

Disclaimer

The views expressed are those of the
Author and not necessarily those of the
UK Ministry of Defence

RUSSIA AND THE MILLENNIUM BUG

The Millennium Bug problem (also known as the Y2K problem) which will affect computers when the date changes from 31 December 1999 to 1 January 2000 is global in nature, and will therefore affect all countries. It is clear, however, that some countries are better prepared than others, and that the Russian Federation can be placed in the group of the least prepared countries. In testimony before the Senate Armed Services Committee on 2 February, CIA director George J. Tenet drew attention to Russia's low level of preparedness and outlined some of the possible effects:

The lowest level of Y2K preparedness is evident in Eastern Europe, Russia, Latin America, the Middle East, Africa and several Asian countries, including China. Y2K remediation is underfunded in most countries.

Global linkages in telecommunications, financial systems, air transportation, the manufacturing supply chain, oil supplies, and trade mean that Y2K problems will not be isolated to individual countries, and no country will be immune from failures in these sectors. There is potential for civil unrest in some countries, particularly if critical service sectors are disrupted for extended periods. Energy flows could be interrupted in some countries. Europe, for example, gets more than one-third of its natural gas from Russia and could be affected if Gazprom has Y2K problems. Some military activities, including those of our allies, depend on the secure and uninterrupted flow of digital information, making overall readiness a potential casualty of Y2K.

The US Senate Committee on the Millennium Problem issued a report in March 1999. It repeated Tenet's claim that Russia was among the countries least prepared for Y2K. In one study, it was estimated that about two-thirds of Russian computer systems could experience some level of interruption after 31 December 1999. Another study estimated that it would cost \$32,246,348,750 to repair all software. This stands at 7.3% of Russia's 1996 GDP. By contrast, the comparable costs for the USA come to only 2.5% of 1996 GDP. In February 1999, the chairman of the State Committee for State Communications and Information Technology, Aleksandr Krupnov stated that it would cost Russia up to \$3 bn to prepare for Y2K. (The CIA has said that it is unaware as to how this figure was

reached.) Krupnov claims that Russian computer networks are now about 20% ready for Y2K.

Public discussion of the issue in Russia has, however, been minimal. While Russian society is much less reliant on computers and other processors than British or American, certain sectors are indeed vulnerable. In January 1999, it was announced that a Russian government commission, headed by deputy prime minister Vladimir Bulgak had been set up to deal with Y2K. Various ministries have been working on the Y2K problem, most notably the Ministry of Defence and Ministry of Atomic Energy.

IMPACT ON THE ARMED FORCES

The most common area of concern in the West is how Y2K might affect the command and control system for Russian nuclear forces. In early March 1999, the director of the 4th Central Scientific Research Institute of Russian MOD, Vladimir Dvorkin, stated that 30 units had been set up in the Strategic Missile Forces. They have inspected 134 various objects, of which 74 were regarded as being in a critical condition in relation to Y2K. Dvorkin estimates that the cost of rectifying this problem will be about R85 million. Dvorkin expects that final tests of all adjusted software will take place in October 1999.

The CIA is of the opinion that there is no danger of an unauthorized or accidental Russian missile launch due to Y2K problems. Russia may have Y2K problems in the early warning systems used to monitor foreign missile launches and at command centres. Problems within these systems could lead to incorrect information being transmitted, received or displayed or to complete system outages. The launching of missiles has nothing to do with the Y2K problem, because there is no date in the launch system, and launching is performed by a specific command. To minimise this risk, the Pentagon and Russian MOD have agreed to set up a joint research centre near Moscow where all information about launches of ballistic missiles and space rockets will be sent. A joint US-Russian defence Y2K coordination centre will be set up at NORAD in Colorado to share early attack warning information, thus preventing confusion should any Y2K related false warnings occur.

The environmental control systems of missile silos could be vulnerable to Y2K problems. Correct temperature and humidity levels need to be maintained within silos, and computers are often used for these purposes. Liquid-fuelled missiles in silos need to be monitored for fuel leakage, and computers are also used for these purposes and could be vulnerable to Y2K.

IMPACT ON GAZPROM

Y2K could have a significant impact on Gazprom, the main Russian gas company. Gazprom accounts for almost 50% of Russia's energy consumption, 15% of Eastern Europe's, and 5% of that of Western Europe. If Y2K causes Gazprom to shut down this could cause Russia, other former Soviet states and various states in Eastern Europe to suffer severe gas shortages. The CIA has identified several potential problems, of which some are:

- Soviet era mainframes are used in Gazprom's pipeline operations centres and are likely to be highly vulnerable to Y2K.
- Supervisory control and data acquisitions (SCADA) systems are used to monitor and control some operations. SCADA systems purchased before the late 1990s are likely to be Y2K vulnerable.
- Satellite ground stations used to transfer data from gas producing regions to Gazprom's headquarters may have Y2K problems.
- Unmanned equipment stations along remote Siberian sections of Gazprom's pipelines may rely on vulnerable embedded processors. These stations are used to relay communications and control pipeline valves. Compressor stations also contain embedded processors, which could be vulnerable.

IMPACT ON CIVIL NUCLEAR POWER

Documentation for plant equipment and software for many Soviet era reactors is either poor or non-existent. This makes it difficult to predict what kinds of problems may develop in connection with Y2K for these reactors. The CIA envisions two ways in which potential problems could develop with Soviet reactors.

The operation of internal components or sensors crucial to the operation of a nuclear power plant could be affected by Y2K problems. For example a valve with a digital controller designed to adjust the flow of cooling water could malfunction because the digital controller does not recognise the year-ending 00.

Y2K problems in the power grid could result in the loss of offsite power to the reactor. The loss of electric power would normally result in reactor shutdown. This could be complicated if internal problems arise in the reactor complex itself. Non safety-related equipment used to operate a plant could have problems. For example in some Soviet reactors, a computer is used to control power production. If this computer failed, safety systems would be activated and control rods would be inserted automatically and the reactor would be shut down. When external power is lost diesel generators supply power to cooling pumps to remove heat from the core. These diesel generators must have adequate fuel supplies on hand of at least a week to prevent fuel melt.

The US Department of Energy is currently sponsoring a study to identify the most likely Y2K failures in Soviet designed reactors from internal Y2K problems or from electric power grid problems.

OTHER AREAS

There would also be an impact in other sectors of the economy. The oil industry and telecommunications could also suffer some ill-effects, as could banking. In March, the deputy chairman of the Russian Central Bank Nikolay Yegorov said that Russia's banking system would require \$500 million to prepare for 2000. He said that the Central Bank alone would need to upgrade 20,000 computers.

However, Russian commerce, industry and individuals rely on the banking systems to a much smaller extent than do those in the West.

Whilst the Y2K problem is not likely to have an apocalyptic effect on Russian society, it is likely that many important sectors of the economy could face considerable disruption, and could therefore increase hardship throughout the Russian Federation. Disruption of energy supplies would clearly have this effect, especially as the Y2K problem will occur in the middle of the winter. It is also possible that Russian computers will be affected by similar problems on 9th September 1999, and 29th February 2000, as computers could also be confused by these dates. Other CIS states may be even worse affected by Y2K than the Russian Federation.

It would appear, therefore, that the main problems are likely to be due to lack of timely preparation. They may include:

- Civil unrest as a result of disrupted energy, telecommunications and distribution networks;
- Knock-on effects for Western finance and energy resulting from failures in Russia.

ENDNOTES

The Conflict Studies Research Centre

Directorate General Development and Doctrine

Royal Military Academy Sandhurst

Camberley Telephone : (44) 1276 412346

Surrey Or 412375

GU15 4PQ Fax : (44) 1276 686880

England