Communications of the Association for Information Systems

Volume 2 Article 10

August 1999

The Russian Federation's Y2K Policy: Too Little, Too Late?

William McHenry
Georgetown University, mchenry@msb.edu

Leonid Malkov
Cogitum, LC, lmalkov@aol.com


Communications of the Association for Information Systems

Volume 2, Article 10
August 1999

THE RUSSIAN FEDERATION'S Y2K POLICY: TOO LITTLE, TOO LATE?

William McHenry
The McDonough School of Business
Georgetown University
mchenryw@msb.edu

Leonid Malkov
Cogitum, LC

RESEARCH

THE RUSSIAN FEDERATION'S Y2K POLICY: TOO LITTLE, TOO LATE?

William McHenry
The McDonough School of Business
Georgetown University
mchenryw@msb.edu

Leonid Malkov
Cogitum, LC

ABSTRACT

In the first six months of 1999 the Russian Federation government instituted a wide range of policies related to fixing the Year 2000 Problem, culminating in an attempt to pass a Y2K Law, a Presidential Decree, and other governmental actions. Many systems are not expected to be fully remediated in time.

Drawing extensively on Russian sources, this paper outlines the evolution of government policies, gives an overview of the state of Y2K remediation as of July 1999, and outlines the key provisions of the government's policies. It is concluded that the Russian government's largely administrative approach to solving the Y2K problem is fairly ineffective and may lead to wider ranging consequences for the economic system as a whole.

Keywords: Year 2000 problem, Y2K, Russia, Russian Federation, cost, risk, remediation, government policy

"In my opinion, the Y2K threat is understood by the majority of managers at this level: 'Yeah maybe, somewhere, something will happen. But dear God let it miss me. Hopefully it will!' ... And if it doesn't miss us, we'll think up something. After all if it doesn't miss me, it probably won't miss everyone else. To drown together on the Titanic isn't so bad...." Vitaliy Fridlyand, 3Com Corp. [Algorithm Online, 1999].

I. INTRODUCTION

With just eight months left before January 1, 2000, the Russian government published a "National Plan of Action for Resolving the 'Year 2000' Problem in the Russian Federation" [Government Commission, 1999a]. This plan and a subsequent addition [Government Commission, 1999b], which includes some target dates, outline a comprehensive set of measures to address the problem. After a four-month delay, President Yeltsin signed a Presidential Decree in June 1999 about "Unavoidable Measures for Solving the Year 2000 Problem" [Federal Commission, 1999j]. The Duma published a draft for a Year 2000 Law, which passed its second and third readings on June 24, 1999, was approved by the Federation Council on July 2, 1999 [Federal Commission, 1999l], but was rejected by President Yeltsin on July 17, 1999 [Yeltsin, 1999b].

These plans and decrees come at a time when it appears that Russian government departments are badly lagging. Y2K work began in earnest only after a decree of the Kirienko government in May, 1998 [Russian Federation, 1998], and many governmental agencies began serious work only around the beginning of 1999. Experts such as Capers Jones assert that this kind of timetable would leave far too little time to ensure that all critical systems are fully remediated, fully tested, and tested in conjunction with other systems in time [Jones, 1998]. Estimates have been made that 30-50% of government systems will still contain Y2K errors on January 1, 2000 [Servocomp, 1999]. As many as 3-4,000 pre-1992 Soviet-era mainframe computers in Russia may have Y2K problems, many in the military-industrial complex [McHenry, 1999]. As recently as March, 1999,

the Gartner Group still ranked Russia with the least ready countries in the world, in the category that 66% of companies in the country will suffer at least one mission-critical failure, and there will be widespread, severe interruptions of government service; widespread, moderate power loss/brownouts, telephone and air transportation interruptions; and moderately distributed, severe interruptions of imports and exports [Marcoccio, 1999]. Indeed, the National Plan includes taking systems offline and replacing them with manual processing as one of three serious options, along with replacing the systems outright or modernizing them [Government Commission, 1999a].

How did the Russian Federation's government allow itself to get into this position? This paper examines the Russian government's early response, the magnitude of the problem, the state of remediation efforts, and policy initiatives as of July 1999. It focuses specifically on the Russian government's activities because highly important areas—the military, nuclear power and energy, telecommunications, and transportation—are still under governmental control. Studying the Y2K problem is interesting in its own right because of the potential catastrophic consequences if certain systems are not remediated on time. But since Y2K arose independently from any other social and political problems, it can serve as an isolated "test case" to understand the capacity of the Russian government, as it evolved, to make technology policy.

II. THE FIRST GOVERNMENTAL RESPONSES

The first known Y2K activity occurred in April 1996, when the President's Committee of the Russian Federation on Policies of Informatization (later absorbed into The State Committee on Communications and Informatization (Goskomsvyaz')), asked the Moscow "Integral" Scientific-Research Institute to study the scale of the problem and to prepare a plan of corresponding measures. At this time an inter-departmental conference was held, at which the attention of leaders of ministries and departments was drawn to the Year 2000 problem

[Bulgak, 1998]. This work apparently contributed to a presentation on the Year 2000 Problem in Fall 1997 to the Russian Federation Government prepared by the Ministry of Science with the participation of the Federal Security Service (FSB) and the Service of External Intelligence (SVR) [Bulgak, 1998]. A June, 1997 analysis of Goskomsvyaz' focused on the so-called "power" (defense and security-related) ministries, tax collection, customs, communications, transport, and banking [Ministry of Transport, 1999a]. The main thrust of this work was evaluating what security risks were posed by Y2K.

In January 1998, Vladimir Bulgak [1998], head of the Russian Federation Government Commission for the Y2K Problem until June 1999, claimed that Y2K work was going on in 32 executive organs, the Bank of Russia, and Sberbank (the citizen's savings bank). However, there was considerable skepticism about Y2K. The theme of exploitation by the West cropped up time and time again, both among computer professionals and government officials [McHenry, 1999]. Several officials, including Bulgak himself, expressed the opinion that the Y2K problem may be exaggerated and may be used as a means for Western companies to force upgrades and even technological dependence. (Bulgak continued to express a similar opinion well into 1999 [Federal Commission, 1999d]). When it was suggested towards the end of 1998 that the Russian and U.S. militaries should share early warning data and that the U.S. should help the Russians prepare for Y2K, one faction in the Russian military believed this effort to be nothing more than an attempt to infiltrate Russian systems [Felgenhauer, 1999]. Even in July 1999, Alexander Ivanov, the head of the State Committee for Telecommunications (Goskomtelekom, which replaced Goskomsvyaz' in June 1999), stated that in connection with the possible shipment of "a large quantity of special and different computer technology" in October 1999 from the West, an attempt of Western "special services" to enter computer systems and networks of Russian governmental and defense-related ministries "is not excluded" [Gazetta.ru, 1999]. Views like these and a widespread belief that Russia's computers were "too young" to have the Y2K problem resulted in little initial work [McHenry, 1999] .

It was not until Prime Minister Kirienko signed the “Order of the Russian Federation Government of May 30, 1998 No. 671-r” that the way was opened for intensive work on the Y2K problem. Goskomsvyaz’ was made the lead governmental agency [Russian Federation, 1998]. Goskomsvyaz’ issued an order in June 1998 which included plans to draw up an inventory of all computers owned by federal and regional bodies to see to what extent they were vulnerable to the problem. A training center was to be established and a testing and certification system worked out. The cost of the program had yet to be established but was estimated at between $100-$500 million. At this point Goskomsvyaz’ was already saying the Y2K problem could not be fully resolved in time. Typical guidelines were issued for making inventories. Working groups were organized in many organizations at many levels to start addressing the problem. Plans were expressed (but apparently never realized) to create a public-private partnership called “Informatika 2000" [Afonina, 1998]. Some evidence suggests that the high level attention given to Y2K at this time was partly a result of Western conversations with Kirienko and Yeltsin, and of activities of the American Chamber of Commerce in Russia and other Western firms [McHenry, 1999].

A very active period of Y2K work started at the beginning of 1999. On January 21 a Governmental Commission on the Y2K Problem comprising high-ranking, important governmental officials was formed [Russian Federation, 1999]. At least one national conference was held (April 19-20, 1999). Goskomsvyaz’ regularly released press releases, making new estimates of the size of the problem, and inaugurated a program to create a network of “centers of competency” to provide advice and remediation services.

III. MAGNITUDE OF THE PROBLEM

Several estimates have been made about the size of the Y2K problem in Russia and how much it will cost to fix it. In probably what was one of the earlier

estimates by the Gartner Group (when the price tag was still $300 billion worldwide), Russia was said to need to spend $12.8 billion vs. $74.6 billion in the US. Another estimate, by the Meta Group and Software Productivity Research, asserted that Russia would need to spend $32 billion, or 7.3% of 1996 GDP, to fix the Y2K problem. (The corresponding estimate by this group for the United States was $188 billion, or 2.5% of GDP) [Mordkovich, 1998].

Four months after Goskomsvyaz' head Alexander Krupnov proclaimed the cost to be $500M, a plausible explanation of how this number was calculated was advanced [Ministry of Transport, 1999b]. Because the government did not collect systematic data about computer technology used at governmental organizations, Goskomsvyaz' decided to adjust easily available U.S. data to the Russian situation using some coefficients. They started with information from the U.S. Senate that U.S. federal government spending will reach $4.7B. This amount was multiplied by three coefficients:

1. The infrastructure of informatization in the Russian government is equal to 25% of the informatization infrastructure of the US federal government.
2. Russian equipment is much more modern, yielding a savings of 30%.
3. Consolidation of efforts due to management by Goskomsvyaz' and large scale procurement provides another 40% savings.

The result according to Goskomsvyaz' is equal (in billions): 4.7 * 0.25 * (1-0.3) * (1-0.4) = 0.49. This is the $500M mentioned by Goskomsvyaz' officials.

Krupnov later increased his estimate to $1.5-3B, which "... [wa]s a concrete calculation of expenditures based on data received from enterprises. The variability of the numbers is impressive—from $150 million for the Ministry of Fuel and Energy to $125,000 for the Federal Border Service" [Y2K Problem, 1999]. It is possible again to break down the estimate using other published estimates.

The hardware and systems software cost of replacing all the old mainframes was said to be $400 million. Bulgak said that 15% of PCs needed to be replaced in the government. Applying that ratio across the board and

assuming about five million PCs in Russia, then 750,000 PCs would need to be replaced [McHenry, 1999]. At a cost of $600 each, that would be about one-half billion dollars. So it is possible that hardware replacement could cost $1B.

The aggregated data, published between February and June 1999, do not particularly add up. Using a conversion rate of 24 rubles to the dollar, and adding up estimates for transportation, telecommunications, energy, the Central Bank and Sberbank, executive departments, the defense-related ministries, and a few other ministries, the cost is as much as $834M. Goskomsvyaz' has continued to publicize $1-2B, although another more recent estimate from June 1999 says it will be $471M [Federal Commission, 1999i]. In July 1999, the new head of the State Committee on Telecommunications stated that $541M will be needed, of which $83M has already been spent [Gazetta.ru, 1999].

If the cost really is $2B, it is a staggering percentage of the budget and GDP. The total planned expenditures in the budget for 1999 were 575.46 billion rubles, less than $25 billion dollars at the rate of 24 rubles to the dollar. Could $2B be found when the overall budget is little more than ten times larger? Even $1B, or 4% of the total budget, is a staggering amount.

In addition, the GDP of Russia in 1998 was 2684.5 billion rubles according to official data, or $112B at the same rate of exchange. Fixing Y2K would cost 1.8% of GDP. Krupnov's original high-end estimate was $3B, or 2.7% of GDP. This estimate is almost the same as the percentage of GDP needed for the Y2K problem for the US economy. Might the $2-3B estimate also be based on foreign data? [Mordkovich, 1998].

These data are sufficiently murky as to leave considerable doubt about the true need for remediation. At some points it was unclear whether the $1.5-3B referred to the government or the economy as a whole. It is conceivable that the highest estimates were made to attract foreign investment [Russia also prepares,1999]. If this is the case, little was achieved. It is possible that the high figures were all based on replacing entire systems rather than trying the longer and possibly more arduous path of remediation. Clearly, resources for complete replacement will not be found.

IV. THE STATE OF AFFAIRS AS OF JULY 1999

It is impossible in a paper of this length to cover all areas of the Russian economy. We start with an overview and then discuss some selected cases.

OVERVIEW

Readiness of Ministry of Defense systems was said to be 22% at the end of February 1999 [Federal Commission, 1999a]. At the beginning of March, 1999, Bulgak stated that "computer systems of all higher organs of power, the defense-complex departments, and also key industrial and bank structures (The Russian Energy System, The Gas Ministry, The Bank of Russia, Aeroflot) are only at 10-12% readiness for solving the tasks that are arising" [Demos, 1999]. At the end of March 1999, only three percent of ministries and departments had completed remediation work [Federal Commission, 1999d], although 80% had created hardware and software inventories [Federal Commission, 1999e]. By April 14, Bulgak asserted that governmental readiness had reached 30% [Federal Commission, 1999g]. On the eve of the World Bank-sponsored Y2K conference in April in Moscow, state organs were finishing their inventories and concluded that about 30% of systems required priority correction or replacement.

During the first months of 1999 the government remained firm that the large bulk of resources would have to be found by entities themselves. No funds were allocated for 1999 Y2K work in the 1998 budget law. By March 1999 only a few of 72 Russian ministries and departments had presented calculations to the Ministry of Finance of needed Y2K resources [Federal Commission, 1999b], and 34 ministries and departments had not presented Y2K plans. Fifteen ministries and departments were ultimately allowed to request State budget funding, but only three had sent in their requests. Among those who had not were the KGB-successor Federal Security Bureau (FSB), the Federal Agency for Government Communications and Information (FAPSI), the Ministry of Defense, and the

Ministry of Internal Affairs (MVD) [Federal Commission, 1999c]. At the end of May 1999, an extension was being arranged because these requests still had not been made [Federal Commission, 1999i]. Among this group was the Ministry of Emergency Situations (MChS), although it did approve a center of competency in March 1999. Finally in July 1999 it was announced that the Ministry of Defense will receive $20M, of which $10.7M had yet to be found. The Ministry of Internal Affairs will be given $6M. The Finance Ministry prepared a draft of a law which will reallocate "above plan" state budget income to the Y2K problem. This Ministry also plans to open up a $50M line of credit for a large purchase of computer equipment abroad, starting in October 1999 [Gazetta.ru, 1999].

In the industrial sector, by April 1999, 500 systems needing remediation were discovered that involved dangerous, ecologically harmful, or continuous production [Federal Commission, 1999h]. The most widely used domestic Supervisory Control and Data Acquisition (SCADA) package in Russia is TRACE MODE from Ad Astra. Ad Astra asserted that many older controllers that may be subject to the Y2K problem are still in use. Of about 3,000 installations of TRACE MODE, 37% were in electricity, 17% in chemicals, and 12% in oil and gas. At the end of February, a very small percentage of active TRACE MODE users had yet carried out comprehensive testing of their systems [McHenry, 1999].

In July 1999, the Fuel and Energy Ministry (which does not include nuclear energy) said it was 35% ready [“@” Daily, 1999]. In mid-July, readiness of the government as a whole was still pegged at 30% [Gazetta.ru, 1999]. In materials prepared in late July 1999 for a meeting of the Goskomtelekom, 152,200 computer systems were reported operating in Russian government ministries and departments, of which 30,300 are considered "critical," i.e. their failure could lead to "heavy consequences for the economic and social spheres" [Federal Commission, 1999p]. Goskomtelekom itself is now said to have 26,115 computer systems, of which 10,081 are considered critical. 8,551 require significant modernization, and it is already planned that 76 systems will be shut down to avoid possible dangerous situations. Six thousand systems perform functions

related to air and space flight, of which 960 are considered critical. Only 360 of these systems have yet been modernized [Federal Commission, 1999p].

In June 1999, Boris Pozin of the Russian systems integrator firm AyTi claimed that only 7-8% of leaders of large state enterprises and commercial firms had an idea of what the Year 2000 problem is, while other representatives of key Russian systems integrators felt that information was much more widespread, especially among lower level managers, and that work on remediation was underway. Valeriy Elizov of Novell felt that, although serious work is going on, little had changed since his November, 1998 Duma testimony. Organizations have been able to best address internal problems of PCs and local area networks. Few have been able to even address questions of interdependencies with other organizations, let alone dependencies on the electric power, gas, telecommunications, and other infrastructures [Algorithm Online, 1999].

LEGACY MAINFRAMES

In the Duma hearings of November 1998, testimony was given that the USSR produced about 15,000 mainframes during the Unified System program. This program lasted from about 1967 until 1991 and was primarily involved in building functional duplicates of the IBM S/360 and S/370 series.[1] Of these, 3,000 to 4,000 may still be running, despite the end of production in approximately 1991. Many are probably in the military-industrial sector. Given their relatively low processing power and the expense and difficulty of keeping them running, they must be handling some important functions. The last new release of an IBM-like operating system took place in 1987. The current chief designer of the main institute that had oversight of this program testified that, "I can reliably say that from a technical viewpoint starting from January 1, and certain operating systems starting from the following January-March, etc. simply will stop loading, if nothing is done with them" [Shmid, 1998]. Attempts were made to organize assembly of IBM mainframes in Russia to provide a migration

[1] See the following works for an overview of the achievements of the USSR in computing: [Davis & Goodman, 1978; Goodman et al., 1988; Goodman & McHenry, 1991; McHenry, 1985; McHenry & Goodman, 1986; Wolcott, 1993].

path for these users, apparently to little avail. Some operating system maintenance work continued at this institute, including the development in 1995 of emulator software allowing some tasks to be run under IBM's VSE/ESA architecture. Nevertheless, most users would have to jump several generations of technology to make use of new IBM mainframes, so even if it were possible to buy replacements for them, time is running out to finish all of the rest of the maintenance that would be needed [Mainframes in Russia, 1995]. Statements that the software can be ported in a matter of days and weeks do not seem realistic. In November 1998, Shmid was already recommending that enterprises start making plans to simply turn off systems using these mainframes.

AIRLINE AND TRAIN RESERVATIONS

Since the breakup of the USSR, Aeroflot was divided into a number of smaller and very small airlines. Plans to create a comprehensive, new airlines reservation system for the whole country were put on hold and then scaled back for lack of financing. It is now scheduled for completion in 2005. The existing system, called Sirena-2 as a whole, actually consists of more than 50 different versions. MS DOS PC-based terminal emulators which maintain compatibility with earlier Sirena versions go by the names of their authors, such as the Fedotov, Veytsman, and Zaytsev terminals. The system seems to be losing participants and generally breaking down. No single body is responsible for oversight of this system as was the case in Soviet times. The chances that the entire airlines reservation system will be working correctly after January 1, 2000 are slim. In February 1999 Aeroflot as a whole had only completed an inventory of 63% of its systems and had not yet defined the necessary financing for remediation [McHenry, 1999].

In contrast, the ministry responsible for train transportation (MPS) managed to survive numerous governmental reorganizations. MPS got started on remediating the reservation system, called Ekpress, in late 1997. By the time of the Duma Y2K hearings in November 1998, most of the 800,000 lines of code were reported checked and a windowing method applied. Testing was to be completed by February 1999. Even in this case the situation was complicated

because several separate organizations were in charge of various pieces of the software. Since the breakup of the Soviet Union, these organizations had difficulty surviving, and lost many of their best programmers [McHenry, 1999].

NUCLEAR POWER PLANTS

Of particular concern are the 29 reactors at nine nuclear power plants and other reactors. The Ministry of the Atomic Energy Industry (Minatom) has repeatedly asserted that primary control systems at the reactors are analogue and will not be subject to the Y2K problem [Federal Commission, 1999m]. Nevertheless, many of these plants used Soviet 2nd and 3rd-generation computers, some completely indigenous, which could present particular remediation problems if legacy software or even some of the systems themselves survived. It took programmers one month to get past a date-dependent password at the Kalinin plant, for example [McHenry, 1999]. Recent assessments by Westinghouse engineers who are working on upgrading the control systems at the several of the Chernobyl'-like plants (RBMK-1000) and the VVER-1000 plants are that the instrumentation and control (I&C) systems are close to or at the end of their useful life and need to be replaced. Some of that work is complete, but on-going upgrades could complicate Y2K efforts [McHenry, 1999]. The situation is considered serious enough that $1.5M was allocated through the US-funded Center for Science and Technology to aid domestic centers of competency and specific scientific groups to work on safety problems for nuclear plants, hazardous materials, and other emergency situations. Funds were first being distributed in May 1999 [International Science and Technology Center, 1999]. The U.S. Department of Energy is funding the use of remediation technology from Accelr8 Technology Corporation for nuclear plants in Lithuania, Ukraine, and Russia. The first training seminars were held at the end of July 1999 [Acclr8 Technology Corporation, 1999].

The Leningrad Nuclear Power Plant (LAES) posted to the web a preliminary inventory and analysis of computer technology subject to the Y2K problem. It uses PCs by Western firms such as HP, Compaq and IBM that are verified by the vendors, and pre-1996 PCs and Russian-assembled PCs that

must be checked individually (e.g. PCs from Acer purchased in 1995 [McHenry, 1999]]. Patches for common Microsoft software, Novell Netware 3.11 and 3.12, and HP-UX are easily accessible. These lower level tests are considered easy, but "there are difficulties with verifying information technology at the higher levels... The reason in our view—the significant labor intensity of verification.... Specialists must be assigned to organize this work or outside organizations must be hired. It does not appear to be possible to carry out this work, at a sufficient level, on the fly" [Garusov, 1999]. This report is dated 1999, but says that a more detailed inventory is still needed.

In addition, the report states that some older Soviet computers and microprocessors are still in use: the SM-1210; the 8080- and 8086-like microprocessors 580VM80, 1816VE31, 1810VM86, 1810VM87; and the V3-M. We know nothing about the latter, but suspect it may be related to an indigenous line of computers developed by the All-Russian Scientific Research Institute of Electromechanics (VNIIEM). The SM-1210 follows the line of HP minicomputers and probably went out of production about 1992. Some assembly language and Fortran routines are used on this machine. These computers show up in the section on systems for management of the reactors, probably for collection and processing of data, although use of acronyms in the report makes it difficult to know exactly what they do. A vibration monitoring system for the first and second reactors uses a 486DX4 computer. Other older software in use includes OS/2, Microsoft Fortran 77 V. 5, Borland C V. 4 and C++ V. 3.1, Clipper 5.2, and dBase. Obviously not all applications based on these machines are critical or have date dependencies, but most need to be checked and then remediation needs to be completed. The report makes no mention of work presumably being done by Westinghouse and its internal Russian partners to help upgrade the I&C systems at the plant [McHenry, 1999]. No one seems to think that the nuclear plants are in danger of exploding, but it is possible that, in the presence of other unforeseen conditions, Y2K problems could contribute to potential disasters.

SOFTWARE PIRACY

Another particularly daunting problem is software piracy for PC-based business software, which reached 92% in 1998 with a replacement cost of $273M [International Planning and Research Corporation, 1999]. Consider just the situation of Novell. Novell said in its November 1998 Duma testimony that 80-90% of all the information systems in Russia are based on one or another version of Novell Netware. They estimated 10-12,000 (government) servers running mostly Versions 3.11 or 3.12 of Netware, which are not compliant. The long-available patch is only available to legal users. From 300,000 to 500,000 state workers use Novell products, and from 30 to 80% of the users are not registered. Some of the worst offenders are the Ministry of Defense, the Ministry of Interior Affairs (responsible for enforcing the anti-piracy law), Minatom, the energy complex, and the tax organs. The logistics of shipping new versions of Netware, making the upgrades, adjusting other software, training users, upgrading hardware if necessary, and testing the whole system by January 1, 2000 are now becoming quite daunting. Novell does have some patches that do not require changing versions, but only for certain versions [McHenry, 1999].

One solution being pursued is to ask Western software firms to provide large discounts or even give away their new version. Some firms have refused, while others agreed [McHenry, 1999]. Pirated copies of upgraded versions may presumably be obtained, but users must be informed that the upgrade is necessary and then must find a suitable upgrade path that works in their environments. The centers of competency are probably engaged in certifying many more versions of software than might need to be done in the West, especially since beta versions may be distributed by software pirates along side “real” versions [Kolesov, 1997].

OUTSIDE MOSCOW

Characterizing the state of remediation in specific regions away from Moscow is difficult, but there is enough evidence to suggest that a number of regional governments got off to a very late start. Russia is divided into 88 administrative regions, known as oblasts, krays, republics, and okrugs.

Goskomsvyaz' itself said that "the regions" had done virtually nothing as of January 1999 [McHenry, 1999].

At the end of July 1999 the city of Moscow is estimated to need no less than $40 million to replace or modernize about half of its computers [Federal Commission, 1999o]. Although Moscow dominates computer usage, PCs may be found throughout the country. Consider, for example, Siberia and the Far East. One analysis of the demand for PCs in 1996 stated that sales in these areas would make up 25.8% of the approximately 1.3M PCs sold that year [McHenry, 1999]. In Novosibirsk, planning began rather early. A decree was issued in August 1998 in response to the Kirienko decree, and inventories were to be completed by the end of 1998. However, the government did not offer financing and testing was not scheduled until the fourth quarter, 1999 [In Novosibirsk, 1999; McHenry, 1999]. Six centers of competency were certified between March and May 1999. All banks were said to be working on it and would present official assurances of readiness by September 1, 1999 [Federal Commission, 1999k]. In the Altay Kray, two centers were certified by the regional government in March, 1999, and a two-week seminar for all administrative levels was being held at the beginning of April 1999 [Federal Commission, 1999f]. In Irkutsk, an "informatization week" was planned in February 1999 which included information about the Y2K problem [McHenry, 1999]. In Khabarovsk, two centers of competency were certified in March and one in June 1999, all affiliates of national systems integrator firms. The local Komp'yulink affiliate, although not a center, started offering BIOS and operating system services, but nothing for applications software, in February 1999 [Popov, 1999]. One center of competency was certified in Vladivostok in April 1999. In all, 24 centers of competency so far are certified by regional governments outside Moscow [State Committee on Communications and Informatization, 1999].

As another example, the St. Petersburg government ignored pleas to begin Y2K work until the May 1998 Kirienko decree. Between October and December 1998, seminars by Western firms helped raise awareness, and an unpaid Working Group on the Y2K Problem was formed under the mayor's office.

Eventually, in March 1999 a resolution was passed banning the sale of non-compliant hardware and software, and the city government allocated all of R300,000 ($12,500) to address the Y2K problem [A&G, 1999]. In June 1999 a partnership with Computerland/St. Petersburg was announced under which the firm would carry out a comprehensive audit of governmental computers in the Leningrad oblast, taking care of their "modernization." Members of Computerland/St. Petersburg will sit on the Y2K commission of Leningrad oblast [Ambar' Corp., 1999].

When McHenry visited St. Petersburg in December 1998, he found the following situation:

- The St. Petersburg city waterworks had only begun to evaluate the scope of the problem, although it asserted that the actual delivery of water did not depend on digitally controlled systems.
- The city electric utility (Lenenergo) had formed a working group and was also evaluating systems, claiming that, while there may be problems with billing, electricity will not be interrupted due to Y2K.
- The city organization in charge of data processing for social services was just getting started, and was confident that its own programmers could handle whatever challenges were presented by Y2K because of prior experience with other maintenance tasks.
- The computer center for the Northwest Railroad was actively seeking funds to replace about 1,000 PCs subject to Y2K problems. When asked what would happen if these systems are not replaced, a high ranking member of the staff stated: "Basically I do not believe [that this will happen]. We in Russia always somehow manage clenching our teeth, storing extra air in our lungs [to get out of the situation]. But if the situation would be like today, say in two weeks it would be Y2K, everything would stop, I guarantee you that" [McHenry, 1999].

As expressed in the epigraph to this paper, there seems to be a cultural predisposition (known as *avos*' in Russian) to rely on hope and fate, to think "our boys" we be able to pull off whatever needs to be done, to wait and see what

happens, and to not create contingency plans. Another frequently cited proverb in conjunction with the Y2K problem is: “Until the thunder peals, the peasant does not make the sign of the cross.” This was cited frequently during the St. Petersburg visit. The only organization at this time that seemed to have made substantial progress was in charge of front-office post office systems, where the level of automation was often moving data on a floppy disk, if that.

V. EXECUTIVE AND LEGISLATIVE POLICY INITIATIVES

Executive approaches to the Y2K problem consisted of

- designating Goskomsvyaz’ as lead organization,
- the publication of guidelines,
- the certification of centers of competency, and two recent additions:
- the publication of the National Plan to address the Y2K problem, and
- the Decree signed by Boris Yeltsin.

Legislative approaches included holding hearings and trying to pass a Y2K Law.

THE CENTERS OF COMPETENCY

One of the chief means used by the Russian government to address the Y2K problem is certifying so-called “centers of competency.” As reported on June 11, 1999, about 162 centers had been certified, mainly by Goskomsvyaz’ or oblast administrations. The most common service provided by the centers was providing information for dealing with hardware and systems software questions for Intel-based PCs and servers. About 23% of the centers provided support for mainframes, including older Soviet-era models. About 65% could handle network questions, and about 30% offered specialized services, sometimes specific to the type of software in a specific branch. As Table 1 demonstrates, certification began rather late, and peaked in March and April 1999. Private organizations dominate, comprising about two-thirds of those certified. More certifications will undoubtedly be made, and other organizations may also provide Y2K consulting,

although they have been called lacking in experience and necessary equipment [State Committee on Telecommunications, 1999].

Table 1. Certification of Y2K Centers of Competency by Month and Type reported as of June 11, 1999 [State Committee on Communications and Informatization, 1999]

	Dec-98	Jan-99	Feb-99	Mar-99	Apr-99	May-99	Jun-99	Total
State	0	9	7	14	11	3	3	47
Academia	0	0	1	1	3	3	1	9
Private	3	7	11	34	24	19	8	106

The greatest concentration of centers, 41%, was in the Moscow area, with 9% in St. Petersburg. Even by June 1999, only 51% (45) of the administrative regions in Russia had at least one certified center. Only nine regions, including Moscow, had more than three centers. Twenty-five regions had only one center. As Table 2 illustrates, the rate at which regions were added was rather slow, and about half of the regions represented did not get their center(s) certified until April, just 8-9 months before the deadline and well into the period when Y2K problems were already manifesting themselves.

Table 2**.** Number of New Regions Adding Center(s) of Competency by Month Reported as of June 11, 1999 [State Committee on Communications and Informatization, 1999]

Type	Dec-98	Jan-99	Feb-99	Mar-99	Apr-99	May-99	Jun-99	TOTAL	Percentage of ALL of this type
Kray	0	0	1	2	1	0	1	5	83%
Oblast	1	4	2	10	5	5	2	29	58%
Okrug	0	0	0	0	1	0	0	1	10%
Republic	0	1	1	1	1	5	1	10	45%
TOTAL	1	5	4	13	8	10	4	45	51%

One reason that these centers emerged rather slowly is that the original decree stated that they would have to be paid by their clients. Russian clients are not used to paying for consulting services, and have few funds to do so. Most want to rely on their own forces, not only because of cost but because they are considered to be far more trustworthy. Russian software firms themselves were seduced by the idea that, because of the relatively young age of most Russian computers, the problem would not be large. Another reason cited was the absence of qualified people, although Russian programmers were hired to do remediation work for Western firms. Apparently 20 invitations to foreign firms were sent to foreign computer firms working in Russia to set up centers of competency. Half refused outright. Novell, IBM, and Microsoft agreed, but have not yet done so officially [McHenry, 1999].

THE NATIONAL PLAN

At the end of March 1999 a "National Plan of Actions for Solving the Year 2000 Problem in the Russian Federation" was published by the Government Commission on Solving the Year 2000 Problem [1999a]. The nine areas of the plan cover

1. Y2K publicity,
2. cooperation with international bodies,
3. getting critical systems ready,
4. creating the proper legal and normative bases,
5. creating the needed organizational infrastructure,
6. creating methodological materials,
7. creating the technical infrastructure,
8. creating mechanisms for outside control of the readiness of critical systems, and
9. preparing contingency plans.

A supplement to the National Plan was published in May 1999 [Government Commission, 1999b], which is organized by these nine areas, listing similar tasks, and attaching time frames and responsible organizations. Some time

frames, however, are quite vague, e.g. January-December 1999, or have already passed.

Parts of the plan that have already been done suggest it was created and followed in principle before it was approved.[2] For example, it calls for "increasing the completion of the full creation of inventories and classifications of systems... and creating... plans which are broken down by basic life-important systems" (to be finished by April 1999) The list of especially critical systems must be made more precise (April-May 1999). It also says work on defining needed expenditures must continue, although without defining how allocated funds in the budget will be reallocated (to be done by May 1999). Trying to arrange for discounts for volume purchases of hardware and software was to be done in May-June 1999.

The plan says that pragmatism must be at the root of Y2K decision-making, eschewing ambitious plans that may come to fruition only with fortuitous circumstances. Its essence is taking existing personnel and redirecting their attention to solving this problem by creating all the necessary bureaucratic mechanisms to do so. It envisions:

- Setting up a system for collecting and processing data about the course of Y2K remediation in federal ministries and departments and other regional governmental units (to be collected monthly by Goskomsvyaz' and in the 2nd, 3rd, and 4th quarters of 1999 by the State Statistics Committee);
- setting up a system of certification for foreign and domestic hardware and software (March-May 1999);
- creating inter-branch and regional commissions to look after work in related branches and across regions (April-June 1999). In particular the supplemental plan contains a long list of departments and ministries that are to form cross-branch groups in May 1999;
- formation of oversight and control structures in staffs and working groups for verifying Y2K readiness of critical systems (March-May 1999);
- continuing the development of the system of centers of competency

[2] It was first expected at the end of February 1999.

(March-May 1999);

- the widespread creation of contingency plans (June 1999), and typical scenarios (August 1999);
- verifications of readiness of computer systems at all levels of the government, ministries and departments (July-October 1999);
- analysis and evaluation of these tests and ordering of additional work if needed (August-November 1999);
- and taking final decisions about what to do for avoiding catastrophes (September-December 1999).

Setting aside the fact that many of these measures are encountering delays, all of these national structures can only go so far when it comes to specific applications software. A spreadsheet or database program may be certified as Y2K compliant, but that does not prevent an organization from using two-digit dates in certain columns or creating a database interface with space for just two digits. The most difficult problem seems to be to compel organizations to actually do the needed work, requiring that the bureaucratic machines in ministries and departments create all the necessary orders and documents to get work going at all levels. The creation of these instructions is envisioned for May-September 1999. Ultimately this problem necessitated both a Presidential Decree and a Y2K Law.

THE PRESIDENTIAL DECREE

The National Plan calls for the creation of a Presidential Decree on Y2K. Expected at the end of March [Federal Commission, 1999d], it was finally signed on June 17, 1999. The Presidential Decree directs that "personal supervision [*kontrol*']" be established for enacting and realizing Y2K measures at all levels of the government, in local governments, in state organizations ("*fundy*") not financed by the government, in stock companies in which the government has shares, and in "other organizations." The Decree recommends that all key high governmental institutions such as the Duma and the Constitutional Court take necessary measures. It recommends taking measures in the banking sphere "all

the way to considering the question of revoking licenses" for banks that cannot show compliance. Measures are to be taken to ensure Russia fulfills its international obligations, and to prevent hardware and software from being brought into Russia that is not Y2K compliant. A report is to be given to the president in November 1999 about the state of affairs [Yeltsin, 1999a], a draft of which is to be ready by October 15, 1999 [Federal Commission, 1999n].

The National Plan's vision of a presidential decree and the decree ultimately signed by Boris Yeltsin differ in two main respects. First, the National Plan asks for a decree that gives the Presidential Commission (author of the Plan) the chief role as coordinator of all Y2K work throughout the government—however, this commission is never mentioned in the Decree! Of course, such powers were already granted the Commission in the order forming it in January 1999 [Russian Federation, 1999]. Second, the National Plan calls for assigning "personal responsibility [*otvetstvennost'*]" whereas Yeltsin only decreed personal supervision. At least as early as February, 1999, Bulgak said that heads of major ministries, the Central Bank, and other agencies are "to take under personal responsibility the management" of Y2K efforts [Russian Business Consulting, 1999]. Bulgak apparently issued an order, which may or may not be enforced, requiring managers of basic departments and the largest Russian companies to personally monitor the safe operation of their computer systems during the 2000 rollover [NTV, 1999]. Plans for the Decree, discussed at the end of March, also say it will include "personal responsibility" [Federal Commission, 1999d]. The Decree may therefore represent a backing away from attempts to impose personal responsibility on top officials. Given that it appears to be watered down, one wonders why it was ultimately needed, beyond the fact that it does do a few things that the Y2K law does not.

THE Y2K LAW

A Y2K law was first introduced at the end of March 1999, passed the first reading on June 4, 1999, was amended with comments from the government and individuals, including an Internet-based conference on it, and passed the second and final (third) reading on June 23, 1999. On July 2 the law was approved by

the Federation Council, and was expected to be signed soon thereafter by President Yeltsin [Federal Commission, 1999l]. The key provisions were:

- federal, regional, local agencies and those responsible for computer systems elsewhere are "obliged" [*obyazan*] to take the "necessary measures" to forestall negative consequences from Y2K;
- users whose rights and legal interests may be damaged must be informed of possible Y2K problems, and if those interests may be damaged, the government must be informed and crisis plans must be created and enacted; federal level bodies responsible for crisis must be informed if the Y2K problem could lead to dangerous or emergency situations;
- users may demand that providers present documentation about Y2K readiness;
- financing is to be done by owners themselves, but governments may also define financing within their scope of activity;
- computer system owners must present certification or a declaration of Y2K readiness, and systems without one of these may not be used by governmental bodies or used if the system impinges upon the rights and legal interests of citizens, legal persons, or the state; the government may define a list of these systems; declarations may be issued by the owners of the systems themselves and must be registered according to the law on certification of products and services;
- penalties are assigned in accordance with existing laws;
- the Y2K problem may not be seen as an "Act of God."

The final version of the law differed considerably from the original draft. The latter included a whole range of penalties, including up to three years in prison for carelessness leading to heavy consequences. These provisions were deleted, according to a participant in the process, because penalties were already covered by other laws [Barkin, 1999]. Provisions that banned producing or importing non-compliant hardware and software were deleted, as were tax and

tariff breaks for Y2K products and services. The scope of the act was broadened to include any computer system that could influence rights and legal interests of others. Making the law less definite left even more on the shoulders of the government, which was charged with creating the necessary additional documents and administering the law. According to the participant, most of the documents were ready [Barkin, 1999].

In late July 1999, this law was rejected by President Yeltsin. Yeltsin stated that the law took on responsibilities of the government, which violated principles of separation of powers. Y2K policy is already defined in two decrees [Russian Federation,1998 and Russian Federation, 1999]. It also allegedly included imprecise and vague definitions and provisions [Yeltsin, 1999b].

The absence of this legal framework reduced, if not crippled, motivation for carrying out Y2K work. Under the law, organizations would have been obliged to remediate, and a climate for sharing necessary information would have been created. In our view, the published governmental policies do not go as far as the law would have gone, and its rejection by Yeltsin leaves many unanswered questions.

MORE CHANGES IN GOVERNMENT POLICY

As this paper was being completed, the actors continue to change, although the administrative approach remains central. As noted in Section II, Goskomsvyaz' was replaced by Goskomtelekom and its head Krupnov is gone. The new Vice Premier of Russian Federation, Il'ya Klebanov, says that the Y2K problem will be solved by November 1999 and that "nothing terrible" will happen in Russia. Several commissions will be created to control the measures being taken to solve it [Federal Commission, 1999k]. These commissions may simply be continuations of those envisioned in the National Plan. In August 1999 all executive departments will be required to use a mandatory single form for reporting Y2K progress. Klebanov promised to carry out selected verification of Y2K readiness at strategically important economic entities, requiring them to prepare reports to the government [NTV, 1999]. He himself is obliged to report about Y2K readiness on a weekly basis to the head of the cabinet of ministers.

First Deputy Premier Khristenko, Minister of Finance Kas'yanov, and Minister of the Economy Shaloval'yanets are tasked with finding finances for Y2K repairs [Gazetta.ru, 1999]. FAPSI will now become involved in testing local telecommunications systems, which should raise the profile of remediation work considerably. In what is apparently a new order, issued by Goskomtelekom, the language of personal responsibility returned. Priority systems for remediation must be defined by August 15, 1999 [Federal Commission, 1999n]. The tenor and provisions of this order suggest that the State Committee on Telecommunications is repeating orders that were given six months earlier, implying that a number of departments did in fact do little during this time period.

VI. CONCLUSIONS

The evidence presented in this paper shows that the Russian government's response to the Y2K problem was indeed quite late. Every indication is that many systems will not be fully remediated and tested by the deadline of January 1, 2000. The intention to import $50 million of hardware in October 1999 is particularly worrisome [Gazetta.ru, 1999]. Three questions remain: has the response been too little, why did this happen, and what may the broader consequences be?

It is often claimed that Russia is less dependent on computers than the developed Western nations, and this is certainly true. The number of systems is fewer, and numerous old systems that were not needed or too expensive to run were simply turned off after the USSR was broken up [McHenry, 1999]. Those that survived and those that have been created recently, it may be argued, are there because they are really needed. Critical services, such as telecommunications, electricity, oil and gas, banking, and transportation all depend on computers, not to mention defense, intelligence, tax collection, elections, and a host of other governmental services. Their failure may cause some significant problems which in some cases may have noticeable economic

effects within Russia and repercussions abroad. The fact that Klebanov must now report on a weekly basis shows the level of governmental concern about these systems.

However, over the past few years Russia entered a state of almost permanent turmoil and economic disruption. GDP declined about 5% from 1997 to 1998, and economic upheaval ensued from the crash of the ruble in August 1998. Many employees have not received salaries for months and sometimes even years, debts between enterprises are extremely high, and it is expected that at least one quarter of Russian banks, including the largest from the top ten list may disappear within one year. It is asserted that the Russian military system is declining and is not providing reliable defense (in particular, satellite monitoring) due to the loss of many locations after the breakup of the USSR and the financial problems over the last 10 years. Four Prime Ministers have occupied the Russian White House since the U.S. Presidential Commission on Y2K started working.

In this economic and political context, it is understandable that investing in Y2K solutions could not be a very high priority. Fixing a bank's computers, for example, does not make sense when the bank itself may fall due to the economic crisis. In this sense it is possible that the "campaign" approach taken by the Russian government to focus higher and higher levels of attention on the problem as the deadline approaches may result in avoiding catastrophes, and so Russia will join the ranks of other countries that are saying that "nothing terrible will happen." This approach may work *in somewhat rough proportion* to the risks involved.

Of three possible approaches–legal, economic, and administrative–it is again understandable why the Russian government chose the third. The legal system in Russia is underdeveloped and commands little respect as a motivator for action. Passing Y2K legislation in developed countries with long-standing and uninterrupted legal traditions is contentious enough. In discussions about the proposed Y2K law (see www.algo.ru/law2000), participants raised the question of whether or not the purpose of the law was mainly to get the attention of

managers, or was it to be a “real” law that would be enforced. How could a manager given no resources to solve the Y2K problem be held responsible for solving it? The legal system provided little, if any, motivation for working on the Y2K problem.

The Y2K law also envisioned economic incentives to spur Y2K work in the form of eliminating tariffs for importing new hardware and software and tax breaks. However, the government could hardly afford to give up any revenue. The government did try to encourage the creation of a market of Y2K services. Towards the end of 1998 very few private firms were getting into Y2K remediation at all. By offering the preferred status as a “center” and directing that certain governmental systems be certified, the government was trying to supply incentives for work to be done. Indeed, although they emerged slowly and are not located everywhere, these centers are probably the government’s best achievement, since they are increasing the distribution of know-how, supplying software tools to test systems, and helping organizations create contingency plans. Issuing methodological materials, doing testing only once, etc. undoubtedly avoided much duplication of work. However, the effectiveness of this system was clearly diminished by rejecting Y2K law, which encouraged certification on a much broader scale.

The main thrust of the Russian governmental approach is administrative, not unlike a typical centralized campaign seen in Soviet times. An author for NTV recently saw this as an advantage, claiming: "...in spite of the wary opinions in the West, Russia fully realizes the seriousness of the Y2K problem and is ready to see it through to a successful conclusion. What's more, our country, well-known for the irrepressible bureaucratic ardor of the still present old Soviet mold, in some ways is even ahead of the whole planet in the solution of the Y2K problem" [NTV, 1999]. Unfortunately, even in Soviet times large scale campaigns could only go so far to solve economic and social problems. By their very nature, resources could only be concentrated on part of the problem. This is one of the reasons that widespread computerization failed to take hold in the 1970s and 1980s [McHenry, 1985]. Now, the motivators behind those campaigns of

resources and Communist Party discipline for individual managers are absent. Although numerous pronouncements were made about personal responsibility, the Yeltsin decree seemed to have weakened it. Once again, without resources, how can there be responsibility? It is therefore not at all surprising that the campaign approach is not working particularly well. Fixing the Y2K problem required early awareness and a sustained effort over many months for the systematic investigation of all systems and their internal and external dependencies, their repair, and their testing. Many systems may remain unfixed as January 2000 arrives.

Besides needing to clean up breakdowns that may occur due to Y2K problems, two more lasting impacts of Y2K need to be considered. The first is what Russia ends up with after all this work is performed. In Western countries it seems that in many cases, there will be a silver lining associated with the Y2K efforts: firms invested in newer hardware or software, improved the management practices in the I/S function, and upgraded entire systems, in some cases adding functionality [Kappleman, 1999]. New organizations were created that cut across traditional boundaries and may lead to more effective inter-sector and international contingency planning in the future. Russia will only get yet another set of "workarounds" that prolong the life of already obsolete systems. On the surface the result will be the same–no particularly huge catastrophes, we hope–but the Western method may create more wealth in the future while the Russian method may diminish it.

The second impact has to do with the government on a broader level. By resorting to administrative mechanisms, the government continues to be reactive, putting out the largest fires at the last minute. This approach is the institutionalization of "too little, too late." Rather than stemming from ignorance, inattention, incompetence, or disbelief, the government's failure with Y2K may stem from its inability to act decisively and effectively within the governmental system that now exists in Russia. It is beyond the scope of this paper to argue whether or not this outcome represents the psychological reactions of the older generation of managers or whether it is an inherent flaw in the structure of the

Russian government as it evolved. If the latter, then the most lasting impact of the Y2K problem may have little to do with computers per se, but may serve as an example of much broader failures in economic policy which still lay ahead.

Editor's note: This article was received on July 30, 1999 and was published on August 8, 1999.

ACKNOWLEDGEMENTS

Partial funding for this work was received from The Mitre Corporation. We thank the many Russians who gave numerous interviews over many years, including during the December 1998 research trip to St. Petersburg on this topic. We also thank members of the MOSAIC group, University of Arizona, whose careful studies of Eastern European computing over many years provided the backdrop for this work.

APPENDIX

CHRONOLOGY OF SELECTED KEY EVENTS

1996	April	Moscow "Integral" Scientific Research Institute tasked to study possible Y2K problems
1997	June 10	Goskomsvyaz' Order RF 10.06.97 No. 78 finances "Integral" work
	September	Russian Federation Government hears presentations by Ministry of Science
1998	January 20	Bulgak makes one of the first public statements about Y2K work in the government
	May 30	Russian Federation Government Order of May 30, 1998 No. 671-r signed by Prime Minister Kirienko opens way for intensive Y2K work, making Goskomsvyaz' responsible
	June 26	Goskomsvyaz' Order No. 107 "About the Organization of Work on Solving the Y2K Problem" includes guidelines for addressing the problem
	November 12	Yeltsin signs Order about Realization of Decisions of Birmingham G-7 meeting, including a paragraph instructing Goskomsvyaz' to report in two months on involving Russia in international Y2K measures
	November 19	Goskomsvyaz' approves two documents about Centers of Competence
	November 24	Russian Parliament (Duma) Hearings about Y2K
1999	January 22	Russian Federation Order No. 100-r creating Governmental Commission on Y2K signed by Prime Minister Primakov
	March 26	Governmental Commission on Y2K issues National Plan of Action for Resolving Y2K Problem
	End of March	Y2K Law introduced into Parliament

	May 18	Governmental Commission on Y2K issues additional measures relating to the National Plan
	June	Goskomsvyaz' reorganized into Goskomtelekom, Klebanov replaces Bulgak
	June 4	Y2K Law passed first reading
	June 17	Yeltsin signs Decree on Y2K
	June 23	Y2K Law passed second and third readings
	July 2	Y2K Law approved by upper chamber of Parliament
	July 17	Yeltsin refuses to sign Y2K Law passed by Parliament
	July	Goskomtelekom order requiring priority systems be defined by August 15, 1999

ACRONYMS

FAPSI	The Federal Agency for Government Communications and Information
FSB	The Russian Federation Federal Security Bureau
Goskomsvyaz'	The Russian Federation State Committee on Communications and Informatization
Goskomtelekom	The Russian Federation State Committee for Telecommunications
Lenenergo	Leningrad Oblast Energy Administration
MChS	The Russian Federation Ministry of Emergency Situations
Minatom	The Russian Federation Ministry of the Atomic Energy Industry
Minfin RF	The Russian Federation Ministry of Finance
MNTTs	International Science and Technology Center
MVD	The Russian Federation Ministry of Internal Affairs
NTV	Nezavisimoe (Independent) Television
Rosenergoatom	State Enterprise "Concern Rosenergoatom" (oversees 8 of 9 Nuclear Plants in Russia)
Sberbank	Russian Federation Citizen's Savings Bank
SCADA	Supervisory Control and Data Acquisition
SVR	The Russian Federation Service of External Intelligence
VNIIEM	All-Russian Scientific Research Institute of Electromechanics
Y2K	The Year 2000

REFERENCES

"@" Daily (1999, July 9) "Ministry Of Fuel And Energy Will Spend Around 2.5 Billion Rubles To Solve The Y2K Problem" (in Russian) *Archive of Daily News*, http://www.algo.ru/adaily/news.asp?ID=949 (current July 10, 1999).

A & G Information Services (1999, March 22) "St. Petersburg State Enterprises And Organizations Are Prohibited To Buy Computers And Software In Which The Problem Of The Year 2000 Is Not Solved" [Subscription News Digest] *St. Petersburg News* 10(300).

Accelr8 Technology Corporation (1999, August 6) “Accelr8 Provides Y2K Solution to Nuclear Power Plants in Former Soviet Union” Press Release, http://www.accelr8.com/pressrels/pr990806.html(current August 7, 1999)

Afonina, O. (1998, December 22) "Seminar on Russia's Y2k Preparedness." *BISNIS Country Reports,* http://www.iep.doc.gov/bisnis/country/9901y2k.htm (current July 7, 1999).

Algorithm Online (1999, June 24-30) "How Well Do Managers Of State Organs And Other Commercial Enterprises Understand The Possible Consequences Of The Year 2000 Problem?" (In Russian) *Question of the Week,* http://www.algorithm.ru/weekquest/Default.asp?ID=12 (current July 27, 1999).

Ambar' Corporation (1999, June 16) "Computerland/St. Petersburg, Government Of Leningrad Oblast, Y2K Problem" (In Russian). *Daily News from St. Petersburg*, http://win.ambar.spb.ru/spbnews/16_06_1999.htm (current July 28, 1999).

Barkin, A. (1999, July 5) Private Communication by E-mail.

Bulgak, V. (1998, January 20) About the Question of Deputy of the State Duma A. D. Vengerovskiy No. 2.12-18/1956 on 12/25/1997 (in Russian). Russian Federation State Duma 0258p-P8, http://www.year2000.ru/Archive/Duma/001.html (current July 1, 1999).

Davis, N.C. and S.E. Goodman (1978) “The Soviet Bloc’s Unified System of Computers”, *Computing Surveys* 10(2), pp. 93-122.

Demos (1999) "Year 2000 - Events, Facts, Commentaries (Archive)" (in Russian), http://castle.demos.su/Facts-arc.htm (current July 1, 1999).

Federal Commission for Securities of Russia (1999a, February 11) "RF Ministry Of Defense Finished Inventory Of Automated Military Systems" (In Russian) *Year 2000 Problem: News*, http://y2k.fcsm.ru/Education/News/9902/990211_5.html (current April 3, 1999).

Federal Commission for Securities of Russia (1999b, March 1) "Minfin RF Presents Proposal About Allocating Resources For Solving The Y2K Problem" (in Russian) *Year 2000 Problem: News*, http://y2k.fcsm.ru/Education/News/9903/990301_1.html (current March 2, 1999).

Federal Commission for Securities of Russia (1999c, March 10) "Federal Organs Of The RF Miss Deadlines For Collecting Data About Solving The Y2K Problem" (in Russian) *Year 2000 Problem: News*, http://y2k.fcsm.ru/Education/News/9903/990310_1.html (current March 12, 1999).

Federal Commission for Securities of Russia (1999d, March 26) "Draft Of The Decree About Responsibility For Solving The Y2K Problem Will Be Presented To The President" (in Russian) *Year 2000 Problem: News*, http://y2k.fcsm.ru/Education/News/9903/990326_6.html (current April 3, 1999).

Federal Commission for Securities of Russia (1999e, March 29) "Governmental Commission On Resolution Of Y2K Problem Has Next Scheduled Meeting" (in Russian) *Year 2000 Problem: News*, http://y2k.fcsm.ru/Education/News/9903/990329_3.html (current April 3, 1999).

Federal Commission for Securities of Russia (1999f, April 1) "In Barnaul Began A Regional Seminar On Solving The Y2K Problem" (in Russian) *Year 2000 Problem: News*, http://y2k.fcsm.ru/Education/News/9904/990401_5.html (current April 4, 1999).

Federal Commission for Securities of Russia (1999g, April 14). The Y2K Problem Is Being Resolved In Russia As It Should Be (in Russian) *Year 2000 Problem: News*, http://y2k.fcsm.ru/Education/News/9904/990414_2.html (current April 21, 1999).

Federal Commission for Securities of Russia (1999h, April 16) "Goskomsvyaz' And The World Bank Will Carry Out An International Y2K Conference In Moscow" (in Russian) *Year 2000 Problem: News*, http://y2k.fcsm.ru/Education/News/9904/990416_1.html (current April 21, 1999).

Federal Commission for Securities of Russia (1999i, June 2) "The Pace Of Fixing The Y2K Problem Is Russia May Slow Down" (in Russian) *Year 2000 Problem: News*, http://y2k.fcsm.ru/Education/News/9906/990602_1.html (current June 5, 1999).

Federal Commission for Securities of Russia (1999j, June 22) "Boris Yeltsin Signed An Order About Unavoidable Measures For Solving The Year

2000 Problem" (in Russian) *Year 2000 Problem: News*, http://y2k.fcsm.ru/Education/News/9906/990622_1.html (current July 1, 1999).

Federal Commission for Securities of Russia (1999k, June 24) "The Y2K Problem Will Be Solved In Russia By November Of This Year - I'lya Klebanov" (in Russian) *Year 2000 Problem: News*, http://y2k.fcsm.ru/Education/News/9906/990624_3.html (current July 3, 1999).

Federal Commission for Securities of Russia (1999l, July 2) "The Federation Council Approved The Law On Preventing The Breakdown Of Computer Systems Due To The Y2K Problem" (in Russian) *Year 2000 Problem: News*, http://y2k.fcsm.ru/Education/News/9907/990702_1.html (current July 7, 1999).

Federal Commission for Securities of Russia (1999m, July 26) "Breakdowns Of Computers At Nuclear Power Plants On The Night Of January 1 2000 'Will Not Happen' - 'Rosenergoatom'" (in Russian) *Year 2000 Problem: News*, http://y2k.fcsm.ru/Education/News/9907/990726_3.html (current July 28, 1999).

Federal Commission for Securities of Russia (1999n, July 27) "State Agencies Of The Russian Federation Define Priority Systems For Solution Of Y2K Problem" (in Russian) *Year 2000 Problem: News*, http://y2k.fcsm.ru/Education/News/9907/990727_3.html (current July 30, 1999).

Federal Commission for Securities of Russia (1999o, July 28) "Moscow Should Spend No Less Than $40 Million To Solve The Y2K Problem" (in Russian) *Year 2000 Problem: News*, http://y2k.fcsm.ru/Education/News/9907/990728_1.html (current July 30, 1999).

Federal Commission for Securities of Russia (1999p, July 28) "Every Fifth Computer In Russian Federation State Structures May Produce Errors In The Year 2000" (in Russian) *Year 2000 Problem: News*, http://y2k.fcsm.ru/Education/News/9907/990728_2.html (current July 30, 1999).

Felgenhauer, P. (1999, February 18) "Defense Dossier: Brass Cool Over Y2K Heat", *The Moscow Times*.

Garusov, Yu.V. (1999) Report. Results Of Inventory And Preliminary Verification Of Information/Computer Technology Of The Station For Y2K Readiness (in Russian) Main Server, Branch Network of the Ministry of the Atomic Energy Industry (Minatom), http://hp.x-atom.ru/y2k/laec/otch_laes.html (current July 8, 1999).

Gazetta.ru (1999, July 12) "Klebanov Will Report Weekly On Y2K Problem" (in Russian) *Daily News* http://www.GAZETA.ru/daynews/12-07-1999/502000_Printed.htm (current July 27, 1999).

Goodman, S.E., et. al. (1988) *Global Trends in Computer Technology and Their Impact on Export Control*, Washington, DC.: National Academy of Sciences Press.

Goodman, S.E. and W.K. McHenry (1991) "The Soviet Computer Industry: A Tale of Two Sectors," *Communications of the Association for Computing Machinery* 34(6), pp. 25-29.

Government Commission for the Solution of the Year 2000 Problem in the Russian Federation (1999a, March 26). The National Plan of Action for Resolving the 'Year 2000' Problem in the Russian Federation. Protocol No. 2 (in Russian), http://www.ptti.gov.ru/gk-doc/2000/natplan.doc (current August 7, 1999).

Government Commission for the Solution of the Year 2000 Problem in the Russian Federation (1999b, May 18). Plan of Measures for Realizing 'The National Plan of Action for Resolving the Year 2000 Problem in the Russian Federation.' Protocol No. 3. (in Russian), http://www.ptti.gov.ru/gk-doc/2000/mainplan.doc (current August 7, 1999).

Kappleman, L.A. (1999) "Year 2000: A Reality Check" *Communications of AIS* 2(1), http://cais.isworld.org/contents.asp (current July 29, 1999).

"In Novosibirsk A Conference On The Y2K Problem Was Held" (in Russian) (1999, June 2) *FIS-Kur'er*, http://www.rbc.ru/fisnews/archiv/all/1999/06/02/120026.html (current July 6, 1999).

International Planning and Research Corporation (1999). *1998 Global Software Piracy Report*, http://www.bsa.org/statistics/GSPR98/ (current July 9, 1999).

International Science and Technology Center (1999) "MNTTs Offers $1.5M In The Framework Of A New Program For Questions Of Safety Connected With The Y2K Problem" (in Russian), http://www.istc.ru/istc/website.nsf/fm/Y2K+Ru (current July 7, 1999).

Jones, C. (1998). *The Year 2000 Software Problem.* New York: ACM Press.

Kolesov, A. (1997, July-August) "Computer Piracy - History and Current Status" (in Russian) *Computer and Life*, 20-26.

"Mainframes in Russia: from ES EVM to ES/9000" (in Russian) (1995) *Computerworld Moscow* 30, http://infoart.irkutsk.ru/it/press/cwm/30_95/mainf.htm (current Feb 20, 1999).

McHenry, W.K. (1985). The Absorption of Computerized Management Information Systems in Soviet Enterprises. Ph.D. Dissertation, University of Arizona.

McHenry, W.K. and S.E. Goodman (1986) "MIS in USSR Industrial Enterprises: The Limits of Reform from Above", *Communications of the Association for Computing Machinery* 29(11), pp. 1034-1043.

McHenry, W.K. (1999, March 2). *The Year 2000 Problem in Russia*. Unpublished Mitre Corporation Report, 210 pp.

Ministry of Transport of the Russian Federation (1999a, January 20) "History of the Issue in the Russian Federation" (in Russian), http://www.mintrans.ru/MCC/P2000/sem02.asp (current July 2, 1999).

Ministry of Transport of the Russian Federation (1999b, January 20) "Evaluation of Expenditures for Solving the Year 2000 Problem in State Information Systems" (in Russian), http://www.mintrans.ru/MCC/P2000/sem04.asp (current July 2, 1999).

Marcoccio, L. (1999) Year 2000 International State of Readiness. March 5, 1999, Expert Testimony to the U.S Senate Special Committee on the Year 2000 Technology Problem, Washington, D.C., http://www.gartner.com/public/static/y2k/y2k0399.pdf (current June 13, 1999).

Mordkovich, O. (1998, July) "Y2K Problem" (in Russian) *For the Director of the Information Department. Computerworld Russia,* http://koi.www.osp.ru/cw/cio/1998/07/04.htm (current February 15, 1999).

NTV (1999, July 7) "On The Edge Of The Millennium Russia Must Solve The So-Called Year 2000 Problem" (in Russian) *Interactive News on the Server YKT.RU*, http://www.optilink.ru/news/070799/ntv.htm (current July 28, 1999).

Popov, M. (1999, March 12) Private Communication by electronic mail.

"Russia Also Prepares For The Year 2000" (in Russian) (1999) *Ural Informatika* 1, http://2000.ur.ru:8080/press/10.html (current July 27, 1999).

Russian Business Consulting(1999, February 9) “Vladimir Bulkav Had A Seminar Devoted to Verifying The Readiness of Computer, Microprocessor And Other Systems For The Year 2000” (in Russian). *Archive of Economic News*, http://www.rbc.ru/news/archiv/econom/1990/02/09/news19990209190149.html (current February 15, 1999)

Russian Federation (1998). About Avoiding The Negative Consequences In The Operation Of Governmental Information-Computing Systems In The Russian Federation. Order Of The Government Of The Russian Federation Of May 30, 1998 No 671-r (in Russian), http://y2k.fcsm.ru/Official/Doc_Gov/ras300598.html (current July 1, 1999).

Russian Federation (1999). Policy About A Governmental Commission For Solving The Year 2000 Problem In The Russian Federation. Order of the Government of the Russian Federation of January 21, 1999, No 100-r (in Russian), http://y2k.fcsm.ru/Official/Doc_Gov/ras210199.htm (current July 1, 1999).

Servocomp (1999) From the Government's Point of View (in Russian), http://www.servocomp.ru/rus/g2000.htm (current Jul 2, 1999).

Shmid, A.D. (1998, November 24). Testimony. Parliamentary Hearings on the Year 2000 Problem, November 24, 1998, http://y2k.fcsm.ru/Official/Doc_Duma/ps241198.htm (current July 30, 1999).

State Committee on Communications and Informatization. Russian Federation (1998a, November 19). Standards for Centers of Competency on the Year 2000 Problem (in Russian), http://www.ptti.gov.ru/gk-doc/2000/cc_poloz.htm (current June 30, 1999).

State Committee on Communications and Informatization. Russian Federation (1998b, November 19). Recommendations on How to Recognize Centers of Competency for the Year 2000 Problem. (in Russian), http://www.ptti.gov.ru/gk-doc/2000/priznan.htm (current June 30, 1999).

State Committee on Communications and Informatization. Russian Federation (1999). List of Working Centers of Competency (in Russian), http://www.ptti.gov.ru/gk-doc/2000/zk2.doc (current August 7, 1999).

State Committee on Telecommunications. Russian Federation (1999). About The Use Of Accredited And Certified Means For Solving The Y2K Problem (in Russian), http://www.ptti.gov.ru/gk-doc/2000/komitet.htm (current July 6, 1999).

"Vladimir Bulgak Had A Seminar Devoted To Verifying The Readiness Of Computer, Microprocessor And Other Systems For The Year 2000" (in Russian) (1999, February 9) *Russian Business Consulting,* http://www.rbc.ru/news/archiv/econom/1999/02/09/news19990209190149.html (current February 15, 1999).

Wolcott, P. (1993). *Soviet Advanced Technology: The Case of High-Performance Computing*, Ph.D. Dissertation, University of Arizona.

"Y2K Problem: Struggle For The Best, Be Ready For The Probable" (in Russian) (1999, February) *ComputerWorld Russia* 05(165), http://www.osp.ru/cw/1999/05/11.htm (current February 12, 1999).

Yeltsin, B. (1999a). Decree Of The President Of The Russian Federation. About Measures That Cannot Be Put Off To Solve The Y2K Problem In The Russian Federation No. 194-RP (in Russian),

http://www.algo.ru/law2000/laws/president.asp (current July 1, 1999).

Yeltsin, B (1999b, July 17). Letter to the Chairman of the State Duma of the Federal Assembly of the Russian Federation G. N. Seleznev, No. Pr-930 (in Russian), http://www.algo.ru/law2000/laws/letter.asp (current July 27, 1999).

ABOUT THE AUTHORS

Leonid Malkov received his PhD in Economics from the Central Institute of Economics and Mathematics, USSR/Russian Academy of Sciences, where he was a senior project leader. He then joined ParaGraph International, one of the first private software firms in Russia, soon after it was founded. He now runs his own firm, Cogitum LC, in Reston Virginia, which specializes in consulting and the development of Internet software and content.

William McHenry is Associate Professor of MIS at the McDonough School of Business, Georgetown University. He has studied Soviet and Russian computing since 1978, publishing articles about hardware, software, networks, informatization policies, and the Internet in such journals as *Communications of the ACM*. He served on three National Research Council panels concerning aspects of Soviet computing and export control policies. He has also studied informational retrieval systems, the WWW search engines, and support systems for knowledge management. He may be found at http://www.msb.edu/faculty/mchenryw.