The Operational Effects of the Year 2000 Problem

Lt. Col. Scott B. Dufaud
U.S. Air Force Year 2000 Program Management Office

Widespread year 2000 problems in military and civilian computer systems have the potential to open the door to grave consequences for the military and the nation's security in general. To prevent giving our enemies advantage over us in the face of potential chaos, people working in all levels in the nation's defense infrastructure must understand the nature of the risks and to fully participate in plans that ensure no weak links are left exposed.

According to retired Col. John A. Warden III (U.S. Air Force), leadership is the key to success or failure in war, and as such, every action taken in a war should be geared to directly or indirectly affect the enemy's leadership [1]. Given the phenomenal success of Warden's "Instant Thunder" plan employed in the Gulf War, this theory has been proven in battle.

Warden's basic premise is that modern nation-states exist as a "system" that consists of five concentric rings or "centers of gravity." The innermost ring is "leadership" and (moving outward) is followed by "key production," "infrastructure," "population," and finally the outermost ring is "fielded military forces." Because the nation-state operates as a system, each of the centers of gravity is dependent on the others for the survival of the system. Each center of gravity is also directly or indirectly affected by the health and status of the others.

Warden asserts that leadership is the key to success or failure in war because when a nation has endured enough pain inflicted through conflict, the leader will sue for peace or lose power. In other words, the cost for continued resistance and conflict is greater than the consequences faced by laying down arms. He also states that prior to the ascendancy of air power, the only way to directly influence a nation-state's leadership was to first engage and destroy the enemy's fielded military forces. Only then were the other centers of gravity exposed and vulnerable. With advanced technology and superior air power, Warden argues that all aspects of a nation-state are equally vulnerable to attack and destruction from the onset of hostilities [1].

Influence Through Strategic Paralysis

Warden and his team of planners devised the Instant Thunder air campaign to achieve a specific effect called "strategic paralysis" to strike at the heart of the enemy's leadership and bring about a quick end to the conflict. Strategic paralysis explains the effects of disconnecting a nation's leadership from its people and the fielded military forces. This would cause a systemic breakdown of strategically critical functions such as communications, electricity, distribution, and other aspects of the national infrastructure. Instant Thunder successfully attacked Iraq's national leadership by cutting off Saddam Hussein's ability to communicate with his subordinates and by halting the availability of key production and infrastructure facilities.

Because the United States is the most technically dominant nation in the world, we have the distinct advantage and capability to deliver strategic paralysis on our enemies while remaining relatively invulnerable to a reciprocal attack on our nation. However, by using advanced technologies, we have become extremely dependent on those technologies to perform our missions. Every aspect of our society and our military is computerized or automated and therefore relies on immediate access to accurate information. Our reliance on technologies has created built-in vulnerabilities and threats to our ability to carry out the mission. We do not have to worry about strategic paralysis being inflicted upon us by our enemies, but our dependence on technology has exposed us to the year 2000 (Y2K) "time bomb," which has the potential to inflict strategic paralysis from within.

Are We Susceptible to Parallel War?

If the eyes and ears of our nation's leaders are blinded because of the Y2K problem, our enemies will have the opportunity to exert influence on U.S. leadership. Without exposing a single asset or suffering a single casualty of their own, our enemies will enjoy the benefits of a direct attack on the U.S. national leadership in the first ring of Warden's model.

Simple analysis shows that the insidious nature of the Y2K problem on an information-based society will attack all five rings of Warden's model equally and simultaneously. Warden points out that because the concept of "parallel war" brings many parts of a nation's system under simultaneous attack, the system cannot react to defend or to repair itself [2]. Not even the greatest military planners with unlimited military resources could ever accomplish what could happen to our nation-state as a result of the Y2K bomb. Our enemies are watching our progress on fixing what is potentially one of our nation's most significant threats in history.

History is full of examples in which the difference between success and failure in conflict has been determined by the possession or absence of key information at key points in time. Richard Gabriel declares that the one constant in the Mayaguez rescue, the Iran raid, the Lebanon incursion, and the invasion of Grenada was intelligence failure [3]. The intelligence mission and every other military mission we perform is based on getting the right information to the right place at the right time. If we cannot move accurate data in a timely manager because of the Y2K problem, we put our mission success at high risk. Likewise,

Notice of Cancellation

Military Standard Software Development and Documentation

MIL-STD-498
Notice 1
May 27, 1998

MIL-STD-498, dated 5 December 1994, is hereby canceled. Information regarding software development and documentation is now contained in the Institute of Electrical and Electronics Engineers (IEEE)/Electronics Industries Association (EIA) standard, IEEE/EIA 12207, "Information Technology-Software Life Cycle Processes." IEEE/EIA 12207 is packaged in three parts. The three parts are IEEE/EIA 12207.0, "Standard for Information Technology – Software Life Cycle Processes"; "IEEE/EIA 12207.1, "Guide for ISO/IEC 12207, Standard for Information Technology – Software Life Cycle Process – Life Cycle Data"; and IEEE/EIA 12207.2, "Guide for ISO/IEC 12207, Standard for Information Technology – Software Life Cycle Processes – Implementation Considerations."

[DoD activities may obtain copies of the IEEE/EIA standards from the Standardization Order Desk, 700 Robbins Avenue, Building 4/D, Philadelphia, PA 19111-5094. The private sector and other government agencies may purchase copies from the Institute of Electrical and Electronics Engineers, Inc., IEEE Service Center, 445 Hoes Lane, P.O. Box 1331 Piscataway, NJ 08855-1331.]

history also shows us that the availability of accurate and timely intelligence is key to success. This is what enabled Gen. George S. Patton to drive his forces with focused speed: He knew what he could expect from the enemy, where to send fuel and ammunition, and when to shift land and air forces.

Rapid offenses and troop movements are complex and require massive amounts of accurate and timely information [2]. Our entire command and control system is based on our ability to gather, analyze, and disseminate information, all through an "infosphere" that is dependent on technology-based equipment and systems that are vulnerable to the Y2K problem. Our ability to fly hundreds of sorties in a limited airspace is dependent on real-time communication with friendly forces over the Have Quick radio system while denying our enemies the ability to jam or overhear those transmissions. Our ability to detect and assess enemy missile launches depends on satellite hardware and software, communication links, threat analysis software systems, and then communication links to end users. Our ability to launch and complete sorties relies on a multitude of different software and hardware systems: air traffic control, radars, avionics, secure communications, Global Positioning System, mission planning systems and equipment, ordinance avionics, automated test equipment, and simulators, to name a few.

All these systems have two things in common: They process and convey information to the operator, and they are controlled to some degree by *automated* information technology. Not all are "date-aware," but our task is to find out which ones are and to fix them.

What We Have Done to Date

The U.S. Air Force Y2K effort is being carried out by two program management teams, one at the Air Force Communication and Information Center and one at the Air Force Communications Agency. These two teams are supplemented by program offices that reside in each major command (MAJCOM), Field Operating Agency, and Direct Reporting Unit that function as an extension of the headquarters staffs. In addition, the Air Force has fully engaged the functional staffs, assigning responsibility for comprehensive inventories Air Force-wide, researching the compliance information for each item, and sharing this data within their domains to the commanders they support.

There are over 200 primary Y2K points of contact Air Force-wide working full time on this issue. This information and more is found on the Air Force Y2K Web page (http://year2000.af.mil), which is one of the best and most comprehensive resources in the world for information, guidance, and current status of our effort. We have an Internet-hosted on-line, real-time database that provides instant status and access to all the over 3,400 systems we are tracking in the Y2K program. We have created three different guidance packages to direct efforts in the field and have trained over 900 people worldwide in an Air Force-developed and standardized certification process. To sum it up, we have energized the Air Force Y2K effort by mobilizing the support communities, thus ensuring their own domains are squared away for Y2K.

What We Need to Do Now

To date, the communication and information and other support communities have been the "pointy head of the Y2K spear." That is, we are solving the Y2K problem through a process of elimination—systems we are aware of are identified and then systematically renovated through the standard Y2K lifecycle documented in the Air Force Guidance Package.

How can we know we have identified the entire universe of systems—hardware, software, technology-controlled equipment—that the Air Force depends on to complete all our missions? We need to engage the operational communities at every level to leverage their knowledge of mission processes. This is the only way to guarantee that all our critical missions are free from negative Y2K impacts.

By engaging the operational communities and the systems they employ to carry out wartime operations, we can identify critical mission processes and components previously missed. We need to be working off the commander in chief's designated mission-critical systems listing to ensure that all electronic pathways to and from these systems are Y2K compliant. Because so much of our operational capability is maintained and executed at contingency sites and deployed locations, Y2K vulnerability analysis needs to be performed on the mission processes employed there. MAJCOMs and main operating bases need to ensure that operational planning processes and systems that direct and employ forces at these locations are Y2K ready.

Only through this analysis can we identify the most critical wartime processes and ensure that adequate contingencies have been properly identified and documented. It is time to make the operational mission the pointy head of the spear—we cannot afford to continue looking at the problem from a purely functional perspective. We must widen our scope to look at the entire Air Force as a whole system to find out where we are most vulnerable. The bottom line is that on Jan. 1, 2000, Y2K mission impacts will hinder the commander in chiefs' abilities to perform their missions—it will be too late to do these things that we should be doing now.

The Y2K problem is not just a communication problem—its an Air Force mission problem. The program management office here at Scott Air Force Base encourages everybody to look at their jobs and their units' missions from a Y2K perspective. How will it affect your duties and ability to support the mission? How will if affect your unit's ability to perform its mission? Find out what is being done at your unit and then take appropriate actions to raise issues and contribute to the solution. The Air Force relies on every person so that it can be the greatest air and space force in history; the way we must handle the Y2K problem is no different. Our success depends on having every individual take personal responsibility for Y2K.

Summary

History has proven Warden's theories to be correct. The new paradigm for war in this technology and information-based age is to directly influence the enemy's leadership by affecting his capability to function as a cohesive system. Blind the enemy's leadership by cutting off communications, taint their information or prevent them from receiving it, disrupt key production facilities and other national infrastructure to deflate national morale, and inflict choke points. By denying an enemy any one of these capabilities, an aggressor gains significant advantage. If the Y2K issue is not adequately addressed, we will allow all these things to happen to our National Command Authorities. Our enemies, *all of them*, will achieve these advantages, simultaneously, without any effort on their part. Y2K is the Pearl Harbor of the 21st century just waiting to happen, but only if we let it. ◆

About the Author

Lt. Col. Scott B. Dufaud is deputy program manager for the U.S. Air Force Year 2000 Program Management Office at the Air Force Communications Agency (AFCA), Scott AFB, Ill. Prior to assuming these duties in November 1996, he was the chief of the Software Management Division at AFCA. Dufaud specializes in software management issues, software engineering process groups, software process improvement via the Capability Maturity Model, technology insertion, and issues of accelerating organizational change. He previously served at Headquarters Strategic Air Command and U.S. Strategic Command, the Air Force Manpower and Personnel Center, and Headquarters Air Force Space Command. He has a bachelor's degree in computer science from Southwest Texas State University and a master's degree in systems management from the University of Southern California.

Voice: 618-256-5697 DSN 576-5697
Fax: 618-256-2874 DSN 576-2874
E-mail: scott.dufaud@scott.af.mil
Internet: http://year2000.af.mil

References

1. Reynolds, Col. Richard T., *Heart of the Storm*, Vol. 1, Air University Press, Maxwell Air Force Base, Ala., January 1995, p. 17.
2. Warden III, John A. and Karl P. Magyar, "Air Theory for the Twenty-First Century," *Challenge and Response*, Air University Press, Maxwell Air Force Base, Ala., August 1994, pp. 322-324.
3. Gabriel, Richard A., "Grenada," Air Command and Staff College Seminar and Correspondence Lesson Book 8, Ver. 10, Maxwell Air Force Base, Ala., pp. 32-44.