The U.S. Department of Defense and Y2K

W
M

8
7
3

The following is an excerpt from our latest book, *How to Prepare for Y2K and Other Crises*.

Last month, we advertised the book before it was completed. We said it would be half size (5½ x 8½) and 70 pages long. —It turned out to be full-size (8½ x 11) and 84 pages in length! The book is filled with information, yet the price remains the same: $5.50+$1.50 p&h.

Here is a glimpse of what you will find in it:

THE DEPARTMENT OF DEFENSE

We will conclude our discovery of the Y2K status of our various federal government agencies with the Defense Department. We are talking about our U.S. Army, Navy, Air Force, Marines, and Coast Guard,—and we find that they too are unprepared for what is coming.

> "**What does it mean to have [only] one-third of our mission critical defense systems working in 2000?**"—*Jim Lord, Year 2000 Survival Newsletter, March 31, 1998.*

Let me begin by telling you a story. Did you ever wonder why that Scud missile was able to destroy that barracks in Saudi Arabia during the Gulf War. —**The problem was a Y2K-type of situation; a computer clock was not set right**. Here is what happened:

> "A preview of possible military disasters was the incident in the 1991 Gulf War, when a Scud missile blew up a barracks in Saudi Arabia, killing 28 National Guard troops inside. A post-mortem of the disaster revealed that **the Patriot air-defense battery failed to shoot down the Scud because the clock in the Patriot's radar system was not properly synchronized**.
>
> "The radar has been designed to be left on for only a short while. Its clock viewed a day as 23 hours and 59 minutes long. However, once this particular Patriot arrived in Saudi Arabia, the radar was left on continuously. So its clock drifted away from the actual time by one minute per day. Then the Patriot's system computer detected an incoming Scud missile; it would see the missile on two radar screens and send both blips to another computer controlling its fire-control system. But since the two blips were not synchronized, the fire-control computer could not connect them because it could not see them as a target.
>
> "The Scud tragedy illustrates why the clocks and calendars inside the computers matter so much. John Pike, a weapons specialist at the Federation of American scientists, explained: '**Systems generally require time synchronization in order to talk to each other. A lot of systems use time synchronization as a way to establish data links. So, if one computer says it is 1900 and another says it is 2000, they can't talk to each other**."—*Boston Globe, June 21, 1998.*

That bears repeating: "Systems generally require time-synchronization in order to talk to each other . . So, if one computer says it is 1900 and another says it is 2000, they can't talk to each other." This helps clarify the problem that very soon will take down our military preparedness.

When Ed Yardeni and John Koskinen (our U.S. Y2K czar) were interviewed by CNN on Y2K on September 18, 1998, they both agreed that **the number one Y2K problem which America faces is its non-compliant Department of Defense, which by the turn of the century will only have about one-third of its mission critical systems Y2K compliant.**

Yet the Department of Defense did not even become aware of the Y2K problem until 1995!

With the world's largest payroll and an arsenal of air, land, and sea weapons dependent on computers, the Pentagon (which will spend over $10 billion on Y2K remediation efforts in the final 18 months before the century ends) is hopelessly behind. Rep. Horn's committee estimates that the DOD will not be ready until 2012.

In the third quarter of 1997, the DOD reported that it had 25,054 affected systems and only 3,143 mission critical systems. Sounds pretty good. A lot of checking must have gone into such exact

DATE OF PUBLICATION: APRIL 1999

numbers. Then, on June 12, 1998, Rep. Steven Horn's Y2K Committee disclosed that **the DOD had falsified both those numbers and the number of actual repairs which had been made**.

The same month, the Office of Management and Budget (OMB) issued a report for the quarter ending May 15, 1998. **The report revealed that the Department of Defense, Veterans Affairs, and Interior have all slowed in their efforts to fix their Y2K problems in the previous three months**. The detailed report outlined progress at 24 federal agencies.

Our defenses are in deep trouble.

"During Bill Curtis' 27-year career as a military computer programmer, he wrote more than a few lines of code that were century-insensitive. 'I made decisions that we could use two digits for the date,' he confesses. Now, as the head of the Department of Defense's Y2K office, Curtis is in charge of fixing his own—and everyone else's—software problems. It's a job nobody else wanted.

"Although the Pentagon began Y2K planning in 1995, repairs of the most vital computer systems were only 9% complete this spring. The F-15 and the Navy's Tomahawk missile are two of 34 as yet undebugged weapons systems cited in a report scheduled to be released this week.

"When pressed, Curtis admits that **even the military's most 'mission critical' systems—perhaps 2,800 in all—won't be ready in time. Officials insist that America's nuclear arsenal is more or less fail-safe**, which means that if the computer systems go haywire, the missiles won't launch. **Whether the same is true of Russia's nukes is an open question."—***Time, June 15, 1998.*

Near the end of 1998, the situation had not improved much.

"**The Defense Department recently received a letter grade of F and is projected to have only one-third of its essential computing systems working properly by the Year 2000. This is nothing less than scandalous**.

"Each Tomahawk missile has embedded computers that use identical software. If this software has a Year 2000 defect, the software engineers must correct the problem only once and then replace the bad software in each missile. **If this step is not taken, of course, the military would lose the capability to perform the specified missions because thousands of missiles would be rendered useless by the malfunctioning software**."—*Jim Lord, Year 2000 Survival Newsletter, March 31, 1998.*

The government has officially reported that "1,800 military mission critical systems" will not be Y2K-compliant when the century changes. What does this mean? It means something terrible. Read this:

"**When it is reported that Y2K repairs to a mission critical system will not be completed by the deadline, it means that all individual copies of that system will become defective and the fundamental mission capability will be lost or impaired. In the case of the Tomahawk [missile], thousands of individual missiles would become inoperative** and the military would no longer be able to destroy land-based targets with missiles from 1,000 miles away.

"The Horn Report Card projects that nearly 3,000 mission critical systems throughout the government will not be ready for the Year 2000. Nearly 1,800 of these are military systems. **This is, of course, a catastrophic loss of military capability** that would likely render the American military a helpless giant."—*Jim Lord, Year 2000 Survival Newsletter, March 31, 1998.*

So each of those 1,800 "military systems" is a single type of weapon or assist structure. It might be a missile or a fighter jet. It might be the radar on a carrier. After the turn of the century, 1,800 of those systems will no longer function. According to Rep. Horn's findings, some of those systems will not be operable until 12 years after January 2000.

But there is more: Some of the confused systems could fire against a supposed enemy, without having been attacked, thinking that a U.S. offensive action was beginning.

"Missiles will not fire without warning [if they have Y2K problems], says Army consultant Rich Hoffman. Though these and other weapons have embedded chips, Hoffman says a malfunction would disable the weapon, not deploy it. **The bigger issue, he says, is the possibility of a mistaken offensive**."—*Popular Science, October 1998.*

In April 1998, the General Accounting Office (GAO) issued an ominous report on the Department of Defense.

One of the 1,800 mission critical systems is NORAD. Another is our Global Command System. Yet another is our Global Positioning System.

"Authorities are investigating whether the nation's strategic defense computers could malfunction because of the millennium bug. Some military computers are almost certain to fail after the clock strikes midnight on Dec. 31, 1999, said John Stephenson, who heads the study by the General Accounting Office, the investigative arm of Congress.

"In an April 30th report to Congress, the GAO warned that time is running out to protect the military's 1.5 million computers. What you hope is

that defense officials will start to apply triage, Stephenson told the *Rocky Mountain News*.

"**They should decide what their most important missions are and which systems support those missions and fix those first**. A top GAO priority is the North American Aerospace Defense Command in Colorado Springs, a facility that monitors America's nuclear defenses. The installation at Cheyenne Mountain [Colorado, NORAD's central facility] is the linchpin of strategic forces. **Its computer-powered equipment can detect incoming enemy missiles.**

"The GAO also may review the satellite relay stations at Buckley Air National Guard Base in Aurora [Colorado]. **Those facilities track missile firings and nuclear explosions**.

"We are looking at NORAD in terms of the integrated tactical attack assessment system, said Yvonne Vigil, an evaluator in the Denver region GAO office. **Describing the complicated NORAD facility as the system of all systems, Vigil said NORAD's computers must be bug-free because their mission is to protect and safeguard the United States.**

"Perhaps the most critical area is the military, in which many old systems called legacy systems still play major roles. The software coding is so archaic that finding the sections calculating dates is difficult.

"A congressional committee estimated in 1996 that **the Department of Defense's Global Command Control System failed when the clock was pushed ahead to the year 2000. Deployed at 700 military installations worldwide, the system is the key tool in battle management and planning**.

"**Other vulnerable systems include the Global Positioning System used for determining a military unit's exact location and for the precision targeting of smart weapons. Most, if not all, of America's missiles are guided to their targets using the GPS system**.

"Other military communications systems could be compromised. **Even on-board computers in jet fighters will be tested**, the GAO report said.

"The report slammed the Department of Defense's handling of the millennium bug problem. **The Pentagon did not have a complete inventory of its computers, was wasting too much time trying to fix noncritical systems, and had inadequate contingency plans if important systems crash**, the report said. They've designated 2,900 mission-critical systems and 25,000 nonmission-critical systems, Stephenson told the *News*. But if you look at the statistics, **both the critical and noncritical systems are being repaired at about the same rate. So what's the point of designating 'mission critical' if it doesn't mean you focus your resources and priority on those?**

"The more they get into assessment of this, they're finding it's more insidious than first thought, the GAO's Stephenson said. **The GAO reports over the past two years on the military's 2000 problem have steadily increased in their alarm**.

"In the April report, the GAO warned bluntly that **failing to quickly fix the problem would mean computer failures that are widespread, costly, and potentially disruptive to military operations worldwide**. 'All the federal reports that we do will ratchet up without trying to create panic,' Stephenson said. 'We're becoming increasingly concerned.'

"Some of the big sector institutions like banks are ahead of the federal government. **'The Department of Defense is peculiarly vulnerable to this problem because it has such a grotesque set of legacy (older) systems,'** Stephenson said. 'It has an awful lot of systems that have been around for an awfully long time.'

" 'Though computer systems at NORAD's Cheyenne Mountain installation are being upgraded, **some military machines still calculate dates in archaic computer languages that are no longer in use. Many programmers who wrote the code have retired or adapted to more modern computer languages. Reviewing tens of millions of lines of military code to find the exact coding for dates and time is intensely time consuming. It is a great steaming heap of spaghetti code which means that it works by nobody knows why anymore!'** Pike said.

"And nobody wants to look too closely for fear that they might break it. When they go in there to start looking at the code, it turns out that half the code doesn't even execute any more."—*Rocky Mountain News, May 10, 1998.*

It is obvious that a very real danger exists. The enemies of America are many, and very soon their military will have an opportunity to attack us during a time when a major blind spot exists in our defenses.

Much more on our Global Positioning System in the next section of this book. But, first, let us briefly consider the U.S. Navy:

"**U.S. Navy operations worldwide could be severely disrupted by any failure to fix the Year 2000 problem in critical systems**, the audit and investigations arm of Congress said Tuesday.

" **'Failure to address the Year 2000 problem in time could severely degrade or disrupt the Navy's day-to-day and, more importantly, mission-critical operations,'** the General Accounting Office said. The GAO said **the glitch could disrupt everything from navy combat capabilities to communications, intelligence gathering, surveillance and fleet mobilization and readiness**.

"In a reply included with the report, the Navy

agreed to a GAO recommendation that it establish a complete and accurate inventory of information systems **and to plan for the continuity of all its critical military operations and business processes rather than only a part of mission-critical systems**.

"Secretary of the Navy John H. Dalton has called for the full involvement of U.S. naval leadership in Y2K issues. He has said the U.S. cannot afford to approach the problem with a business-as-usual attitude. **The problem touches virtually all areas of the Navy and Marine Corps from foxholes, to flight lines, to destroyer deckplates as well as shore infrastructure**."—*Orange County (California) Register, September 1, 1998.*

THE GLOBAL POSITIONING SYSTEM

This is a complicated subject, but I will try to simplify it.

Military ships, aircraft, and ballistic missiles have guidance systems to help them locate where they are and where they should go.

For at least 30 years, the U.S. used *gravitational maps* for this purpose. There are minor fluctuations in earth's gravitational field, found throughout the world. Locating them, both America and Russia earlier used such maps for military guidance; and Russia still does.

Very soon—for the first time since shortly after World War II—the U.S. will no longer be able to respond in the event of a Russian nuclear attack. Here is why:

We now use the global positioning system (GPS). It uses satellites and special, very accurate clocks for this purpose. There are 24 NavStar satellites, which receive signals from the Primary Standard Clocks at the Naval Observatory in Washington, D.C. They provide precise navigational signals for receivers to plot their positions from.

The Defense Communications Agency (now called Defense Information System Agency, or DISA) upgraded their system from the older LORAN-C models to GPS synchronized networks in the late 1980s and early 1990s. These networks are capable of moving immense amounts of data and voice communications with great accuracy—to any location in the world, even inside a submarine or deep in an underground missile silo.

Without the new GPS system, the U.S. government would find it nearly impossible to coordinate large-scale battle plans. *—Yet, on August 22, 1999, the GPS satellite system's clocks will roll back 1,024 weeks, making global network synchronization impossible.* The effects of this failure cannot be overestimated.

(It should be mentioned that the **GPS is also used for civilian usage, including the banking system. It is believed by banking experts that, on August 22, 1999, a worldwide depression may begin**. Time will tell. The banking system requires communication between banks and central banking institutions.)

While the world is watching Y2K with growing concern, the vulnerability of the GPS is being overlooked.

In April 1996, the government awarded Boeing a $1.3 billion contract to repair the GPS—and make it able to continue on through the next century. *Boeing now says that it cannot complete its repair work on the GPS until December 1999.* That is a full four months without the GPS; that is, if Boeing completes its work on time.

It is reported that the U.S. arsenal of guided missiles rely on GPS to guide them. But, **beginning August 22, the GPS will only provide erroneous data**.

In December, the new IMOSC (Integrated Mission Operation Support Center) system is slated to be completed by Boeing.

The Russian system of gravitational mapping will be fully functional until 2000; when, due to the Y2K problem, their system will no longer operate correctly. Even the Russians know their nation is crumbling. Some believe that if Russia wanted to regain its power, this four-month window of U.S. ballistic missile blindness would be its last opportunity. (Most of the NATO countries in Europe have converted to the GPS system also, so they would also be blinded for several months.) **For four brief months the balance of power will tilt fully in Russia's favor**.

What is the likelihood of all that happening? None can really know. However, we do know that Russia will not rule the world. According to the book, *Great Controversy*, the United States of America will be the leading world power at the end of time, and no one else. God is in charge, and will care for His commandment-keeping people.

— Vance Ferrell