When mistakes could cost lives

▸ *No danger of stray nukes, but other problems may be lurking*

By Robert L. Scheier, Gary H. Anthes and Allan E. Alter

COULD YEAR 2000 gremlins trigger Armageddon?

Fortunately, the answer is "no," say military officials and experts in the U.S. and Europe.

While date-sensitive information is used in the software that plays a part in launching intercontinental ballistic missiles, "Every plausible implication the year 2000 may have on the computer systems involved . . . has been examined and solutions have been devised," said a spokesman for the U.S. Strategic Command.

Outside experts agree that year 2000 bugs won't cause an accidental nuclear launch, but they can't rule out other grim possibilities. For example, such bugs could prevent strikes from being launched because of flaws in communications systems or the systems used to maintain the missiles, the experts said.

That kind of uncertainty lurks in every weapon that relies on software — and the problems can be enormously hard to find.

Take the case of the rogue Norwegian Navy torpedoes, which in the early 1990s went off course so badly that one steered back at the ship that launched it.

Pentagon officials are "scrambling around . . . trying to figure out how to budget it, how to approach it."

– DOD systems integrator

Ingvar Tronstad, an electrical engineer and former Norwegian Navy commander, said the torpedoes were getting inaccurate data because updates on their location were being sent a split second earlier or later than the torpedoes expected them. Over the seconds and minutes the torpedoes ran, the errors added up and were compounded by an error in application logic, sending the torpedoes off course.

This error involved only seconds, but many such "embedded systems" use years in critical calculations, said Tronstad, now the chief scientist at Ascent Logic Corp., a systems integration and consulting firm in San Jose, Calif.

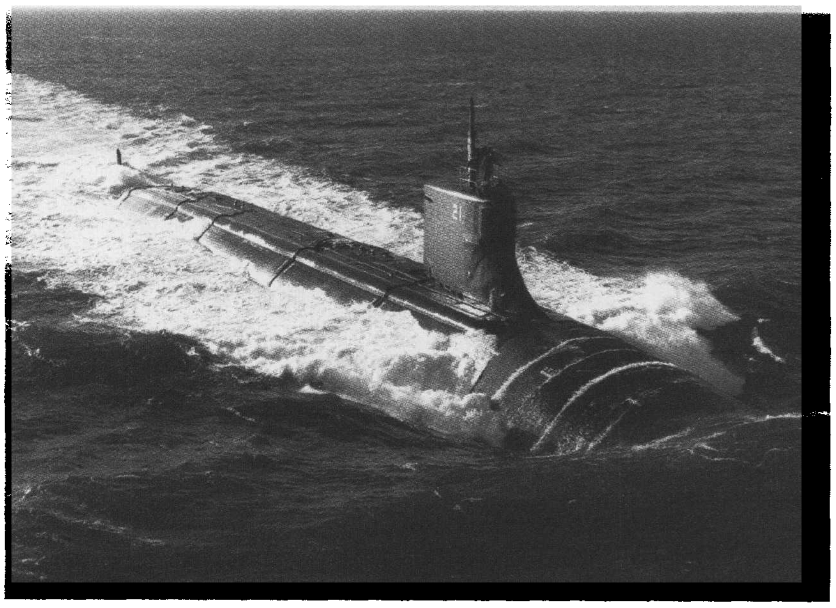
The failure of date-based filters that prioritize data could prevent the right data from getting to the right person at the right time, said Adam Luther, director of computer services at the Center for Defense Information, a Washington nonprofit watchdog group.

Even if the application itself doesn't use years, a related system that handles configuration management or maintains software licenses can fall victim to date-handling problems.

The U.S. Air Force learned that in March, when an incorrect expiration date in the license manager for a word processor shut down the application during a military exercise. As a result, the Air Force couldn't send critical mission data, grounding 2,700 simulated flights in the Persian Gulf and elsewhere until the Air Force and vendor created a fix.

After the snafu, tests of other systems revealed a similar problem that would have shut down the Combat Intelligence System, which generates information and images needed for targeting, on Nov. 11. "It's extremely fortunate that it was an exercise environment that this happened in," said Col. Carl Steiling, director of Theater Battle Management Core Systems at Hanscom Air Force Base in Massachusetts.

"The scenario that we fear most is that something like this may occur without our knowledge," Steiling said.

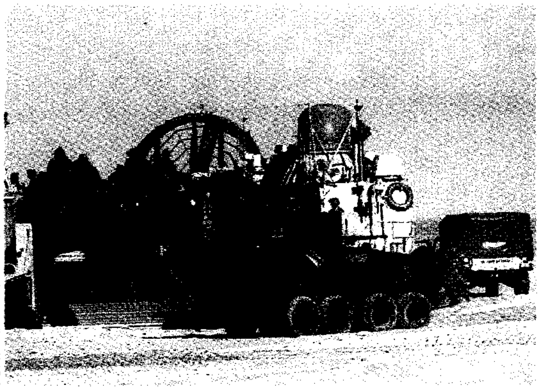

U.S. NAVY

"If you are doing a command-and-control system in a submarine, you are very date-dependent," says one programmer. "Anything that depends on inertial navigation . . . has these date dependencies."

THE YEAR 2000 AND THE MILITARY: WHERE ARE THE RISKS?

Date dependencies lurk throughout military software. No one knows exactly where they are, but the high-risk areas include the following:

LOGISTICS


DEPARTMENT OF DEFENSE

Systems that coordinate the movement of soldiers and their supplies are so critical and date-dependent that some call them the Pentagon's year 2000 "weak link."

Year 2000 bugs could prevent the shipment of critical spare parts. Date-based maintenance programs could prevent weapons from being used because the software has decided they haven't been maintained on schedule.

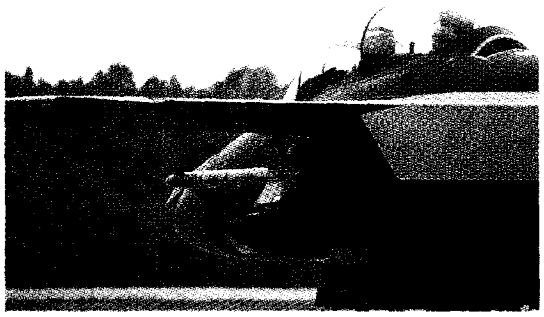
Many DOD logistics systems weren't built to exchange data, which makes it harder to trace, fix and test for bugs that occur between — not just within — military systems. Links also have to be checked between military logistics systems and those used by its civilian suppliers and shippers.

COMMAND, CONTROL, COMMUNICATIONS

DEPARTMENT OF DEFENSE

Communications systems use dates to decide how to code and decode classified communications and to filter communications. Years are used in navigation systems, in the systems used to launch nuclear weapons and to guard against nuclear attack. Defense officials said they have fixed, or will fix, such important systems first. But ever-changing requirements make it hard to decide which systems are most critical and to test all the ways they might work together. Some observers worry that enemies will launch electronic attacks on U.S. information systems while they are dismantled for repair. In addition, the U.S. can't completely test its systems until European and Asian allies — who are said to be lagging — finish their year 2000 work.

EMBEDDED SYSTEMS



Software that runs inside of weapons generally works only for short periods of time and thus usually doesn't rely on years. But all of it must be checked anyway.

These systems can cost eight times as much to fix as civilian applications because they're often written in older, obscure languages. Poor documentation and multiple ways of calculating dates make it harder to scan for problems.

Some of the code is burned into chips that may no longer be produced. The Pentagon says many such year 2000 problems will be solved by routine maintenance. But that still leaves the possibility of bugs where embedded systems share data with other applications.