

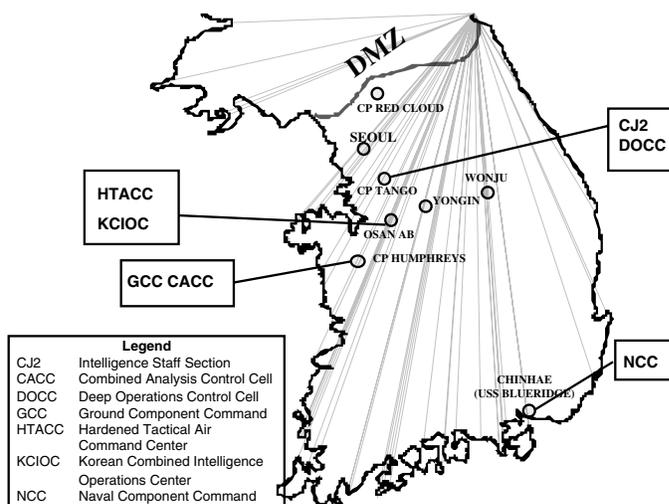
# UPDATE ON THE YEAR 2000 (Y2K): OPERATIONAL EVALUATION EFFORT

## CAPITALIZING ON THE Y2K EXPERIENCE

As everyone knows, the Year 2000 clock rollover turned out to be uneventful around the world. For the Department of Defense, major credit goes to the systematic planning and fixing that ensured that C<sup>4</sup>I and information systems were ready to operate in the Y2K environment. In addition to the January 1, 2000 clock roll, there were concerns about the February 28-29 and March 1 rollovers. Since almost all of the systems and applications had been checked during the CINC OPEVALS in 1999, there were no surprises on these dates.

DOT&E's FY00 effort primarily focused on documenting the Y2K evaluation methodology and lessons learned. We then applied what we had learned in assessments of C<sup>4</sup>I systems of United States Forces Korea (USFK) and Joint Forces Command (JFCOM).

Since the conclusion of the Y2K OPEVALS, DOT&E has continued initiatives resulting from the Y2K work. We sponsored representatives at the U.S. European Command, the Joint Forces Command, and United States Forces Korea, who work in areas related to operations planning, C<sup>3</sup>, and interoperability. During August 2000, for example, we sent a team of nine people to support activities of USFK's annual Ulchi-Focus Lens 2000 command post exercise. This effort, which used the *thin lines* methodology developed for the Y2K OPEVALS, concentrated on activities related to understanding and improving operational processes for preparing target nominations in the development of the Integrated Tasking Order, and on intelligence dissemination with emphasis on requests for information and intelligence summaries. Our team's observations once again illustrated the complex interoperability demands of modern, computer-based Command, Control, Communication, Computer, and Intelligence (C<sup>4</sup>I) systems, and aided USFK in meeting the extensive challenges of combined forces military operations. Figure 1 depicts the Korean locations for the Ulchi-Focus Lens effort.



**FIGURE 1. Leveraging Y2K Methodology for USFK**

We will continue similar initiatives with other theaters so that the United States' Unified Commanders will be able to respond quickly to contingencies or threats to our vital national interests.

## **BACKGROUND INFORMATION**

With the approach of the Year 2000 and the potential for catastrophic computer system problems, the Department of Defense began an extensive project intended to forestall trouble. Investing some \$3.6 billion over 5 fiscal years, the Services, Agencies, and the Unified Commands looked into all possible areas where the millennium bug might appear. This culminated in an extensive series of operational evaluations by the Unified Commands, which found few substantive Y2K hazards, but did disclose some important interoperability problems. Although DoD had expected to unearth a lot of Y2K difficulties, the real benefit of the effort was to point out the need for continued attention to interoperability in our complicated C<sup>4</sup>I system-of-systems.

Spending such a large amount of money brought with it the question, "Was it worth it?" In fact, it was money well spent. The greatest advantage came first in having the various CINCs determine the *thin lines* of mission critical command and control systems, and then in verifying warfighting system interoperability via operational evaluations. Thin lines are those minimum essential C<sup>4</sup>I systems that allow each command to meet its critical mission and operational requirements; they would be the linchpin of operations in any contingency in a Y2K environment. Without this C<sup>4</sup>I system-of-systems, modern military operations would not be possible. Moreover, the concept of defining and understanding the C<sup>4</sup>I thin lines did not exist before DoD undertook this Y2K evaluation effort; how ready the commands would have been for war in the Year 2000 without the corrections we have made is problematical. We have, however, made such substantial improvements in understanding our C<sup>4</sup>I systems that one cannot deny the value of our accomplishments.

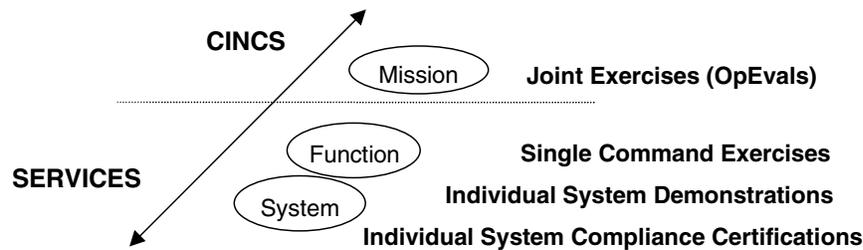
## **THE METHODOLOGY**

DOT&E provided support for Y2K verification activities worldwide, including expert assistance for cross-functional, inter-Service, and cross-system testing. The amount of effort that DOT&E provided varied by command, and was governed by the nature and complexity of each situation. The European Command (EUCOM) was heavily involved with the air war over Serbia; thus, DOT&E representatives assisted in key OPEVAL planning and conduct of the operational evaluations. Because of the rapid turnover of people assigned to Korea and the relatively small staff there, DOT&E, along with contractor support, made up a substantial part of the evaluation planning and assessment team. DOT&E contributed significantly to OPEVAL planning and execution in all of the commands.

Some of the most commonly recurring systems in the evaluations were the Local Area Networks (LANs), various electronic mail applications, secure and normal voice telephone and facsimile, the Secret Internet Protocol (SIPRNET), and the unclassified but sensitive Internet protocol (NIPRNET). In addition, each command evaluated a number of unique programs and applications. The most commonly encountered systems and applications fell in to three basic categories:

- Global Command and Control and Related Systems or Applications
- Intelligence Related Systems and Applications
- Communications

The Services conducted tests of individual systems at the program manager and command function levels. These tests were the basis for certifying individual systems as Y2K compliant. Subsequent CINC OPEVALs concentrated on mission-level activities, and primarily tested compliant systems for system-to-system interoperability in executing critical missions. Each CINC, however, oversaw and supervised testing the thin lines from sensor to shooter by his components and supporting agencies. Figure 2 illustrates Service/CINC evaluation responsibilities.



**Figure 2. Service and CINC Y2K Verification Activities**

Through extensive OPEVAL planning, the Department of Defense identified 2,107 mission critical systems and 4,749 non-mission critical systems. Of the 2,107, the Joint Staff included 452 in their Master CINC Thin Line List; these were the primary systems addressed during the CINC Y2K OPEVALs. It was not necessary to evaluate each of the 452, however. Several were trusted systems and some had no date processing functions, leaving a total of 358. The individual Services or Agencies tested and evaluated the remainder, ensuring that they became Y2K compliant, if necessary.

All of the commands learned a great deal about their current capabilities as well as how they can be improved. Perhaps the most important single benefit came from the homework that needed to be done prior to the exercises. To prepare for the OPEVALs, the commands identified their critical missions and subordinate critical mission support tasks, and then developed their thin lines according to their mission requirements. Thus, a major result of the Y2K OPEVALs was the definition and critical review by the Unified Commands of their C<sup>4</sup>ISR infrastructure from the perspective of operational rather than technical capability. Upon analyzing their enterprise processes, the CINCS found only a third of their systems, on average, to be critical.

**THE OUTCOME: RELEARNING INTEROPERABILITY AND CONFIGURATION MANAGEMENT LESSONS**

The OPEVALs were, in general, very successful, detecting a total of 34 hard failures and 8 soft failures. Specific Y2K-related failures are classified. Table 1 depicts the type of Y2K faults noted and the actions taken to fix them.

**Table 1. CINC OPEVAL System Failures**

CINC	Hard Failure	Soft Failure	STATUS				
			Fixed H / S	Under Review H / S	Delayed Fielding H / S	Fix Planned H / S	No Action H / S
JFCOM	3	0	3/0	0	0	0	0
CENTCOM	5	0	1/0	1	2	0	1
EUCOM	2	0	2 / 0	0	0	0	0
PACOM	2	0	2 / 0	0	0	0	0
USFK	5	0	2 / 0	0	0	1	2
SOCOM	3	0	0 / 0	0	0	1	2
SOUTHCOM	1	0	1 / 0	0	0	0	0
SPACECOM	4	4	2 / 3	2 / 0	0 / 0	0 / 0	0 / 1
NORAD	1	2	1 / 2	0	0	0	0
STRATCOM	0	0	0	0	0	0	0
TRANSCOM	8	2	5 / 0	0 / 1	0 / 0	0 / 1	3 / 0
<b>TOTAL</b>	<b>34</b>	<b>8</b>	<b>19 / 5</b>	<b>3 / 1</b>	<b>2 / 0</b>	<b>2 / 1</b>	<b>8 / 1</b>

**Legend:**

H / S = Hard Failure/ Soft Failure

No Action = No Action Taken; No good fix currently available; No fix planned; or No fix--System to be Replaced.

Throughout the OPEVALs, two issues appeared among the commands with some regularity. First was the need for *continuous configuration management*. Often, agencies or offices had installed new or different applications or programs on their computers. These differences prevented locations or offices from communicating with each other unless the applications became standard. Despite efforts to control configuration management, another difficulty cropped up everywhere: incompletely addressed or unresolved problems with *joint interoperability*. Configuration management was vital to ensure that the command had installed and used only Y2K-certified systems and applications. Joint interoperability problems arose because many commands and Services employed systems that, although aimed at similar goals, could not work together or be accessed and employed by others, thus causing needless duplication and work. The two issues overlapped when commands or components used different versions of the same application or system, thus rendering them wholly or partially incompatible.

The commands also encountered an old problem that nobody should forget: organizations had failed to exercise their systems and capabilities to make sure that they worked. For example, one of the commands held a rehearsal of staff activities for the Y2K rollover period. This command intended to use satellite communication terminals and UHF and EHF radios in the event its computer-based systems failed. These backup systems had not been used for extended time periods, several years for some of the pieces. When the rehearsal began, the players discovered that all of the equipment had been stored or turned off for so long that *none* of the alternate communications worked. Several days elapsed before parts could be obtained to correct the problems or bring the equipment up to date.

CINCs found that they could perform their critical missions during and after Y2K date changes. The tests found several problems with thin line systems, both Y2K and non-Y2K related. These were generally resolved using alternate systems plus manual procedures short of full contingency plans. Y2K problems consisted of three types. Some were system interoperability failures, in which each of two systems operated as intended but the systems had a Y2K interoperability problem. In other cases,

systems and peripherals such as printers did not interoperate properly. Sometimes, systems that had previously been certified as Y2K compliant had newly identified Y2K system failures. These Y2K problems consisted of such simple things as incorrect dates on message headers or facsimile transmissions, with no other effects on content, function, or operation. In other cases, the problems were severe enough to cause incorrect transmission or exchange of data or imagery.

Non-Y2K problems discovered during the OPEVALs centered on issues of configuration management and the tendency for people to install new versions of a variety of applications or systems on their computers without regard to Y2K certification, as well as problems with joint interoperability. Non-Y2K issues also included previously unrecognized, everyday midnight crossing anomalies, obsolete software on particular installations, and known bugs that were to be corrected in software updates. Usually, the non-Y2K problems were corrected prior to the end of an OPEVAL, but configuration management difficulties were prevalent and presented a major area requiring attention by commanders.

### **THE IMPORTANCE OF CONTINUED INTEROPERABILITY EVALUATIONS**

Since the C<sup>4</sup>ISR infrastructure is in a state of continual change, and because the OPEVALs helped in identifying C<sup>4</sup>ISR architectures and thin line critical systems, the Department of Defense should consider institutionalizing the periodic conduct of OPEVALs, focusing on interoperability possibly once every three or four years. Several agencies could assist such evaluations, including the new Director of Interoperability, the Joint Interoperability Test Center, Joint Forces Command, and DOT&E. Such periodic exercises would update the Unified Commands' assessments of their ability to meet mission requirements, allow them to verify interoperability of existing systems and new programs, and identify those systems that could be eliminated. A recurring issue throughout all of the commands was the realization that people and agencies that believe they are working with similar (even the same) programs find out that these systems do not always interoperate flawlessly. The Y2K OPEVALs illustrated that to have systems and users ready for an emergency, they and the people who operate them must be exercised frequently.

