address:        Gazsvyaz Ltd
address:        16, Nametkina Street,
address:        117884, Moscow, V-420
address:        Russia
phone:          +7(095) 719 31 10
fax-no:         +7(095) 719 34 44
e-mail:         polyakov@gazprom.ru
nic-hdl:        AP164-RIPE
mnt-by:         GAZSVYAZ-RIPE-MNT
```

```
changed:        polyakov@gazprom.ru 20010305
source:         RIPE
```

```
traceroute to www.transneft.ru (212.73.97.101), 30 hops
max, 38 byte packets
 1  leng (10.0.0.171)  0.651 ms  0.421 ms  0.367 ms
 2  er1.sea1.speakeasy.net (64.81.31.1)  17.002 ms  61.922
ms  38.755 ms
 3  220.ge-0-1-0.cr2.sea1.speakeasy.net (69.17.83.233)
44.950 ms  38.290 ms  40.450 ms
 4  ge-5-1-440.hsa2.Seattle1.Level3.net (209.247.91.169)
21.712 ms  9.244 ms  9.488 ms
 5  ge-4-0-1.mp2.Seattle1.Level3.net (209.247.9.93)  9.811
ms  9.452 ms  15.084 ms
 6  so-0-0-0.bbr2.NewYork1.Level3.net (64.159.0.238)
89.942 ms  89.009 ms  187.223 ms
 7  ge-5-0-0.gar1.NewYork1.Level3.net (209.247.9.210)
142.875 ms  116.657 ms  114.578 ms
 8  65.59.192.14 (65.59.192.14)  158.776 ms  163.312 ms
237.457 ms
 9  bcr3.amd.cw.net (195.2.1.13)  288.488 ms  270.121 ms
300.334 ms
10  208.173.211.234 (208.173.211.234)  294.116 ms  288.974
ms  288.474 ms
11  208.173.216.1 (208.173.216.1)  289.694 ms  204.489 ms
182.175 ms
12  ycr1-so-1-0-0.Stockholm.cw.net (208.173.216.26)
191.737 ms  190.465 ms  190.578 ms
13  ycr2-so-2-0-0.Stockholm.cw.net (166.63.220.30)  190.987
ms  190.655 ms  189.498 ms
14  zcr2-so-0-3-0.Moscow.cw.net (166.63.220.50)  213.879 ms
212.076 ms zcr2-so-0-0-1.Moscow.cw.net (166.63.220.34)
212.128 ms
15  zar1-ge-1-3-0.Moscow.cw.net (208.175.234.134)  213.046
ms  212.710 ms  212.007 ms
16  cisco-f00.serial.oilnet.ru (212.73.96.4)  213.335 ms
214.987 ms  213.082 ms
17  * * *
18  * *


Trying "www.transneft.ru"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41663
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 2,
ADDITIONAL: 0

;; QUESTION SECTION:
;www.transneft.ru.       IN   ANY

;; ANSWER SECTION:
www.transneft.ru.   83831     IN   A    212.73.97.101
```

```
;; AUTHORITY SECTION:
transneft.ru.       83831     IN   NS   ns1.transneft.ru.
transneft.ru.       83831     IN   NS   ns.oilnet.ru.

Received 92 bytes from 127.0.0.1#53 in 1 ms



% This is the RIPE Whois server.
% The objects are in RPSL format.
%
% Rights restricted by copyright.
% See http://www.ripe.net/ripencc/pub-
services/db/copyright.html

inetnum:      212.73.96.0 - 212.73.97.255
netname:      SVYAZNEFT-NET
descr:        Join Stock Company "SVYAZTRANSNEFT"
country:      RU
admin-c:      AANB1-RIPE
tech-c:       AM82-RIPE
tech-c:       VIP10-RIPE
status:       ASSIGNED PA
mnt-by:       SVYAZTRANSNEFT-MNT
changed:      v.pokhodun@mail.oilnet.ru 20030319
source:       RIPE

route:        212.73.96.0/19
descr:        Svyaztransneft route object
origin:       AS12879
notify:       man@stn.oilnet.ru
mnt-by:       SVYAZTRANSNEFT-MNT
changed:      man@stn.oilnet.ru 20000526
source:       RIPE

person:       Andrey A Bobrovitch
address:      Lublinskaya 6
address:      Moscow 109390
address:      Russia
phone:        +7 095 179 60 58
fax-no:       +7 095 950 80 75
e-mail:       jsc.stn@stn.oilnet.ru
nic-hdl:      AANB1-RIPE
notify:       v.pokhodun@mail.oilnet.ru
changed:      v.pokhodun@mail.oilnet.ru 20030516
mnt-by:       SVYAZTRANSNEFT-MNT
source:       RIPE
```

```
person:       Alexander Myakishev
address:      6 Lublinskaya ul.
address:      Moscow 109390
address:      Russia
phone:        +7 095 171 8574
phone:        +7 095 174 2574
fax-no:       +7 095 179 6318
nic-hdl:      AM82-RIPE
changed:      v.pokhodun@mail.oilnet.ru 20030319
mnt-by:       SVYAZTRANSNEFT-MNT
source:       RIPE

person:       Victor Pokhodun
address:      6 Lublinskaya ul.
address:      Moscow 109390
address:      Russia
phone:        +7 095 950 8062
phone:        +7 095 174 2544
fax-no:       +7 095 9508075
e-mail:       v.pokhodun@mail.oilnet.ru
nic-hdl:      VIP10-RIPE
changed:      v.pokhodun@mail.oilnet.ru 20030319
mnt-by:       SVYAZTRANSNEFT-MNT
source:       RIPE
```

```
traceroute to www.tnk-bp.com (195.209.60.25), 30 hops max,
38 byte packets
 1  leng (10.0.0.171)  0.454 ms  0.361 ms  0.347 ms
 2  er1.sea1.speakeasy.net (64.81.31.1)  178.436 ms
163.369 ms  97.733 ms
 3  210.ge-0-1-0.cr1.sea1.speakeasy.net (69.17.83.237)
107.424 ms  71.559 ms  58.444 ms
 4  ge-5-0-340.hsa1.Seattle1.Level3.net (63.211.220.65)
38.110 ms  18.257 ms  11.770 ms
 5  ge-6-0-0.mp2.Seattle1.Level3.net (209.247.9.65)  22.378
ms  9.830 ms  26.271 ms
 6  so-2-0-0.bbr2.Washington1.Level3.net (209.247.10.130)
73.145 ms  83.567 ms  113.827 ms
 7  so-0-0-0.mp2.London2.Level3.net (212.187.128.133)
192.409 ms  148.633 ms  146.751 ms
 8  so-0-1-0.mp2.Stockholm1.Level3.net (4.68.128.70)
181.086 ms  181.949 ms  187.074 ms
 9  so-11-0.hsa2.Stockholm1.Level3.net (213.242.68.206)
182.884 ms  183.129 ms  182.098 ms
10  213.242.69.22 (213.242.69.22)  182.647 ms  181.909 ms
182.230 ms
11  se-ov.nordu.net (193.10.252.42)  181.082 ms  183.146 ms
181.840 ms
12  fi-gw.nordu.net (193.10.68.42)  189.166 ms  188.131 ms
186.756 ms
13  ru-gw.RUN.Net (193.10.252.146)  195.656 ms  194.886 ms
195.202 ms
14  gella-runnet.msk.RUN.Net.80.232.193.in-addr.arpa
(193.232.80.86)  204.723 ms  204.738 ms  204.174 ms
15  ZR-MG-2.garnet.ru (195.209.63.23)  205.098 ms  202.862
ms  204.367 ms
16  * * *
17  * * *
18  *

Trying "www.tnk-bp.com"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43184
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 3,
ADDITIONAL: 4

;; QUESTION SECTION:
;www.tnk-bp.com.              IN   ANY

;; ANSWER SECTION:
www.tnk-bp.com.          86256     IN   A    195.209.60.25

;; AUTHORITY SECTION:
tnk-bp.com.         86256     IN   NS   fire.tnk-bp.com.
```

```
tnk-bp.com.          86256     IN   NS   ns.demos.ru.
tnk-bp.com.          86256     IN   NS   ns1.demos.net.

;; ADDITIONAL SECTION:
ns.demos.ru.         86253     IN   A    194.87.0.9
ns.demos.ru.         86253     IN   A    194.87.0.8
ns1.demos.net.       26314     IN   A    195.133.0.8
fire.tnk-bp.com.     86256     IN   A    195.133.144.33

Received 183 bytes from 127.0.0.1#53 in 1 ms



% This is the RIPE Whois server.
% The objects are in RPSL format.
%
% Rights restricted by copyright.
% See http://www.ripe.net/ripencc/pub-
services/db/copyright.html

inetnum:      195.209.32.0 - 195.209.63.255
netname:      GARNET-2
descr:        Garant-Park-Telecom
descr:        Russia, Moscow, Leninskie Gory, 1,
descr:        building 75 G, block 6 Science Park of MSU
descr:        Moscow 119992, Russia
country:      RU
admin-c:      PAN-RIPE
tech-c:       PAN-RIPE
status:       ASSIGNED PA
notify:       panov@parkline.ru
mnt-by:       ROSNIIROS-MNT
changed:      Panov@parkline.ru 20030903
changed:      ip-dbm@ripn.net 20030905
source:       RIPE

route:        195.209.32.0/19
descr:        Garant-Park Delegated Block 2
descr:        Science Park, Moscow State University
descr:        Lenin's Hills, Moscow, Russia
origin:       AS5537
notify:       noc@parkline.ru
mnt-by:       AS5537-MNT
changed:      aes@park.ru 19961023
changed:      aes@park.ru 20010829
source:       RIPE

person:       Alexander V Panov
```

```
address:      MSU, Science Park, Garant-Park-Telecom
address:      Moscow
address:      Russia
phone:        +7 095 7898207
fax-no:               +7 095 9308800
e-mail:       panov@parkline.ru
nic-hdl:      PAN-RIPE
mnt-by:       PAN1-RIPE-MNT
changed:      panov@parkline.ru 20030314
source:       RIPE
```

```
traceroute to www.yukos.com (213.152.139.139), 30 hops max,
38 byte packets
 1  leng (10.0.0.171)  0.821 ms  0.433 ms  0.396 ms
 2  er1.sea1.speakeasy.net (64.81.31.1)  14.538 ms  11.337
ms  11.723 ms
 3  210.ge-0-1-0.cr1.sea1.speakeasy.net (69.17.83.237)
11.232 ms  8.771 ms  10.056 ms
 4  ge-5-0-340.hsa1.Seattle1.Level3.net (63.211.220.65)
10.143 ms  10.111 ms  9.551 ms
 5  ge-6-1-0.mp2.Seattle1.Level3.net (209.247.9.73)  9.075
ms  8.997 ms  10.094 ms
 6  so-0-0-0.bbr1.NewYork1.Level3.net (64.159.0.234)
122.656 ms  90.660 ms  227.565 ms
 7  ge-3-0-0.gar1.NewYork1.Level3.net (64.159.1.182)
257.074 ms  255.198 ms  162.192 ms
 8  65.59.192.14 (65.59.192.14)  89.142 ms  89.813 ms
90.012 ms
 9  bcr3.amd.cw.net (195.2.1.13)  168.676 ms  168.922 ms
168.124 ms
10  208.173.211.234 (208.173.211.234)  183.333 ms  182.632
ms  182.971 ms
11  208.173.216.1 (208.173.216.1)  183.719 ms  181.540 ms
182.139 ms
12  ycr1-so-1-0-0.Stockholm.cw.net (208.173.216.26)
190.747 ms  190.846 ms  190.625 ms
13  ycr2-so-2-0-0.Stockholm.cw.net (166.63.220.30)  190.631
ms  190.330 ms  190.080 ms
14  zcr2-so-0-3-0.Moscow.cw.net (166.63.220.50)  213.048 ms
212.952 ms zcr2-so-0-0-1.Moscow.cw.net (166.63.220.34)
212.564 ms
15  cable-and-wireless-internal-peering.Moscow.cw.net
(208.175.234.82)  212.742 ms  210.607 ms  210.876 ms
16  213.152.128.133 (213.152.128.133)  211.997 ms  248.019
ms  210.149 ms
17  * * *
18  *

Trying "www.yukos.com"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 34390
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4,
ADDITIONAL: 3

;; QUESTION SECTION:
;www.yukos.com.                IN   ANY

;; ANSWER SECTION:
www.yukos.com.      3525 IN   A    213.152.139.139
```

```
;; AUTHORITY SECTION:
yukos.com.          3525 IN   NS   ns.sibintek.net.
yukos.com.          3525 IN   NS   ns2.sibintek.net.
yukos.com.          3525 IN   NS   ns3.sibintek.net.
yukos.com.          3525 IN   NS   ns.yukos.ru.

;; ADDITIONAL SECTION:
ns.sibintek.net.    172725    IN   A    213.128.194.2
ns2.sibintek.net.   172725    IN   A    194.87.74.5
ns3.sibintek.net.   172725    IN   A    195.2.70.250

Received 185 bytes from 127.0.0.1#53 in 1 ms



% This is the RIPE Whois server.
% The objects are in RPSL format.
%
% Rights restricted by copyright.
% See http://www.ripe.net/ripencc/pub-
services/db/copyright.html

inetnum:      213.152.139.128 - 213.152.139.143
netname:      YUKOS-NET
descr:        yukos company net
country:      RU
admin-c:      SD5593-RIPE
tech-c:       SD5593-RIPE
status:       ASSIGNED PA
remarks:      Yukos network
mnt-by:       CWSVYAZ-MNT
changed:      auto-dbm@ripe.net 20020806
source:       RIPE

route:       213.152.128.0/19
descr:       CWSVYAZ
origin:      AS12976
mnt-by:      CWSVYAZ-MNT
changed:     Dmitry.Asmolov@cis.cwplc.com 20010428
source:      RIPE

person:       Serechenko Denis
address:      3th floor
address:      14, Ul. 8 Marta
address:      127083, Moscow
phone:        +7 095 797 9160
fax-no:       +7 095 797 9161
e-mail:       Denis.Serechenko@ionip.ru
```

nic-hdl:  SD5593-RIPE
changed:  sd@ionip.ru 20040210
source:  RIPE

## References


Alimov, Rashid. *Mayak's Power Supply Unsafe*. Bellona. September 2002.

Arvedlund, Erin E. "A New Twist in Russia's Yukos Oil Affair". *The New York Times*, 16 April 2004.

Balashak, James J., Alexander Radchenko, and Valentin Filkov. *A Glance at Russia's Power Sector*, Deloitte & Touche, May-June 2002.

Cheyne, Hilary and David Mor. *The Power Infrastructure*. Dartmouth College Computer Science. March 1999.

Gershwin, Lawrence K. *Written Statement for the Senate Special Committee on the Year 2000 Technology Problem*. 5 March 1999. National Intelligence Council, Central Intelligence Agency.

Graham-Rowe, Duncan. " Electricity Grids Left Wide Open to Hackers". New Scientist, August 2003. Available on-line from <http://www.newscientist.com>.

Krane, Jim. *Electrical Grid Vulnerable to Hackers*. September 2003. Available on-line from <http://www.crn.com>.

Law, Anne. RAO *Unified Energy System of Russia*. March 2004. Available on-line from <http://www.hoovers.com>.

Tatro, Marjorie. Electric Power Network Surety. Sandia National Laboratories.

Tober, Bruce. "Russian government quiet about its move towards Linux". NewsForge, 16 July 2002. Available on-line from <http://www.newsforge.com/os/02/07/16/1319244.shtml?tid=23>.

Central Intelligence Agency. (2003). *The World Factbook: Russia*.

Department of Energy. *Country Analysis Brief: Russia*. September 2003. Available on-line from <http://www.eia.doe.gov/emeu/cabs/russia.html>.

Institute for Traffic Care. Moscow Urban Traffic Project. (2002). Synopsis available on-line from <http://www.itctraffic.com/moskouENG.htm>.

U.S. Department of Commerce, International Trade Administration, Business Information Service for the Newly Independent States. (2000) *Russia's Pipeline System and Oil and Gas Transportation Projects*. Washington, D.C.: Mikhailov, Nick.

U.S. & Foreign Commercial Service and U.S. Department of State. (2003). *US&FCS Market Research Reports: Internet Security*. (International Market Insight ID 90704). Washington, D.C.: Lakaeva, Irina.

World Economic Forum. (2003). World Competitiveness Report 2003-2004.

Doctrine on the Information Security of the Russian Federation. Signed by Valdimir Putin, 9 December 2000. No. Pr-1895. Available on-line from <http://www.medialaw.ru/indep/en/d2-4.htm>.

Gateway to Russia. *Russia`s Power Engineering,* General Characteristics of the Power Industry and Its Components. April 2004. Available on-line from <www.gateway2russia.com>.

*General Description of RAO UES of Russia.* 2000. Available on-line from <http://www.rao-ees.ru/en/>.

*RAO UES-The Challenge Ahead*. Pan EurAsian Enterprises, Inc. April 2003.

"Russians sees big business, organised crime in charge: poll". *Johnson's Russia List*, 26 August 2003. Available on-line from <http://www.cdi.org/russia/johnson/7302-2.cfm>.

*Threat Alert System and Physical Response Guidelines for the Electricity Sector*. North American Electric Reliability Council. October 2002.

*Threat Alert System and Cyber Response Guidelines for the Electricity Sector*. North American Electric Reliability Council. October 2002.

"Vladimir Putin's Speech at the First Session of the Council Under the President for the Fight Against Corruption". *Johnson's Russia List*, 12 January 2004. Available on-line from <http://www.cdi.org/russia/johnson/8014-9.cfm>.