the Bulletin of the Atomic Scientists

March/April 1999
Vol. 55, No. 2

Safe or Sorry: The "Y2K Problem" and Nuclear Weapons

By Michael Kraig

At 2:25 a.m. on June 3, 1980, warning displays at U.S. nuclear command centers began showing the launch of enemy missiles. Preparations for retaliation against an apparent Soviet attack were quickly instituted: Bomber crews started their engines, Pacific Command's Airborne Command Post took flight, and Minuteman missiles were readied for launch.

In the end, it was a short-lived scare. The numbers of missiles shown in the displays didn't make sense-and they kept changing. It was a false alarm. Technicians eventually traced the problem to the random failure of a 46-cent computer chip. Not one, but several nuclear command posts had been affected.1

Millenarian fever

The "millennium bug" or the "Y2K problem"-a result of computer codes that use two rather than four digits to express the year-is expected to cause between two and five percent of all computer chips to malfunction when the date-as they interpret it-rolls over from 99 to 00.

A 25 percent failure rate doesn't seem like much until the possible rippling effect of a single failure is considered. Failing chips can cripple subsystems, which in turn can cause partial or total failure of entire systems. Those impaired systems may cause any or all of the other systems with which they are connected to fail as well-and Pentagon systems interface with an average of 1213 other systems.

Is it possible to find the chips with Y2K problems? Maybe. But a lot of systems have been built up over time, and it may be impossible to ask the manufacturer of any particular chip whether it is affected. In fact, the original manufacturer-if the company is still in business-may be as clueless about the Y2K compliance of a particular chip as anyone else. The prospect of getting information from authors of software code-which is similarly prone to failure because of the Y2K problem--is at least as bleak.

So what should the world's greatest defense department in the world's greatest superpower be doing? In an ideal world, it should scan every chip and every line of computer code it owns for dates that, although often hidden, are nonetheless critical to all sorts of functions-sorting data, processing records, performing mathematical calculations, and so on. But it is not an ideal world. Even if the Pentagon could check every chip and every line of code, as Lt. Gen. William Donahue, the commander of the Air Force Communications and Information Center has said, in January 2000 the military would still have to deal with "'known unknowns'--known problems with unknown solutions--and a few 'unknown unknowns.'"2

Y2K meets nuclear weapons

Both governments and militaries like predictability. Surprises are annoying, troubling, even dangerous. The millennium bug is a potential mischief-maker in that it may lead to unpredictable failures of systems and cause ambiguous or confusing data to be generated. Systems failures and ambiguous data create uncertainty, and in a fast-moving world in which more than 4,000 nuclear warheads are still on 15- to 30-minute alert, no one has much tolerance for uncertainty.

When it comes to nuclear weapon systems, two separate areas of concern can be delineated-maintaining force readiness and ensuring safety.

Force readiness may be impaired by systems that cause automatic shutdown. This might occur, for instance, if the permissive action links (pals) that protect a warhead from accidental or unauthorized detonation were to interpret an anomalous date as an attempt to illegally unlock it. Pals would respond by disabling the warhead. Similarly, some chips-concluding that "00" means that no maintenance checks have been made since 1900-could shut systems down for maintenance. Problems with guidance sets could lead to targeting inaccuracies, as could the breakdown of satellites that send targeting data to missiles in mid-flight.

Safety. Force-readiness problems are undoubtedly on the minds of planners at Strategic Command (STRATCOM), but few non-STRATCOM analysts worry that "damage expectancy" criteria would not be met or that not every "selective attack" option would be available. Outside analysts are much more worried about a breach in nuclear safety.

The most nightmarish of worst-case scenarios--a nuclear weapon exploding in its silo or a missile launching because of a Y2K failure--is not plausible. Pals and environmental sensing devices prohibit nuclear detonation without command authorization and the proper environmental conditions.3 However, there are other, more realistic worst-case scenarios.

Communications foul-ups. The ability of the United States to monitor Russian activities is based on a highly interdependent conglomeration of radar arrays, satellites, communications networks, and data processing stations. With 2,440 U.S.--and 2,000 Russian--warheads on high alert, it is essential that all military communications systems be repaired and tested before the turn of the century. It is difficult to evaluate how well that process is going. But we do know that in 1993, when NORAD technicians rolled dates forward to January 1, 2000 for a simulation, the result was total system blackout.

Human error. Another safety-related problem is the increase in simple human error that is likely to occur when computers malfunction. As John Pike of the Federation of American Scientists recently told MSNBC, "The thing you worry about is people improvising. . . . If systems behave peculiarly, people will be nervous, overworked, and stop trusting the system. Consequently, the man-machine interface starts behaving in unpredictable ways."

And finally, one danger that cannot be ruled out is fire, which could cause the possible dispersal of radioactive material. This might occur if the support systems for ballistic missiles were to break down-- whether the missiles were in dormant, semi-dormant, or ready-to-launch mode.

The problem of denial

A Russian government report issued in August estimated that half of the 50 operating systems and 100 software programs used by the Russian government will have serious millennium bug problems. And until February, both Russia's civilian and military leaders denied that Russia's nuclear forces could have Y2K difficulties. Boris Mikhailov, principal director of the Impulse State Scientific Production Association, where many of Russia's nuclear systems were developed, said simply, "I have worked here since July of 1980, and I never heard of anything like this."4 Similarly, Russian Defense Minister Igor Sergeyev said in August that there was no Y2K problem for Russia's nuclear weapons, "since in the Strategic Missile Forces we use special technologies."5

In contrast, outside observers recalled instead an incident in 1995 when Russia came very close to mistaking the launch of a Norwegian scientific rocket (about which it had received prior notification) for a U.S. Trident missile attack.

It was not until last September that Presidents Bill Clinton and Boris Yeltsin agreed to establish a system for exchanging information on missile launches and early warning. Since then, the U.S. and Russian delegations have held two meetings about which information to share and how to share it. But a joint U.S.-Russian early warning center, planned for Moscow, may not be ready until after January 1.

Consider this exchange from a December 8, 1998 Defense Department briefing:
"Q.: When is that shared early warning center going to be established?
"A.: We're hoping to have it done by late '99. It could be early 2000. It's a complex process, obviously. We will be building it in a facility provided by the Russians, and it will use some American and some Russian equipment as well.
"Q.: Am I confused on this point? I thought the point of that was to, in case there was some sort of Y2K glitch in the early warning . . .
"A.: That is one of the issues.
"Q.: Then it's sort of pointless to have it in early 2000 then, isn't it?
"A.: We're aiming to try to have this done in late '99. Realistically it might be done before that. But the fact that the system is not . . . if it is not done by the end of 1999, it doesn't mean that this work is useless because we will be sitting down with the Russians, working very closely with them, designing systems, designing sort of exercises on shared early warning tasks . . ."

The scorecard

Some progress has been made. According to the B-1B System Program Office, the B-1B bomber has passed all end-to-end systems tests. In addition, the "Global Positioning Systems satellites are well prepared for their rollover event on August 22, 1999."6

On the other hand, each of the military services has its own ground receivers, which may behave idiosyncratically. For example, the navy's software for processing GPS data interpreted January 1, 1998 as the 366th day of 1997.7

Reports from the Defense Special Weapons Agency, the unit that oversees the warhead stockpile and other programs at Sandia Laboratories, designated three mission-critical systems as Y2K compliant without actually testing them. This was not, concluded the department's inspector general, the result of deliberate falsification-just ignorance. Marvin Langston, the deputy assistant secretary for C3I, told USA Today, "I think there's very little real mischief going on here. There aren't as many people lying to us as there used to be."

The latest quarterly Y2K report from the Defense Department to the president, issued on November 17, contained both good and bad news. Air Force Gen. Robert Behler reported that independent simulated tests of 25 million lines of computer code for STRATCOM systems had been completed at Offutt Air Force Base, Nebraska. And a number of systems associated with advance warning had completed the repair or renovation phase, including the Defense Support Program Satellites, ground radar arrays (PAVE PAWS, PARCS, and BMEWS), the Satellite Control Network, the Defense Satellite Communication System, the milstar satellite networks, and the Minimum Essential Emergency Communications Network. A week-long "integrated" test or "operational evaluation" in December 1998 analyzed the Y2K preparedness of the entire ground radar array network. These systems were put through a series of scenarios involving tactical warning.

The "Cheyenne Mountain Upgrade," which incorporates four extremely critical and relatively new norad computer systems for data reception, data processing, user interface, and communications, was also described as a renovated system. It is probable that the system, which became fully operational in 1997--13 years late and billions of dollars over budget--had Y2K repairs made at the same time that software patches were installed to cure its many defects.

In any case, if managers of these communications programs are telling the truth (which is not something that can be taken for granted), major parts of the nuclear infrastructure may be poised for the turn of the century-assuming that ongoing mission-level tests will not reveal flaws that cannot be repaired in time. Ongoing evaluations need to be monitored closely.

On the negative side, Behler confirmed that the renovations of 23 critical systems, including 11 already in place and 12 new ones coming on line, are running late.

It also appears that the navy's nuclear submarine command and communication systems cannot be renovated. Several of the navy's key communications components are far behind the curve. These include the Integrated Submarine Automated Broadcast Processing System (the on-shore component of the Very Low Frequency Communications System), and the automated submarine processing system. According to Brookings expert Bruce Blair, these two systems are the primary mode of communications with ballistic-missile submarines.8 The navy says that to be compliant, the systems must be replaced, an unlikely possibility before the year 2000. And if they are not replaced, the command link with U.S. nuclear submarines will be severely weakened.

Other naval communications systems are also behind, including the satellite ground system and satellite information processing system, and the Naval Communications Processing and Routing System, which manages all of the navy's communications, including its connection to the Defense Department-wide military communications network.

Finally, the Defense Department's Quarterly Report contains an ambiguous reference to the "mission critical portion of the Trident strategic weapon system." According to the report, "One mission critical subsystem that requires a workaround will be notified of the workaround by naval message on 15 December 1999." In other words, the problem will not be corrected, and contingency plans for system failure will be forwarded to submarine crews two weeks before the year 2000.

Britain, which purchased Tridents from the United States, is relying on the United States to fix its Y2K problems. If the U.S. program fails, the British program will fail as well.

Brought down by Ma Bell?

The Defense Department, including STRATCOM and norad, rely, in part, on commercial phone lines, ground cables, and telecommunications switching centers. Accidents have been prevalent in at&t and Bell switching nodes, even without Y2K problems.9 The chance of more difficulties will only increase as the year 2000 nears.

John Hamre, the deputy secretary of defense, told a House subcommittee last June that "if Ma Bell's or Bell Atlantic's system fails on year 2000, we're going to have mission failure, and I don't have any control over that."

The Defense Department inspector general has concluded that the department's "telecommunications capabilities may become unstable, unpredictable, and the cumulative impact of non-Y2K compliant operational occurrences could result in system failure."10 Unfortunately, neither the General Accounting Office nor the inspector general has focused specifically on whether the nuclear communications network relies on the commercial telephone network.

A great time to de-alert

Given the complexity of Y2K vulnerabilities, the delay in implementing improvements, the ambiguous completion date for the early warning data-sharing agreement, and the virtual absence of a Y2K program in Russia, it would seem prudent to take a safety-first approach to the nuclear arsenals. But so far, the Pentagon's contingency planning has aimed at meeting pre-existing force readiness goals--it has failed to weigh the relative importance of meeting those goals or assuring nuclear weapon safety.

The White House and Congress need to intervene in the Pentagon's Y2K process by becoming more active in defining and creating viable contingency plans. This intervention should include serious consideration of arms control measures.

The best way to comprehensively address Y2K dangers is to mutually de-alert nuclear forces. Minuteman III and MX missiles are still three short steps from launch-including one simple computer command for targeting, one command for "fuzing" or arming the weapon, and the physical turn of launch keys by two individuals. These steps can be

implemented in a minute or less.11 A variety of de-alerting measures could increase launch time by minutes, hours, days, or weeks. And the process would allow both countries greatly increased confidence that regardless of potential failures in warning systems, neither could be the victim of a surprise attack.

Unfortunately, U.S. officials have rejected de-alerting options. Their dismissal stems from the continued U.S. commitment to preemptive strike, launch on warning, and first use. Partly in response to U.S. intransigence, Russia has adopted a first-use policy as well. U.S. officials argue that de-alerting could lead to a potential "race to re-alert," but it is hard to see how that "race" could be more dangerous than current hair-trigger force postures.

Logistical and political barriers to de-alerting exist, but they are manageable. Verifying de-alerting measures might require difficult technical steps in the case of Russia's mobile missiles, but here the start I inspection regime already in place could be useful.

Both Russia and the United States could have doctrinal problems with fully de-alerting their submarine forces, which they regard as the most survivable leg of the nuclear arsenal. If submarines were brought in from patrol, the particular advantages of a sea-based deterrent would be lost.

But Russia already has trouble keeping even one missile submarine on patrol, and some of its submarines are merely glorified launch pads sitting in dock, while the United States keeps four Tridents in forward-deployed positions at all times.

Even for the United States, the need for a fail-safe leg of the triad is based on the assumption that surprise attacks against its bomber bases and intercontinental missiles are likely events. But arms control groups have repeatedly pointed out that it is also destabilizing for the United States to deploy extremely accurate Trident II D-5 missiles in the Baltic, where their flight time to Russian targets is 15 minutes or less. In any case, if de-alerting were successfully and verifiably implemented, surprise strikes against submarines sitting at base would be not merely improbable but impossible.

Whatever arms control measure is ultimately favored, the time to act is now. Some U.S. corporations have leveraged the Y2K problem for their benefit, spending thousands and even millions on upgrading, integrating, and streamlining their computer systems for more efficient operations. The nuclear powers could reap an even greater benefit by abandoning their reckless disregard for the dangers that Y2K presents and instead recognizing Y2K as an opportunity to make meaningful strides in disarmament.

1. Alan Phillips, M.D., "20 Mishaps that Might Have Started Accidental Nuclear War," Physicians for Global Survival Newsletter, January 1997, revised January 1998.
2. Lt. Gen. William Donahue, "Achieving Success in the Y2K Battle," Air Force Printed News, Oct. 13, 1998.
3. "An Engineering Guide to Nuclear Weapons Development, Production, and Stockpile, WR713," Sandia National Laboratories Briefing to the General Accounting Office, 1995.
4. Bill Powell, "A Looming Disaster? Russia's Crumbling Arsenal Is More than Worrisome," Newsweek, June 23, 1997.
5. Nick Wadhams, "Russia Moves Slow on Computer Bug," Associated Press, September 15, 1998.
6. Adam Hebert, "GPS Systems Will Provide Early Test of Year 2000-Type Preparations," Defense Information and Electronics Report, vol. 3, no. 31 (Aug. 7, 1998).
7. Ibid.
8. John Donnelly, "Nuclear Commanders Evaluate 'Y2K' Impact," Defense Week, vol. 19, no. 49, pp. 1, 7 (Dec. 14, 1998).
9. Peter G. Neumann, Computer Related Risks (SRI International Computer Laboratory, ACM Press, 1995).
10. Richard Lardner, "Pentagon Says Y2K Remediation Costs Have Increased by $600 Million," Inside the Pentagon, vol. 14, no. 48, p. 17 (Dec. 3, 1998).
11. Discussion with Bruce Blair, Brookings Institution, Nov. 25, 1998.

Michael Kraig is a Herbert Scoville Jr. Peace Fellow at the British American Security Information Council (BASIC). More information about the Y2K problem as it relates to nuclear weapons can be found at http://www.basicint.org