Russia's Nuclear Arsenal: Why the Y2K Bug Didn't Bite

Wendin Smith

The new millennium has arrived, and the much-vaunted "Y2K bug" was, for the most part, not a problem. Aside from a few isolated technical snags, fears about a worldwide crisis when computers misread "2000" as "1900" were exaggerated. Most importantly, we can all breathe a sigh of relief that the worst-case scenario—a Russian nuclear crisis—did not occur. This was a cause for considerable and legitimate concern; however, up to the last moments of 1999, many expressed doubts about whether Russia's nuclear arsenal would make it through the New Year unscathed. This article traces the origin of these concerns and examines the steps taken by the Russian and American governments to ensure that disaster not occur.

Throughout 1999, the United States and Russian governments repeatedly issued assurances that, while no absolute guarantees could possibly exist, neither government anticipated any misfirings or related catastrophes resulting from computer failures within Russia's strategic nuclear arsenal around the turn of the millennium. At the same time, however, many leading scientists and politicians expressed concern over the legitimacy of these official claims. The public was receiving mixed signals about whether it should trust the CIA and the general of the Russian Strategic Armed Forces—or whether it should assume that information was being filtered in the interests of national security and public calm.

The underlying distrust stemmed from the lingering Soviet tendency to gloss over severe problems and only grudgingly admit responsibility for catastrophe. Observers could not help but wonder when Russian authorities said that there would be no problems: did that mean that they were not aware of any simply because they had failed to investigate them? Or did it mean that problems were indeed identified but were officially being denied? Investigating these three facets

Wendin Smith is a master's degree candidate at The Fletcher School of Law and Diplomacy.

of the Y2K problem—the assurances that troubles would not erupt, apprehension among specialists, and the difficulty of deciphering Russian communications on this score—illustrates the complexity of the Russian nuclear arsenal issue.

To understand the scope of the problem, it is helpful to examine Russia's nuclear arsenal and the degree to which it has changed over the past decade. In the first few years after the dissolution of the Soviet Union in 1991, all nuclear weapons from Kazakhstan, Belarus and Ukraine were returned to Russian soil. The Y2K nuclear arsenal problem, therefore, did not extend to other former Soviet republics. In addition, extensive efforts since 1991 by the United States through the Nunn-Lugar program have facilitated the destruction of 365 ballistic missiles, 343 ballistic missile launchers, 49 bombers, 136 submarine missile launchers and 30 submarine-launched ballistic missiles.[1] Additional U.S. government programs have helped to secure and protect current Russian nuclear facilities. The Russian government made similar efforts to secure and protect its nuclear arsenals from threats ranging from terrorists to the Y2K bug.

The fact that the number of weapons has decreased was not in itself enough to alleviate concerns. In fact, even after the strategic nuclear arsenal reductions conducted under the Strategic Arms Reduction Treaty (START I), Russia maintains a large nuclear weapons arsenal as the backbone of its defense posture. Three main types of delivery systems compose Russia's nuclear triad: the intercontinental ballistic missile, the submarine-launched ballistic missile and bombers that deliver missiles by air. The Russian Ministry of Defense believes that each leg of this triad is essential to deter attack against Russia. Especially today, with budget constraints, low morale in the military and difficulty meeting conscription targets, the cash-strapped Russian military openly relies on its 2,000 nuclear-tipped missiles as the basis of its national security and defense policy.[2]

The number of strategic and tactical nuclear weapons in Russia remains large. At the end of 1998, Russia was capable of launching a total of 3,590 intercontinental ballistic missiles. The second leg of its triad, the submarine, accounted for 348 delivery systems with 1,576 warheads ready to launch. Finally, Russia carried 800 air-launched cruise missiles aboard its 70 bombers. At the turn of the millennium, the numbers of armaments are likely quite similar, although it is estimated that no more than 2,000 of these warheads are capable of being launched at any time. While exact numbers are not available, Russia reportedly maintains around 4,000 non-strategic nuclear weapons in naval and land-based systems; approximately 22,000 nuclear warheads await dismantlement. All of the delivery and warhead systems rely heavily on computers that lacked a comprehensively implemented program to deal with the potential Y2K problem. Before January first arrived, no one knew to what extent these Russian computers would indeed misread the year 2000 as 1900—or when, precisely, a problem could erupt on this account in the future.[3]

Negotiations and preparations to address the concern over the preparedness of Russia's Defense Ministry for potential problems resulting from the millennium bug focused on three main threats. First, the repair of existing delivery systems and warheads in Russia was—and still is—in decline. Experts questioned the capacity of existing arsenals to function properly. Faced with such problems, confidence in the ability of Russia's delivery systems to withstand Y2K complications was low. Second, Russia's early warning system is essentially non-functional. Thus, the Strategic Rocket Division, the branch of Russia's military responsible for the nuclear arsenal, found itself in the quandary of having nuclear arms on hair-trigger-alert to respond to attack without the satellite and warning systems necessary to forewarn them of incoming missiles. Third, Russia lacked the budget and time necessary to complete Y2K preparations.

EXISTING DELIVERY SYSTEMS AND WARHEADS IN DISREPAIR

The safe and secure storage of Russia's nuclear stockpile was among the most pressing Y2K concerns. The Materials Control, Protection, and Accounting (MCP&A) program administered by the U.S. Departments of Defense and Energy successfully engaged Russian counterparts to ensure nuclear stockpile security and protection to the year 2000 and beyond. MCP&A continues to be the cornerstone of U.S.-Russian cooperation in nuclear security. As a result of this MCP&A engagement, the Russian Ministry of Defense recognized that it had not adequately anticipated the lurking Y2K problems for its nuclear stockpile. In response, the Russian Defense Ministry established Y2K monitoring stations at the largest nuclear warhead storage facilities. Specialists trained to monitor the security and environmental controls within the facility's telecommunications and power centers manned these stations around the clock. In addition, the Ministry of Defense conducted "capability tests" to assess the ability of its personnel to respond to an emergency.[4] These assessments and monitoring stations were essential first steps in securing Russia's delivery and warhead systems from problems associated with Y2K non-compliance and were likely key to the ultimate success of the endeavor.

However, Russia's nuclear weapons systems are laced with embedded controlling functions (such as ballistics and sensors) that were thought to be vulnerable to Y2K-related problems. In addition, most missiles keep track of time since the last monthly or yearly servicing; a Y2K glitch could have transformed these weapons into "plutonium-packed paperweights" if the systems had shut down on January 1, 2000.[5] Russia requested approximately $15 million in equipment in order to upgrade its ability to respond to a Y2K-induced emergency. Through Nunn-Lugar funding, the Pentagon provided this assistance in time to alleviate additional Y2K concerns.

RUSSIA'S NON-FUNCTIONAL EARLY WARNING SYSTEM

Both U.S. and Russian officials issued assurances that nuclear missiles would not be accidentally fired as a result of computer-generated Y2K glitches, and their assurances turned out to have been warranted. Even such assurances did not completely rule out the chance, however, that missiles could have been launched. Nuclear missiles on hair-trigger alert might have been launched by human error, if, as Senator Lugar states, "operators are not able to tell the difference between a peaceful rocket and a military rocket on their computer screens."[6] This nightmare scenario could have been caused either by the absence of a functioning early warning system or by a failure within such a system caused by a Y2K-related problem, for example.

Russia's early warning system is designed to detect incoming missiles launched from anywhere in the world. The early warning is intended to give the Russian government time to enact emergency measures to secure government assets prior to the missiles striking Russian soil, and should allow the Russian government to respond by launching its own missiles. The system relies heavily on computers to mesh data from satellites, radar and other sensors. Currently, many of its satellites and radars are out of service, leaving Russia unable to track potential incoming missiles across all its 11 time zones concurrently. Y2K-generated problems could have caused the early warning system to falsely register incoming missiles, prompting the request for permission to launch a counter-offensive. Therefore, the potential for an accidental launch of any one of Russia's 2,000 nuclear-tipped missiles seemed acute, regardless of government efforts to fix the computer tracking systems.[7]

In 1963, the U.S. and then-Soviet Union began installing seven direct communication links in order to assure immediate communications between the two presidents, the secretary of state and foreign minister and other officials. In 1998, Defense Secretary William Cohen followed up on this communications concept by ordering plans for sharing early warning information so that the U.S. and Russia "don't enter into a nightmare condition where everybody is all of a sudden uncertain when their screens go blank."[8] To do this, U.S. and Russian defense officials set up a joint center in Colorado to watch for any false alarms of missile attacks caused by Year 2000 computer problems. When Secretary Cohen and his counterpart, Defense Minister Sergeyev, set up the center, both agreed that it would reduce the chance that a "turn-of-the-millennium computer error will create an end-of-the-year security incident."[9]

At Peterson's Air Force Base in Colorado, Russian and U.S. military personnel sat side by side as part of a pioneering missile watch. The specialists shared workstations beginning on December 27, 1999, and kept vigil in shifts of 20 personnel until mid-January 2000. Throughout the watch, the military officers were in telephone contact with command centers in both the United States and

Russia. This Center for Strategic Stability made use of the North American Aerospace Defense Command (the joint U.S.-Canadian command better known as NORAD). Using a mesh of satellites, radar systems and other sensors, the system can detect missile and space shots (including the heat of a SCUD missile launch) from 22,300 miles in space. Personnel at the center were prepared to relay data on any other defense-related problems that might have emerged from Y2K problems, such as off-course aircraft or defense concerns from other countries. Cohen and Sergeyev have discussed creating a permanent missile early warning system center in Moscow after the turn of the millennium—an idea that President Clinton and former President Yeltsin strongly support.

RUSSIA LACKED TIME AND MONEY FOR Y2K PREPARATIONS

The Pentagon spent $3.8 billion to prepare its most important defense systems for January 1, 2000. The Russian Ministry of Defense spent much less, since it did not have the capacity to do so. Since the fall of the Soviet Union, the military has been assaulted with an array of troubles: budget cuts, reduced morale, humiliation in combat, fractured borders, draft evasion, faltering chain of command and faltering maintenance. Over the past decade, the military has been cut from five million to 1.2 million personnel. Military personnel often lack adequate food, heat, clothing and other basic needs in order to live, let alone maintain combat-readiness. The air force has not received a new plane since 1992, and the lack of fuel has forced pilots to an average of only 25 hours of flight time annually—in sharp contrast to the Western minimum of 200 hours. Russian defense officials estimate that over 70 percent of the ships are in need of major repairs. Many have sunk due to rusted hulls. Of the 100 submarines that patrolled just a decade ago, only three are currently estimated to be on patrol at any given time. Likewise, the army has received no new weapons over the past few years and has as few as 10,000 combat-ready troops.[10] In the face of mounting budget concerns and the pressures of the military action in Chechnya, Russia simply did not have the capacity to expend the necessary capital to rectify potential Y2K problems.

In addition to financial constraints, Russia had begun its Y2K preparations quite late, prompting concerns about whether it had budgeted enough time to prepare for the new year. As Ken Baker, U.S. Assistant Secretary of Energy stated in September 1999, "The worst enemy right now is time."[11] In response to the Russian Defense Ministry's requests, the U.S. Department of Defense rushed to provide Russia with Y2K-compliant software, emergency generators, fire trucks, warhead handling vehicles and backup communication equipment in time for the turn of the century. While this additional $15 million of equipment helped prepare Russia for potential Y2K emergency failures, the fact that it was requested so late added to fears about Russia's preparedness.

At the eve of the New Year, both U.S. and Russian officials said they were highly confident that Y2K failures would not lead to the inadvertent or unauthorized launch of a ballistic missile by either country. However, a September 14, 1999 Pentagon memo underlined the potential for "opportunistic engagements by hostile forces" taking advantage of widespread system failures.[12]

Thanks to tremendous efforts, the nightmare of a nuclear "Y2K Armageddon" was averted. Since Russia's vast territory crosses 11 time zones, however, the potential for lurking Y2K bugs to bite in other sectors later in the year remains a possibility. Will there be enough electricity to power essential systems at nuclear power plants? Will existing power grids fail? What other systems might fail? U.S. Senator Christopher Dodd (D-Connecticut) is the vice-chairman of a Senate committee reviewing Y2K readiness issues in the U.S. and around the world. In a press briefing last fall, he urged:

> ...Not to forget that there are many Chernobyl-type facilities within the borders of the former Soviet Union—16, to be exact. No one is expecting any sort of catastrophic nuclear meltdown because of Y2K. On the other hand, we need to have a very clear understanding that Y2K failures will not create immediate safety hazards for the people in these countries and beyond their borders. Computers controlling daily operations may well experience problems that impact safety operations. The stability of these nuclear power plants is among Russia's highest priorities.[13]

While discounting a heightened possibility for "another Chernobyl," a CIA official in mid-October 1999 pointed to Soviet-designed nuclear plants in Russia and Ukraine as the most vulnerable to potential Year 2000 computer failures, particularly if coupled with energy losses due to power grid failure.[14] The U.S. Department of Energy worked closely with the International Atomic Energy Agency to help resolve Y2K problems with the Soviet-designed reactors. Through workshops, conferences, reviews and training sessions in Russia, the U.S. and Europe, the U.S. Department of Energy helped prepare nuclear energy sector personnel for potential Y2K problems.

A number of safeguards were in place to mitigate potential problems linked to Russia's nuclear arsenal at the turn of the century. This does not mean that the country is completely out of the woods: Y2K-related failures remain a tangible possibility in Russia's telecommunications, banking, municipal supply and emergency systems. Prior to the New Year, the risks were known to have been even greater. In his September 1999 prepared statement to the Senate Special Committee on the Year 2000 Technology Problem, Senator Richard Lugar cited a disturbing report publicized by the American Chamber of Commerce in Russia. The impact of Y2K problems could have: (1) caused utilities to operate at 40 percent of their capacity for the first two months of 2000, (2) disrupted transportation 80 percent of the time, (3) reduced telecommunications capacities 50 percent of the time for three months, and (4) disrupted hospitals, financial markets, and banks for 20 to 60 days.

Contrary to the worst fears, Russia did indeed pass the Year 2000 threshold without any publicized problems in its nuclear arsenal. The breadth and depth of the potential systemic breakdowns spurred a new level of Russian-U.S. cooperation, which in large part can be thanked for the smooth transition. ■

NOTES

[1] "Y2K and Russia: What Are the Potential Impacts and Future Consequences?" Prepared statement of Senator Richard Lugar before the Senate Special Committee on the Year 2000 Technology Problem. United States Information Agency, September 28, 1999.

[2] Jim Wolf, "Old Nuclear Foes Join to Avert Y2K Catastrophe," Reuters, October 18, 1999.

[3] These data are available are drawn from the database of the Center for Nonproliferation at the Monterey Institute for International Studies.

[4] "Millennium Bug Tests Under Way at Nuclear Power Plants," Radio Free Europe/Radio Liberty, October 12, 1999.

[5] Will Englund, "Lack of Preparation Leaves Y2K's Effect on Russia an Enigma," Baltimore Sun, October 17, 1999.

[6] David McGuire, "Lugar: Fix Russian Y2K," Newsbytes, September 29, 1999.

[7] Tom Bowman, "U.S., Russian Military Ally Against Y2K Bug," Baltimore Sun, October 27, 1999.

[8] "U.S., Russia Working on Y2K "Hotline" Glitches," Reuters, September 28, 1999.

[9] U.S. Defense Secretary William Cohen at a 14 September meeting with Russian Defense Minister Sergeyev. Quoted in Wolf, October 18, 1999.

[10] Barry Renfrow, "Russia Tries to Save Military," Associated Press, July 2, 1999.

[11] Reuters, September 28, 1999.

[12] Wolf.

[13] "U.S.-Russia, Agree to Joint Monitoring," UPI, September 13, 1999.

[14] Englund.

Master of Arts
In
Humanitarian Assistance

This one-year masters is a joint degree with
the School of Nutrition Science and Policy (SNSP) and
the Fletcher School of Law and Diplomacy at Tufts University.

Its focus is on world relief and development
intended for mid-career professionals who have significant
field experience in humanitarian assistance.
The program offers an academic setting
where professionals can develop their knowledge and skills
in the areas of nutrition, food policy, and economic, political,
and social development as they relate to humanitarian assistance
in famine, complex emergencies and other disasters.

Contact: ggamba01@tufts.edu
Feinstein International Famine Center
96 Packard Avenue, Medford, MA 02155
Tel: 1-617-627-3423
Fax: 1-617-627-3428
www.tufts.edu/nutrition/famine