Strategic Management of Information and Communication Technology: The United States Air Force Experience with Y2K

Mark Haselkorn, Principal Investigator, National Research Council

ISBN: 0-309-11129-3, 142 pages, 8 1/2 x 11, (2007)

Strategic Management of Information and Communication Technology: The United States Air Force Experience with Y2K

Mark Haselkorn, ***Principal Investigator***

Policy and Global Affairs

Computer Science and Telecommunications Board
Division on Engineering and Physical Sciences

NATIONAL RESEARCH COUNCIL
OF THE NATIONAL ACADEMIES

THE NATIONAL ACADEMIES PRESS
Washington, D.C.
www.nap.edu

THE NATIONAL ACADEMIES PRESS 500 Fifth Street, N.W. Washington, DC 20001

NOTICE: The project that is the subject of this report was approved by the Governing Board of the National Research Council, whose members are drawn from the councils of the National Academy of Sciences, the National Academy of Engineering, and the Institute of Medicine. The principal investigator and members of the advisory committee responsible for the report were chosen for their special competences and with regard for appropriate balance.

This study was supported by Contract No. V101(93)P-1637, TO #17 between the National Academy of Sciences and the United States Air Force and a grant from the Institute of Electrical and Electronics Engineers, Inc. Any opinions, findings, conclusions, or recommendations expressed in this publication are those of the author and do not necessarily reflect the views of the organizations or agencies that provided support for the project.

International Standard Book Number 13: 978-0-309-11128-7
International Standard Book Number 10: 0-309-11128-5

Additional copies of this report are available from the National Academies Press, 500 Fifth Street, N.W., Lockbox 285, Washington, DC 20055; (800) 624-6242 or (202) 334-3313 (in the Washington metropolitan area); Internet, http://www.nap.edu.

Suggested citation: National Research Council (2007). *Strategic Management of Information and Communication Technology: The United States Air Force Experience with Y2K*. Mark Haselkorn, Principal Investigator. Policy and Global Affairs. Washington, D.C.: The National Academies Press.

Printed in the United States of America

THE NATIONAL ACADEMIES

Advisers to the Nation on Science, Engineering, and Medicine

The **National Academy of Sciences** is a private, nonprofit, self-perpetuating society of distinguished scholars engaged in scientific and engineering research, dedicated to the furtherance of science and technology and to their use for the general welfare. Upon the authority of the charter granted to it by the Congress in 1863, the Academy has a mandate that requires it to advise the federal government on scientific and technical matters. Dr. Ralph J. Cicerone is president of the National Academy of Sciences.

The **National Academy of Engineering** was established in 1964, under the charter of the National Academy of Sciences, as a parallel organization of outstanding engineers. It is autonomous in its administration and in the selection of its members, sharing with the National Academy of Sciences the responsibility for advising the federal government. The National Academy of Engineering also sponsors engineering programs aimed at meeting national needs, encourages education and research, and recognizes the superior achievements of engineers. Dr. Charles M. Vest is president of the National Academy of Engineering.

The **Institute of Medicine** was established in 1970 by the National Academy of Sciences to secure the services of eminent members of appropriate professions in the examination of policy matters pertaining to the health of the public. The Institute acts under the responsibility given to the National Academy of Sciences by its congressional charter to be an adviser to the federal government and, upon its own initiative, to identify issues of medical care, research, and education. Dr. Harvey V. Fineberg is president of the Institute of Medicine.

The **National Research Council** was organized by the National Academy of Sciences in 1916 to associate the broad community of science and technology with the Academy's purposes of furthering knowledge and advising the federal government. Functioning in accordance with general policies determined by the Academy, the Council has become the principal operating agency of both the National Academy of Sciences and the National Academy of Engineering in providing services to the government, the public, and the scientific and engineering communities. The Council is administered jointly by both Academies and the Institute of Medicine. Dr. Ralph J. Cicerone and Dr. Charles M. Vest are chair and vice chair, respectively, of the National Research Council.

www.national-academies.org

PRINCIPAL INVESTIGATOR

Mark Haselkorn, University of Washington

ADVISORY COMMITTEE

Ernest J. Wilson III (Chair), University of Maryland, College Park

Chris Demchak, University of Arizona

Robert W. Lucky, Telcordia Technologies, Inc. [Retired]

Anthony Valletta, SRA International, Inc.

Staff

Thomas Arrison, Project Director, Policy and Global Affairs (2005–2007)

Michael Cheetham, Project Director, Policy and Global Affairs (until 2004)

Jo Husbands, Senior Project Director, Policy and Global Affairs

Herb Lin, Senior Scientist, Computer Science and Telecommunications Board, Division on Engineering and Physical Sciences

Shalom Flank, Consultant, Computer Science and Telecommunications Board, Division on Engineering and Physical Sciences

Sponsors

United States Air Force

Institute of Electrical and Electronics Engineers, Inc. (IEEE)

PREFACE

This report grew out of a National Research Council (NRC) project titled "Managing Vulnerabilities Arising from Global Infrastructure Interdependencies: Learning from Y2K." In mid-1998 the NRC initiated planning meetings to take advantage of what was then perceived as "an extraordinary opportunity to learn…how various factors, including current management structures and practices, impact…risk that threatens serious damage to information and other critical infrastructures." The initial focus was on vulnerabilities stemming from "the interconnectedness of complex 'systems of systems,'" with the goal to gather data on such systems both before and after the December 31, 1999, rollover to the Year 2000 (Y2K).

In early 1999 the Institute of Electrical and Electronics Engineers became a sponsor of the project. In mid-1999 the NRC began working with Air Force personnel from Information Warfare Defense (a unit attached directly to operations in headquarters) and the Air Force Y2K Office to establish a case study. Dr. Mark Haselkorn of the University of Washington was appointed as principal investigator to conduct the research and write up the results of the case study. An advisory committee was also appointed to provide general guidance.

In November and December 1999, Dr. Haselkorn conducted several sets of interviews at a stateside Air Force base and at an overseas Air Force base. After the end-of-year rollover, in February and March 2000, he repeated the process. These interviews involved not only base working groups but also policy-making units at the major command and headquarters levels. He also conducted supporting phone interviews throughout the project. On April 14, 2000, an all-day Air Force–wide Y2K Lessons Learned Workshop was held in Washington, D.C. (A detailed list of the groups interviewed is provided in Appendix B.) In the 18 months following the workshop, Dr. Haselkorn compiled the results of the interviews and the workshop and summarized his findings. This paper represents the results of Dr. Haselkorn's research. The views expressed are those of the principal investigator and do not necessarily represent positions of the advisory committee, the National Academies, or the sponsoring organizations.

This paper has been reviewed in draft form by individuals chosen for their expertise, in accordance with procedures approved by the National Academies Report Review Committee. The purpose of this independent review is to provide candid and critical comments that will ensure that the report meets institutional standards for quality. The review comments and draft manuscript remain confidential to protect the integrity of the process. In addition to external reviewers, two members of the original advisory committee also reviewed Dr. Haselkorn's draft report.

We wish to thank the following individuals for their review of this paper: John L. King, University of Michigan; John Koskinen, U.S. Soccer Foundation; Bruce McConnell, McConnell International, LLC; David Mussington, RAND Corporation; Walter Scacchi, University of California, Irvine; Anthony Valletta, SRA International, Inc.; and Ernest J. Wilson III, University of Maryland, College Park.

Although the reviewers listed above have provided many constructive comments and suggestions, they were not asked to endorse the content of the report, nor did they see the final draft of the report before its release. Robert Frosch, Harvard University, oversaw the review of this report. Appointed by the National Academies, he was responsible for making certain that an independent examination of this report was carried out in accordance with institutional procedures and that all review comments were carefully considered. Responsibility for the final content of this report rests entirely with the principal investigator and the institution.

PRINCIPAL INVESTIGATOR'S NOTE

Most of the following report was written prior to the events of September 11, 2001, the Southeast Asian tsunami in 2004, and Hurricane Katrina in 2005, yet the lessons learned from Y2K are still relevant in the aftermath of these devastating events. September 11 was a tragic demonstration of the need for more comprehensive and dynamic strategies for managing our critical systems, as well as the need to base these strategies on an effective communication infrastructure that links and coordinates key participants from disparate organizational entities. Similarly, disasters like the tsunami and Katrina demonstrated the damaging effects that an incomplete plan for strategic management of information and communication systems could have on the coordination and delivery of emergency services.

This is an account of the efforts of one large, highly diverse, technologically dependent global organization, the United States Air Force (hereafter simply USAF, or Air Force), to address a widely dispersed threat to its information infrastructure, namely the rollover to the Year 2000 (Y2K). The specific information and communication systems discussed in this report are simultaneously critical operational systems themselves and vital components of the communication infrastructure that supports other critical systems. In other words, these systems are simultaneously something to be protected and part of the system for protection.

The Air Force response to Y2K evolved over more than five years. It ultimately involved thousands of people throughout the 108 USAF bases, interacting in varying, often nontraditional ways to address perceived threats. In addition, hundreds more people at numerous major Air Force units were active in developing guidance and support packages and in monitoring their implementation, while personnel involved in the acquisition, design, development, fielding, and maintenance of systems and applications also responded from their particular perspectives. Whatever the state of an organization's strategic management of information and communications technology (ICT), Y2K stressed existing practices in ways they had never previously been stressed.

This report presents the lessons of the Air Force Y2K experience under three interrelated headings: (1) lessons for managing ICT complexity, (2) lessons for aligning organizational and ICT strategies, and (3) lessons for minimizing ICT risk, including security, information assurance, and infrastructure protection. In each area, lessons are derived from the analysis of interrelated and dynamic responses of various Air Force elements to the perceived threats of Y2K. These lessons are preceded by discussion of background issues that provides necessary context, particularly aspects of ICT in general, Air Force ICT in particular, and theY2K problem itself. The report concludes by turning the lessons into recommendations for improving Air Force management of information and its supporting infrastructure and discussing the implications of these lessons for other organizations.

This report does not in any way constitute an evaluation of the Air Force's response to Y2K. Such an undertaking would have required a broader look at the entire organization and a deeper look at component units. It would also require collecting sufficient data from other organizations to allow one to compare the Air Force response to institutions of similar size and complexity. Such an exploration would have been worthwhile, but it was beyond the scope and resources available for this effort.

The fact that Y2K did not result in widespread catastrophic failures has led many people to quickly forget the experience, yet the lack of obvious impact makes it a rich source of critical lessons for strategic management of information and communication technology. Rather than being an account of fundamental flaws and cascading effects, this report is about maintenance and modernization, life-cycle management of systems and software, functional interdependency and continuity, guidance policies and certification, system ownership and responsibility, training and organizational roles, security and information assurance, and system vulnerability and robustness. Y2K tested the evolving Air Force system for management, modernization, and protection of information and its supporting infrastructure.

Without the contributions and generous involvement of numerous individuals, particularly the more than 100 people who provided me with information and support in setting up and conducting interviews, this study would not have been possible. I would particularly like to thank Brig. Gen. Gary Ambrose, Lt. Col. Gregory Rattray, and Maj. John Bansemer of the USAF; Tom Arrison, Michael Cheetham, John Boright, and Jo Husbands of NRC Policy and Global Affairs; Herb Lin and Shalom Flank of the NRC Computer Science and Telecommunications Board; Dr. Joseph Bordogna and Dr. Kenneth Laker, 1998 and 1999 presidents of the IEEE, respectively; and Adam Peake of the Center for Global Communications in Tokyo, Japan. I would like to thank Luke Maki of the Boeing Corporation for reviewing some early chapter drafts. I would also like to thank the members of the project advisory committee: Ernest J. Wilson III (Chair), Chris Demchak, Robert W. Lucky, and Anthony Valletta.

Finally, I would like to thank the project sponsors, the Air Force and IEEE.

Mark Haselkorn
Principal Investigator

CONTENTS

BOX AND FIGURES

BOX

FIGURES

SUMMARY

This report describes lessons learned from the efforts of the United States Air Force (hereafter simply USAF, or Air Force) to address a widely dispersed threat to its information infrastructure. The Air Force's response to the Year 2000 (Y2K) evolved over more than five years and involved thousands of people throughout the 108 USAF bases, interacting in varying, often nontraditional ways to address perceived threats. In addition, hundreds more people at numerous major Air Force units were active in developing guidance and support packages and in monitoring their implementation.

This report is perhaps the most detailed publicly available case study of the Y2K response in a single organization and the lessons learned from that response. Although a great deal was written about Y2K before the event, surprisingly little analysis was conducted after January 1, 2000 (see Box 1-1). The fact that Y2K did not result in widespread catastrophic failures has led many people, particularly those outside the information and communications technology (ICT) field, to label it a nonevent or even a hoax—and doubtless discouraged extensive analysis after the fact.

However, as this report makes clear, the experience serves as a source of critical lessons for strategic management of ICT and echoes earlier findings of analysts in the field of information systems management. In addition, other sources make it clear that enough problems were experienced in the course of the Y2K rollover to demonstrate the reality of the problem and the importance of remediation efforts (GAO 2000). Serious known disruptions were avoided in the banking and insurance sectors, two NATO nation spy satellites went down for two days, and numerous other documented failures were either avoided or responded to in real time during rollover.

These lessons and related recommendations are described in Chapters 2, 3, and 4, and they cover the management of ICT complexity, aligning organizational and ICT strategies, and minimizing and mitigating ICT risk. A final brief concluding chapter focuses on the general lesson of viewing technology risk within its social and organizational context. Together, these chapters present general implications for large, complex organizations that rely on ICT to achieve their mission in the face of risks in such areas as information assurance, information security, and critical infrastructure protection (CIP). The recommendations, naturally, focus on the Air Force and its context, but they are applicable to other large, complex, ICT-dependent organizations as well.

The fact that Y2K did not produce major sustained disruption for the Air Force or other organizations makes it a *more* valuable source for long-term lessons for operational and strategic management of ICT systems. Rather than focusing on fundamental flaws and cascading effects, the bulk of this analysis is relevant to the overall strategic management of ICT, including maintenance and modernization, life-cycle management of systems and software, functional interdependency and continuity, guidance policies and certification, system ownership and responsibility, training and organizational roles, and security and information assurance.

Background of the Project

The report grew out of an effort by the National Research Council (NRC) and other groups, such as the Institute of Electrical and Electronics Engineers (IEEE), to observe lessons from the Y2K experience that might be applied to CIP and other areas. The assumption was that there would be a number of critical, highly visible failures. Y2K could be studied as a surrogate for information warfare attacks, with the ultimate goal of making systems more resistant.

Planning meetings were organized in mid-1998. In mid-1999 NRC volunteers and staff began working with Air Force personnel from the Information Warfare Defense (a unit attached directly to operations in headquarters) and the Air Force Y2K Office (AFY2KO) to establish the case study. Interviews were conducted at a continental United States (CONUS) base and an outside the continental United States (OCONUS) base before and after the end-of-year rollover. These interviews involved not only base working groups but also policy-making units at the major command (MAJCOM) and headquarters (HQ) levels. Supporting telephone interviews were conducted throughout the project. On April 14, 2000, an all-day Air Force–wide Y2K Lessons Learned Workshop was held in Washington, DC.

Staff turnover at the NRC resulted in significant delays in the completion and publication of the report. Notwithstanding the delays, the author and the NRC believe that the insights generated by the project have long-term relevance and merit a wide audience.

The Air Force and Y2K: Shifts in Perception

ICT is critical to almost all Air Force mission and functional objectives, including maintaining readiness in the face of uncertainty. While information warfare, offensive and defensive, may be a unique element of the military management challenge, the Air Force's concern that increased functionality and connectivity can lead to increased vulnerability is relevant for any technology-dependent organization. While security risks generally arise from outside threats to systems, threats to information assurance often emerge from internal system complexities.

The Air Force encompasses nine major commands and has a complex organization for managing and funding ICT. Responsibility lies in the Chief Information Officer's office, but as in other large and diverse organizations, there is a wide gap between the executive agency and the distributed, frontline, operational management and use of ICT.

Ensuring the availability of experienced ICT personnel also presents challenges. For the Air Force, these include competition with the private sector and regular shifting of personnel (temporary duty, or TDY). As the Air Force is highly dispersed geographically, functional units may face very different environments, funding, and infrastructure, particularly CONUS versus OCONUS bases.

A variety of perceptions became attached to the Y2K problem, both before and after. The widespread attention and news coverage linking the event with the new millennium, along with frequent mention of possible catastrophic failures, fostered numerous misconceptions of the problem but was helpful in ensuring that resources were

available and that organizations put procedures in place to respond. The coverage also produced anxieties and expectations that, fortunately, were not realized, but they may make it more difficult to appreciate the lessons learned.

Within the Air Force, perception and response strategies shifted over time. The Air Force recognized the problem early because computer professionals working on specific systems brought it to light in the early and mid-1990s. By 1997 awareness mushroomed, and the emphasis widened from ICT and electronic data to include embedded chips and traditional infrastructure.

There was also a shift from a technological to a mission perspective. It became apparent that the problem was too complicated for any one functional area, including ICT, to handle by itself. The first step was often to conduct an inventory with the goal of determining compliance, but system complexity, definitional uncertainties (for instance, what is "compliance?"), and a lack of clarity about ownership and responsibility complicated this.

Early on, the Air Force played a key role in developing government-wide approaches focused heavily on finding, fixing, and testing mission critical systems. Over time, however, it became clear that it would be impossible to test everything in advance of the rollover. Therefore, there was a shift from fixes to continuity planning. By 1999 complex efforts to complete and validate system renovations began to conflict with equally complex efforts to develop and prepare viable contingency plans.

Finally, there was a shift in focus from technology to legal and political issues. Early on, the legal staffs of corporations became involved. In July 1998, the Year 2000 Information Disclosure Act was passed, providing liability protection from inaccurate statements made by organizations acting in good faith when sharing Y2K information. Congressional and Government Accounting Office attention was part of the management environment.

Lessons for Managing ICT Complexity

Participants in the Air Force's response to Y2K learned more about organizational operation and management than about technology. It became clear that traditional management strategies based on localized response would not be effective and that a more comprehensive approach was needed. For many organizations, including the Air Force, Y2K was the first time they needed to manage a single ICT project that cut across the entire organization. The pervasiveness of the problem and the interdependency of organizations and systems meant that Y2K could not be addressed by breaking the response into discrete components. Interdependency also meant that no single group could fully control the response. The Air Force, like many organizations, created a temporary Y2K office to manage the problem—no existing office could do the job.

While common objectives and deadlines across the entire organization made Y2K a unique ICT project, the issues and conditions it revealed are relevant to any strategic ICT project that goes beyond a given functional area. Mergers, deployment of major systems in large organizations, and systems to facilitate interagency coordination are examples of efforts that are often undermined by the failure to fully understand and appropriately address organizational and system interdependencies.

Fortunately, Air Force recognition of the Y2K problem was early and widespread. The perception that everyone would be impacted in the same way at the same time—there was a common enemy and a set deadline—contributed to this heightened awareness. As the Air Force's approach took shape, it reflected several lessons that are highly relevant to the management of ICT complexity in general.

- **Enterprise-wide ICT management requires broader, more integrated efforts.**

Early on, it became clear that it would be impossible for individual commands and units to define the problem, set priorities, and track response efforts on their own. For example, commands and units made attempts to stratify response needs by the criticality of the system, the likelihood of an adverse occurrence, local conditions, and optimal response strategies. However, the translation from critical missions to critical systems was not straightforward, and classification schemes could not be developed that translated well across different commands and units. No existing unit had the scope or authority to coordinate a cross-organizational ICT project.

- **The focus of ICT management must shift from hardware and software to data, knowledge, and organizational goals.**

Over time, it became clear that the key priority for Y2K response was the protection of data as they serve organizational goals—fixing just hardware and software was not sufficient. Once IT professionals recognized this, the focus of the Y2K response shifted to the operational use of data.

- **The organizational information strategy must align ICT and operational goals.**

As the Air Force response to Y2K took shape, operational and strategic managers who saw themselves on the periphery of ICT were thrust into its center. For the Air Force and others organizations, *Y2K represented the first large-scale, formal effort to align ICT management with operational and strategic management.* The challenge of integrating ICT and strategic management was perhaps the most significant aspect of Y2K and is covered in more detail in the next section.

- **ICT must be managed cross-functionally.**

Information in organizations tends to flow along functional lines. The success of the Air Force's Y2K response depended on overcoming this "stovepiping" tendency. Even at early inventory and assessment stages, it was important to maintain a functional perspective toward ownership and responsibility. This was difficult for several reasons: (1) the need to comply with multiple guidance and unique reporting requirements; (2) the underbudgeting of man-hours; (3) an increased workload for communication; and (4) the need to keep up with directives and changes in directives. Until a temporary cross-functional entity to oversee the Y2K response was established and headed by someone

who represented the core value of the organization (in the Air Force's case, a pilot/general), no unit had the perspective and authority to coordinate this effort.

- **The overall information strategy must center on people, information, and mission.**

Y2K taught organizational ICT leaders that they needed to develop an enterprise-wide information strategy that would be aligned with the overall organizational strategy. Over time, Y2K caused these leaders to focus less on specific technologies and more on the effective use of information by people in support of overall organizational missions. In doing this, ICT leaders demonstrated the value of an integrated, cross-functional perspective beyond Y2K.

- **Do not return to business as usual.**

As a cross-enterprise activity, Y2K forced people to grapple with complex issues that were not fully under their control. This is not a particularly comfortable position for most people. With the passing of the crisis, there was a natural tendency to seek a return to more familiar methods and roles. Some changes made in response to Y2K have become part of new business as usual practice, while other changes that were lost need to be rediscovered.

Lessons for Aligning Organizational and ICT Strategies

Traditionally, the strategic management of organizations and the operational management of ICT in those organizations have displayed significant differences. ICT management tends to focus on short-term needs, is technically based, and occasionally experiences failures as part of the job. Strategic management of an organization tends to be negotiated, focuses on longer-term and wider-range impacts, and can view failure as career threatening.

ICT and operational personnel were brought together in new ways by Y2K, as the Air Force example illustrates. Early on, when Y2K was seen as an "IT issue," resources were hard to come by. Later, attention from higher levels of management resulted in more resources being made available, but that attention also required ICT personnel to take account of a much lower tolerance for risk from upper-level managers.

Complete, final alignment between organizational and ICT strategies is not sustainable because the strategic context changes constantly, as does the ICT portfolio. Nevertheless, achieving a dynamic alignment is increasingly important for both sides of the operational-ICT divide. The Y2K experience highlights several key areas of emphasis and underlying tensions in this necessary process.

- **Central management and local execution must be balanced.**

Both central and local perspectives are "right" and have value, yet they are often in opposition. The Air Force is aware of the desirability and complexity of balancing this tension (for example, "central guidance/local execution"). Designating a single point of

contact (POC) is helpful, but that POC must represent the multiple relevant perspectives on each major action or issue in order to achieve a constructive, dynamic balance.

- **Consider evolution of the problem over time.**

Large ICT projects evolve over time. For instance, Y2K evolved across Air Force organizational layers in two directions: initially, as locally identified problem-solving activities that evolved up into centrally managed initiatives, and later, as a centrally managed initiative that evolved down into locally driven problem-solving activities. The evolution of ICT projects in both directions generates tensions across organizational layers.

- **Clarify ownership and responsibility.**

Neither local nor central units alone can be fully responsible for a cross-organizational ICT issue. Generally, local units attempt to assert control over the systems they rely on, but during difficult times such as Y2K, central ownership of these shared systems was seen as desirable since it lessened local responsibility for assessing and addressing the problem. One of the important benefits of the Y2K experience was that it forced diverse owners of systems and overlapping system components to communicate with each other in an effort to coordinate responsibility and action.

- **Consider the impact of local diversity.**

Central owners and maintainers of ICT systems face the confusing task of understanding and managing a complex system of systems that spans significantly different functional and geographical environments. Those who acquire and develop systems may have difficulty anticipating how local conditions impact the fielding of those systems. The Y2K response had to address this diversity of local ICT environments, yielding insights into the ongoing challenge to achieve strategic alignment of ICT.

- **Consider the role of local autonomy.**

During Y2K, locally developed software was seen as more problematic than commercial off-the-shelf (COTS) software. Several features of Air Force management and funding practices foster local autonomy in ICT. For example, military credit cards for flexible purchases ("impact cards") allow local users to respond quickly to local demands but can present general system problems (for instance, security). On the other hand, systems and guidance were sometimes pushed from central to local units without dedicated funding in the hopes that the bases would "find a way" to support them. The Y2K response created an environment in which issues involving coordination among central and local units had to be addressed.

- **Build trust between local administrators and central managers.**

Another example of a local versus a central issue that arose for the Air Force during Y2K was the perception by local units that central guidance was not appropriate for their local situation, or that central units were using them as a "testing ground" rather than supporting their efforts. It is important that central guidance be delivered at an appropriate level and that mechanisms are maintained to foster stronger working relationships across horizontal organizational boundaries.

- **Strengthen cross-functional relationships across the organization.**

In addition to issues across the organizational hierarchy, Y2K also emphasized the need for clear mechanisms for coordination and communication across functional organizational boundaries. Specific efforts were employed to overcome the tendency of the organization to operate within functionally organized units.

- **Overcome funding disincentives to working across organizational boundaries.**

Using funding streams to identify project and system owners can help accounting practice but leads to a piecemeal view of systems, adding to the complexity of tackling a problem. Without specific funding, Y2K was not seen by some local users as their problem. Complications also arose because some parts of the organization work on a fee-for-service basis and others do not. Y2K created a precedent for cross-functional projects to receive significant resources and be managed in more creative ways.

- **Balance the perspectives of central administrators and operational managers.**

The Air Force Y2K response was characterized by an increased involvement of higher-level administrators in ICT decision making. This was both helpful and burdensome. Strategic ICT management cannot be achieved without the involvement of higher-level management, but the value-added of some new layers of decision making in operational issues is unclear. Y2K demonstrated the need to find an appropriate balance.

- **Address cross-boundary issues in the life-cycle management of systems.**

The end-to-end testing required for Y2K was complex to design, but the approach gained confidence over time, although it seemed that there was always more to do. Some Air Force ICT managers tried to build on this experience post-Y2K. Yet, maintaining the resource stream and management practices (for example, the use of block release dates) that proved effective during Y2K proved difficult as central management focus shifted to other issues. Y2K emphasized that life-cycle management of systems needs to be part of a strategic, cross-organizational effort.

- **Tackle the huge informational effort needed to support the management of integrated systems.**

The first impulse in responding to Y2K was to inventory those systems in place, identify the owners of the systems, and have the owners determine whether there was a problem. However, this is a huge, dynamic body of information that is often not available or not consistently maintained. It is impossible to manage what you don't even know you have, and maintaining up-to-date information on ICT resources is a huge task. Information of long-term value was created through Y2K, but little time or energy was available to leverage the response effort into an ongoing means of addressing informational needs.

- **Address issues of organizational culture.**

The Y2K response was often more impacted by informal patterns of communication than by formal directives and guidance distributed through regular channels. Who a communication came from could mean more than what the communication said. Subculture differences, such as those that exist between the acquisitions function and ICT management, also played an important role. This split was reflected even at the top, with the Air Force's CIO coming from the acquisition side and the deputy CIO the computing side. User cultures also displayed differences, especially CONUS versus OCONUS units. In addition, the Air Force's "culture of perfection" affected its Y2K response.

- **Empower permanent organizational entities focused on cross-boundary issues.**

No permanent unit within the Air Force had the scope and authority to manage a cross-organizational ICT project like Y2K. For this reason a temporary unit was created. The Air Force's Y2K response demonstrated the value of a permanent entity focused on integrating organizational and ICT strategies. The Y2K response enabled personnel to gain experience with crisis management and to build cross-functional teams. A more permanent entity or entities would serve as a focal point for ongoing efforts to manage ICT-related risks, as well as assure a corporate memory in the ongoing balancing act that is strategic management of ICT.

Lessons for Managing ICT Risk

The experience with the Y2K response, both in the Air Force and in the wider world, provides a number of lessons for how ICT risk management is understood and practiced. These lessons are instructive as organizations develop capabilities in the areas of information assurance and CIP. In general, these tasks have more to do with managing uncertain risks than with fixing things. In addition, it is important to bridge the conceptual gap between external risk from an outside threat and internal risk from system complexity.

- **Consider the role of perception of risk to appropriate response.**

The Y2K response was impacted by a changing perception of risk. As the visibility of the Y2K problem increased and senior managers became increasingly involved, the tolerance for risk was dramatically reduced. This occurred across the U.S. government. Local managers sought to prioritize, but central managers were far less willing to accept risk.

- **Understand the limitation of industry assurances.**

Naturally, ICT managers sought assurance from vendors regarding Y2K compliance. However, industry could not guarantee how products would behave when interacting with other components, so industry statements failed to reduce uncertainties.

- **Recognize the role of political, legal, and media factors.**

Attention from the political system (most notably Congress), legal factors, and media scrutiny all affected the Y2K response environment. The Year 2000 Information Disclosure Act specified that a "good faith" effort to discover and address potential Y2K problems would immunize organizations from liability. The Air Force adopted a higher, "due diligence" standard. This increased pressure to treat all problems equally. Political and media attention were beneficial in bringing a critical mass of resources to bear on the problem, but press writers did not fully understand the issues, and their coverage encouraged a broad, nonspecific zero-tolerance response.

- **Distinguish non-ICT infrastructure from information systems.**

The Y2K response was unnecessarily complicated by the inclusion of non-ICT infrastructure like automobiles and alarm systems. The small but legitimate risk from hardwired dates in embedded chips was difficult to locate and impossible to fix. The risk of cascading effects was especially low. Yet this became the public focus of Y2K. Combined with a zero risk tolerance, this issue produced a huge effort with minimal impact.

- **Explore existing risk management mechanisms.**

The Air Force had preexisting risk management mechanisms, such as continuity of operations plans (COOPs) and operational risk management (ORM), but these were generally not relevant to the Y2K response effort, in part because they did not address the challenges of managing cross-organizational ICT risk. These mechanisms could have been extended and employed more effectively.

- **Evaluate the effectiveness and appropriateness of response.**

Assessing the impact of risk management activities is difficult, but based on the outcome, the Air Force's Y2K response was found to be effective. Nevertheless, it is very difficult to evaluate the cost-effectiveness of the effort. To mention just one factor complicating such an evaluation, a non-trivial fraction of what was spent on Y2K would have been spent on new systems and upgrades anyway.

The Social and Organizational Context of Technology Risk

Since Y2K was not an external hostile threat, it did not fit easily into existing categories of information security. Y2K showed that threats can come not only from intentional actions of a conscious enemy but also from the unintentional consequences of our own actions, confounded by the complexities of the ICT system itself, the environments within which this system operates, and our inability to adequately manage these complex interactions.

Uncertainties stemming from systemic risk can be as great, or greater, than uncertainties from the risk of hostile enemy attack. Both kinds of risk need to be managed within a coherent strategy. Developing such a strategy involves a variety of trade-offs and expanded perspectives on the nature of technology risk.

This case study of the Air Force's response to Y2K raises several important questions about how our organizations and society can be most effective in a world where dependence on ICT, and the interdependency of ICT systems, is growing. It concludes by focusing on a single critical factor: that technology is socially embedded, existing in the context of people and organizations. Like other aspects of ICT, security, information assurance, and infrastructure protection must be managed from this perspective.

This lesson has been demonstrated in many incidents both before and after Y2K. In this sense the experience gained from the response to Y2K reinforces the lessons of the Three Mile Island and Chernobyl nuclear accidents, the *Challenger* and *Columbia* shuttle accidents, and the Bhopal disaster. The "decision" (however complex its evolution) to represent calendar years with two digits was human and organizational, not technical; just as the mismatch between metric and English measurement that destroyed the *Mars Climate Orbiter* in 1999 was a human and organizational error, not a technical or a mathematical one (or a terrorist attack).

This report rejects the idea that the Y2K problem was simply one of fixing the technology, recognizing that it was driven instead by a concatenation of institutional, leadership, economic, social, and political factors as well as technical ones. The Air Force's Y2K experience teaches us about software as a social system. It highlights the limitations and pathologies that typically grow out of social organization, training, and group complexity.

Y2K reminded organizations that the ultimate goal of IT is not the continued functioning of local clusters of technology but, rather, the effective use of information in support of strategic missions and goals. It forced organizations like the Air Force to take on the challenges of managing an enterprise-wide ICT project, teaching them that by becoming more process based and less technology based.

It is reasonable to believe that the lessons described in this report can be generalized, including the conditions that led to or exacerbated the problem, and what factors enabled or interfered with remediation. Systems of all kinds are becoming more interconnected and interdependent. If system architectures focus more on data and interaction and less on execution and specific procedures, if complex technology systems are also understood as components of social systems, then perhaps problems like Y2K can be left to the previous millennium. Eliminating all such risks is not possible, and would not be worth the massive amount of resources required even if it were. Understanding these risks makes risk management and planning for mitigation far more productive.

In the end, the Y2K experience helped introduce the Air Force and other technology-based organizations to a human, organizational and social perspective on technology risk. The degree to which these organizations understand this perspective and choose to act on that understanding is a key question for the future.

Chapter 1 Background

> Why do I think some of this happened?…I think there was a lack of context given to the Y2K problem. We did a great job of telling everybody that there was a Y2K problem, and we did a terrible job of putting it in context. (AMC/SCA)

The lessons from the Year 2000 (Y2K) are not obvious solutions to straightforward problems, nor are they based on clear choices among distinct options. These lessons generally involve subtle distinctions and the balancing of complex, rational, though often competing, needs and aims. This chapter provides the background and context to help you understand these difficult but critical lessons. It is presented in two parts: (1) a review of the complexities of information and communication technology (ICT) management, for the world in general and for the United States Air Force (hereafter simply USAF, or Air Force) in particular, and (2) a review of the complexities of the Y2K challenge, primarily as a problem to be addressed but also as a research opportunity from which to learn. These areas provide the context for the lessons presented in Chapters 2, 3, 4, and 5: "Managing ICT Complexity," "Aligning Organizational and ICT Strategies," "Managing ICT Risk," and "Technology Risk as a Socially Embedded Issue."

This chapter does not provide a detailed, chronological account of the diverse and dynamic response to Y2K, which lasted more than five years, either within the Air Force or around the world. Instead, we present numerous response details here and within the discussion of results and lessons learned in the following three chapters. Over the course of this report, you are given a clear picture of the Air Force's complex Y2K activities within the context of the events occurring around them. For a chronological, top-down description of the Air Force Y2K response, as well as details of the legislation, congressional funding, corporate approach, management structure, and preparation for Y2K, refer to the Air Force Year 2000 Office (AFY2KO) Final Report (USAF 2000). Much of the discussion in the following section (and the lessons learned) is relevant not only to the Air Force or the military but also to a wide range of private and public organizations. It covers general aspects of the ICT world and specific aspects of ICT in the Air Force. It also describes general aspects of the Y2K problem and basic trends in the response to this problem. These trends played out in the Air Force and in the world at large.

1.1 RESEARCH ON Y2K

This report is perhaps the most detailed publicly available case study of the Y2K response in a single organization and the lessons learned from that response. Although a great deal was written about Y2K before the event, surprisingly little analysis was conducted after January 1, 2000 (see Box 1-1). The fact that Y2K did not result in widespread catastrophic failures led many people, particularly those outside the ICT field, to label it a nonevent or a hoax—and doubtless prevented extensive analysis after the fact.

At the same time, the report should be read in the context of the broader field of information systems management, where many of the generic lessons arising from the Air Force experience of Y2K have already been documented in other settings. The

critical need to align organizational and ICT strategies has been a concern of the information systems community for decades.

Box 1-1. Overview of Research and Commentary on Y2K

Popular Literature and News Media

During the late 1990s, in the run up to the millennium rollover, a substantial popular and business literature on Y2K appeared. Although these sources provide context for the Air Force's effort to address the Y2K problem, most of this popular literature is not relevant to the issues discussed here. Reporting in the general news media on Y2K was also extensive in the run up to January 1, 2000, along with reporting in the immediate aftermath on the generally smooth transition and the relatively few problems that did occur. American RadioWorks produced a useful retrospective report on Y2K in 2004 (website address provided in the bibliography).

Government and Private Sector Reports

The efforts of governments, international bodies, multinational corporations, and other organizations such as professional societies were very important to the ultimate success of Y2K remediation and contingency planning. One prominent example is the President's Council on Year 2000 Conversion. The regular status reporting of federal efforts by the General Accounting Office is also a valuable resource (GAO 1997, 1998a, 1998b, 1998c, 1999). These reports provide information about the extensive efforts undertaken across the U.S. government to coordinate remediation efforts across agencies. The efforts of the Department of Defense and the military services, in particular, complemented efforts of the Air Force as described in this report. In 2000, GAO performed a top-down, retrospective evaluation of Y2K. One of GAO's main recommendations—that the capabilities created within and across organizations to deal with Y2K should be leveraged to address other ICT risks—is consistent with this report.

In a retrospective report for the Office of Science and Technology Policy, Mussington (2002) examines efforts to address Y2K and the implications for research and development in the area of critical infrastructure protection. Mussington's focus on the interactions between organizations and the broad ICT infrastructure complement this report's findings drawn from the examination of a single enterprise. Mussington also emphasizes the importance of decentralized information-sharing efforts that crossed organizational and national borders.

Academic Literature

The existence and functioning of ICT systems in their social and organizational contexts raise a number of research questions and issues that are interdisciplinary in nature and, taken together, might be termed "social informatics" (Kling 1999). This field has a long history (Kling and Scacchi 1982). The conclusions of this report are broadly consistent with this literature, work from which is selectively referenced.

Journal articles in management, information systems, and software engineering contributed perspectives to Y2K planning or drew lessons from the experience after the fact. The *Journal of Clinical Engineering*, for example, which deals with medical equipment engineering, devoted most of its July-August 1999 issue to Y2K preparation, including case studies of particular health care institutions (for example, Mercado 1999). *Information Systems Frontiers* devoted its August 1999 issue to exploring the ethical, legal, and risk management aspects of Y2K. Included in this issue is a very useful piece on how to leverage capability created to address Y2K in the service of ongoing ICT management tasks (Isaacs 1999). In the September-October 1998 issue of the *Journal of Software Maintenance: Research and Practice*, Marcoccia provides a case study of how one organization built infrastructure to effectively deal with Y2K.

In contrast to what appeared before the Y2K rollover, retrospective, objective analysis of organizational responses to Y2K has been more limited. One exception is an article in the September 2006 issue of *Management Science* that shows how companies that invested heavily in ICT in advance of Y2K were better positioned to take advantage of e-business opportunities following the rollover than were companies that invested less (Anderson et al., 2006).

1.2 ICT GENERAL BACKGROUND

In March 2000, after a day of Y2K interviews at Scott Air Force Base, the National Research Council (NRC) research team met with the commander of the 375th Air Wing for a briefing. As the team settled in, the colonel pointed across the street and described some problems he was having with a roof repair that had resulted from a construction project that did not meet code. He explained how the project funding complicated the situation: there were three or more groups involved, and it was not clear who was responsible for addressing the code problem.

As with the roof repair, funding issues had a significant impact on ICT systems on the colonel's base. However, the roof was a physical object whose use was visible and therefore obvious, and the components of the roof that did not meet specifications could be observed. Moreover, changes to the roof across the street would not affect all the other roofs on the base. With the ICT systems, it was far from obvious where a given system was located, where it began and ended, and even what it consisted of. In addition, it was far more difficult to identify the things that needed to be checked or repaired, or how those repairs would impact other ICT systems on the base. It was not even clear who was using an ICT system and what they were using it for.

Funding is only one of numerous complexities that greatly complicate management issues in the ICT world. Following is a discussion of some of the most important of these additional ICT complexities.

1.2.1 ICT Is Pervasive

> Another complicating factor…is the very pervasiveness of information technology. Practically everybody in the Air Force has a computer…that is connected to a network from which they access information from everywhere in the world, and most people tend to take a somewhat parochial view of it. …So determining who actually is responsible for taking care of the various pieces of information technology can be a difficult and sometimes challenging process. (AMC/HQ)

ICT is everywhere, yet it is nowhere in particular. Most people work with only a small piece of the overall system. Because the information they receive from this system is essential to their work, people usually seek to maintain some control over their piece. Yet when problems such as Y2K occur, pervasiveness can work in reverse. Rather than seeking to control their piece of the system, people view others as responsible for addressing an issue that exists only partially in the environment they control.

The pervasiveness of ICT can create confusion not only for system users but also for policy makers and managers. Who owns what, and how do one manager's actions affect another's? Who is responsible for the network? For firewalls? For operating

environments? For data? For information in electronic form? For work practices and measures of success? For ICT policy and long-term strategy? Uncertainty in these areas can lead to multiple lines of guidance and authority. "IT is too available and redundant. There are too many ways to be tasked. Too many parallel worlds" (374th AW/XP). The pervasiveness of ICT makes it more like an environment than a discrete machine.

1.2.2 ICT Is Multipurpose

ICT is both pervasive and multipurpose. Within an ICT system, it is not obvious who is using it or what they are using it for. This is true at many levels of the ICT system. At the content level, for example, designers of electronic information are keenly aware of the potential for multiple uses. "A wide variety of users can access a hypermedia with different purposes; thus, it is important to have different task models for different types of users" (Paterno and Mancini 1998). Since different people can use the same system for different purposes, even dedicated and intelligent people who share the same overall strategic objective can disagree on the basic priorities for design and use of an ICT system.

The honest differences that can exist over what constitutes the best ICT system extend beyond use and content design to management issues at many other levels of the system. At the operating environment level, for example, features that make ICT systems easier to field and maintain may at the same time make them more difficult to protect from outside threats. Compare the following statements:

> We need to do a lot of work on…common operating environments. Because we are finding out that servers have different disk drives on them, different versions of Oracle, different versions of the operating system. And as a result of that we can't distribute software in a rational manner. (SSG)

> From the information warfare perspective, diversity is not such a bad thing. If every piece of software is absolutely standardized, one hole gets you in everywhere. When an adversary has to figure out which executable is on which computer among 1,300 possible options, that makes his targeting problem hugely more difficult. (AF/XOIWD)

Just as end users have honest differences of perspective on the most desirable features of an ICT system, so do managers and ICT professionals.

1.2.3 ICT Elements Are Diverse and Often Dynamic

As the previous section mentioned, ICT infrastructure consists of a wide diversity of levels and elements, each with unique attributes and issues. Even a narrow view of these system elements includes such diverse elements as computer hardware, communication devices, operating systems, application software, and data and database management systems. A fuller view of the ICT infrastructure, however, includes even more diverse elements, such as ICT policies and best practices, relevant personnel and job categories, training and continuity plans, consequence management, security and information

assurance strategies, funding mechanisms, and the organization's culture of communication.

System elements differ in many ways. One significant difference is in their rate of change. Hardware and operating software change at a tremendous rate, driven by a dynamic information technology (IT) industry that lives off rapid innovation and accompanying sales. However, as the Y2K situation highlighted, data and databases change only with tremendous effort, if at all. Meanwhile, such complex interdisciplinary elements as ICT funding mechanisms and an organization's communication culture may extend beyond a given organization's control or have a life of their own. Thus, diversity and change are ongoing ICT issues.

> Each [personal computer] has its own distinct version [of the operating environment]. If you compare what you have versus someone else in the office, you'll find out they are different. …And in fact if you made them the same, your machines will not always work. Because if you buy your machines at different times—different times is just months apart—from the same vendor configured with the same basic software, they will have changed to a new version of the BIOS (Basic Integrated Operating System) and they will have incorporated whatever is the latest in terms of the dynamic libraries and so on. That's the industry and that's the realm we're in. (AMC/SCA)

While this statement is about one small element of the overall ICT infrastructure (personal computer [PC] platforms), it gives a good sense of the tremendous impact of diversity and change, particularly as driven by the IT industry.

ICT diversity and change issues involve organizational as well as system elements. Different units within an organization generally experience different rates and directions of change, often driven by differing functions and goals. For example, "AMC is usually much better organized about their information technology than ACC…because AMC is information or commission driven. AMC is constantly deployed…ACC is getting better" (AFCIC/SY).

Diversity and change issues at the system and organizational levels play important roles in the forthcoming discussion of lessons learned from the Y2K experience.

1.2.4 Traditional IT Is Less Reliable than Traditional Infrastructure

The Air Force is familiar with high-reliability software such as that used in avionics systems. However, this high reliability comes at a great cost that is not compatible with the economics and pace of the mass-market software industry. For a number of reasons, high-reliability software is the exception rather than the rule.

There is a much higher likelihood of error and downtime in the logistics software that tracks cargo than in the planes, trucks, runways, and roads that actually move it. A key reason for this is that software in general, and commercial off-the-shelf (COTS) software in particular, is not really engineered, at least not in the way that engineers design, build, and maintain traditional infrastructure. Software development tends to have more in common with art than with engineering. As a former Microsoft vice president said, "Programmers are like artists. …It's like a play—there's motion, things work, it's not static. You know where you're going. ...Things just flow" (Corcoran).

However, it would be unfair to simply blame programmers or profit-driven software companies for the reduced reliability of ICT systems. These systems are incredibly complex and, in some cases, perhaps the most complex entities ever created by human beings. They can develop a life of their own and evolve in ways that resemble the evolution of any complex organism. History books indicate that the infrastructure for the industrial revolution took 300–500 years to fully develop. We are about 50 years into the information age, so these systems are still not fully understood and developed.

Whatever the cause, the end result is that users must learn to adjust to a lower level of reliability from their ICT systems than from the power in their buildings and the sound in their telephones. Managers, too, need to distinguish between the reliability of their traditional infrastructure and that of the new information infrastructure. As an Air Force software manager put it, "We don't have any programs that don't have something wrong with them."

During Y2K the lower reliability of information infrastructure as compared to traditional infrastructure led some people to see a need for new and different organizational tactics for developing, operating, and maintaining ICT. "The same system is used for buying planes and tanks as is used for buying IT and software. But IT is more difficult to manage. The development, operation, and maintenance modes are more difficult to determine for IT and software" (AMC/SCA). Many of these management difficulties stem from interdependencies among elements of ICT.

1.2.5 ICT Elements Are Interdependent

The considerable complexity of ICT stems, in part, from its ubiquitous and multipurpose nature, the diverse perspectives of ICT users and professionals, the diverse elements that constitute ICT systems, and the ways in which those elements are developed and evolve. Yet, probably the most complex and confounding aspect of ICT is the extensive interdependency of the various system elements.

ICT interdependency issues are manifested at many levels, from the compatibility of hardware and software to the highest levels of intersystem interaction. This highest level of ICT interdependency is often called the "system-of-systems" perspective. From this perspective, any given system can be seen as being composed of other interdependent systems and being a part of still others.

Interdependency at the system-of-systems level often extends beyond any given organization (not just users or units). Therefore, this is an extremely difficult perspective for an individual or organization to maintain on a daily, operational basis. For instance:

> We treat our systems today…on a system-*by*-system basis and usually not on a system-*of*-systems or mission basis. And so there are disconnects, not necessarily within…any one system, but where it affects the system of systems. …We really don't understand the configuration of our system of systems. That problem is exacerbated by the way systems are viewed and, more importantly, by the way systems are funded. They're funded individually as a system and so there is no real impetus to look at it as a system of systems. (MSG)

As with the 375th Air Wing's roof repair, funding contributes to management difficulties, but with ICT the funding issue is interwoven with numerous other complexities, such as those presented here.

ICT management is a special challenge, and there is no magic formula for any given organization to meet this challenge. That is because in addition to general ICT complexities, each organization must consider unique issues that are intimately connected to its particular mission, strategic objectives, environment, and culture. For this reason, it is particularly helpful to continue the ICT background within the context of a specific organization.

As faced by the Air Force, the ICT management challenge is particularly illustrative and intriguing. The Air Force is a large, multifunctional organization that relies heavily on its new information infrastructure to accomplish a complex global mission. It has particularly high requirements for ICT flexibility, security, and information assurance. The following focus on the USAF is intended to make this discussion of particular use to that organization. However, the availability of the Air Force's experience with Y2K also increases the value of this work for anyone interested in strategic ICT management.

1.3 United States Air Force ICT

Like any modern organization, the Air Force must meet the general challenges of managing its ICT resources within the context of more specific challenges associated with its unique mission, strategies, and organizational environment. For the Air Force, these more specific ICT challenges stem largely from

- the nature of its mission and functional objectives
- heightened security and information assurance considerations
- particular organizational makeup, establishment of policy, and decision-making practices
- special personnel and training issues
- large size and geographical dispersion

1.3.1. Mission and Functional Objectives

The current Air Force vision for its national security mission is closely tied to successful management of its ICT assets. "Information superiority" is a central building block of this vision (USAF 2000b). Leadership recognizes that successfully managing ICT and related interdependent systems means establishing, maintaining, and evolving a general, flexible capability rather than achieving a specific objective.

> We have been thinking a lot about the future of the Air Force in the twenty-first century. The next two decades will present many unknowns. Our challenge will be to create a system of integrated aerospace systems that will be able to meet the full spectrum of future national security requirements—without being able to predict today precisely what those requirements will be. (Peters 2000)

To accomplish its mission of readiness in the face of uncertainty, the Air Force must maintain a multifunctional organization. ICT and the information it provides are critical to almost all of those functions. Perhaps most obvious is the actual combat activity. "With advanced integrated aerospace capabilities, networked into a system of systems, [the Air Force will] provide the ability to find, fix, assess, track, target and engage anything of military significance, anywhere. …Information superiority will be a vital enabler of that capability" (USAF 2000b).

Less visible but more complex to manage are the wide range of Air Force logistic and support activities. These have always been vital activities, but they are becoming even more critical and complicated with the Air Force restructuring around an expeditionary force concept. Aerospace Expeditionary Forces (AEFs) present numerous advantages for readiness and rapid deployment, but support capabilities are not organically assigned to these forces. In the logistics area, this means an even greater reliance on ICT systems for flexible, just-in-time support activities. "Effective, efficient logistics will be key to sustaining expeditionary forces. [The Air Force] will harness information technology, rapid transportation and the strengths of both the organic and industrial logistics base to ensure responsive, dependable, precise support" (USAF 2000b).

However, logistics systems (an increasing number of which are COTS) are not engineered to the level of reliability of avionics or special purpose weapons systems (see Section 1.1.4). This further complicates the challenges faced by the people and units who field, use, and maintain Air Force logistics and support systems.

AEFs may present special considerations that make Air Force logistics ICT particularly challenging, but the logistics challenge is shared by all the military branches (as well as any organization that incorporates just-in-time delivery into its operational and information strategy). For example, a recent Pentagon study of the Gulf War revealed the need for faster ways of deploying Army logistics and support units. Logistics was "hard-pressed to keep up with the rapid pace," and if victory had not been so swift, "maneuver forces would have outrun their fuel and other support" (Rosenberg 2001). ICT is the backbone of the effort to rapidly deploy logistics support.

Despite the many challenges associated with achieving and maintaining information systems that are reliable, timely, flexible, and secure, the national security mission of organizations like the Air Force leaves little margin for error.

> It's all about information. The need to provide war fighters the information they need—information they can trust—is a key component of the Expeditionary Aerospace Force concept. How effective we will be in the future is derived from our ability to rapidly collect, process, analyze, disseminate, retrieve and protect information while denying these capabilities to our adversaries. (Commander AFCIC, reported in USAF 2000c)

Therefore, the conduct of information warfare, both defensive and offensive, is a unique part of the Air Force ICT management challenge.

1.3.2 Security and Information Assurance

The critical value provided by Air Force ICT systems comes with an accompanying serious risk.

> Military operations today are heavily dependent on globally shared critical infrastructures. Technological advances have interconnected these infrastructures, better enabling mission accomplishment anywhere in the world. While this connectivity better enables mission accomplishment, it also increases our vulnerability to human error, natural disasters, and physical or cyber attack. (USAF 1999a)

While this statement focuses on the communications component, the recognition that increased complexity leads not only to increased mission capabilities but also to increased risk holds for all of ICT's many diverse elements. Incompatible data or ineffective practice can lead to mission failure as quickly as bad communications, as the lost *Mars Climate Orbiter* vividly demonstrated.

A wide range of issues is associated with ICT risk, including risk *to* systems from the outside and risk *from* internal system complexities. As a military organization, the Air Force must address intentional threats stemming from the deliberate acts of people intending to harm Air Force information capabilities. These threats may be physical (for instance, destroying communication lines) or may occur in cyberspace (for instance, denial-of-service attacks), and they may arise from the political motivations of an enemy state or simply the adolescent demonstrations of a hacker's ability. These security issues are generally covered under the term critical infrastructure protection, or CIP (EOP 1998a).

For the Air Force and other high security organizations, there is a special challenge to maintaining secure operations while simultaneously achieving the full capabilities of ICT systems. The functional strength of modern ICT systems often depends on an environment where information flows freely, fostering the innovative combination of data from disparate sources to create new information value. Security and CIP considerations generally run counter to this functional ideal: "The tension is between continuing IT management for usability and not giving your adversary the keys to your kingdom" (AF/XOIWD).

To take advantage of its ICT assets, the Air Force must link people, units, and their systems, both within and outside the service. These linkages introduce security concerns, but they also introduce another critical class of ICT risk. This second class of risk stems not from the intentional actions of an adversary but, rather, from the very system complexity and interdependency required to accomplish the mission. As stated earlier, most people see and touch only a small piece of the overall system. This means that as people and systems are increasingly linked, they can increasingly do things that, while sensible from their perspective, may have unintended impacts on others or the mission. These impacts may not be felt immediately, but they may play out over time and in concert with a sequence of other actions and modifications. Y2K is a member of this class of systemic problems (as was the loss of the Mars spacecraft mentioned earlier).

There are clear differences between security and systemic issues. While security focuses on outside threats to functionality, systemic risks are often an aspect or cost of that functionality. While security involves deterrence of an outside adversary, addressing

systemic risks involves effective management, communication, and coordination among those within the system. For this reason, some people see these two classes of ICT risk to be distinct, even competing, priorities.

Despite these differences, systemic and security risk share important commonalities. Specifically, systemic risk represents weak points in the system that can be exploited by those seeking to do harm. In addition, efforts to make ICT systems more robust through improved continuity and consequence management must consider both types of ICT risk. Perhaps most importantly, efforts to increase confidence in the output of ICT systems, often called "information assurance," must consider and even integrate both security and systemic risk since the causes of data and information corruption are both intentional and unintentional.

As discussed in Chapter 4, there are lessons from the Air Force Y2K experience not only for general information assurance efforts but also for addressing ICT security issues.

1.3.3 Organization, Policy, and Decision Making

Where are the organizational homes of Air Force ICT, and how do they contribute to policy and practice? Air Force leadership recognizes the importance of these and related issues that constitute part of the extended ICT infrastructure: "We will ensure [that] technological innovations continue to be accompanied by innovations in doctrine, organization, and training" (USAF 2000b). Achieving this vision, however, will not be easy. The complexities of Air Force organizational structure and of ICT can greatly complicate organizational and policy issues.

The Clinger-Cohen Act of 1996 called for each federal agency to designate a Chief Information Officer (CIO) with three general responsibilities:

> providing advice and other assistance to the head of the executive agency and other senior management personnel of the executive agency to ensure that information technology is acquired and information resources are managed [appropriately]
> developing, maintaining, and facilitating the implementation of a sound and integrated information technology architecture for the executive agency
> promoting the effective and efficient design and operation of all major information resources management processes for the executive agency, including improvements to work processes of the executive agency. (IMTRA 1996)

While, in one sense, final responsibility for ICT policy and practice lies with the CIO's office, the language of the act is focused on advising and improving the executive agency. In a large and diverse organization such as the Air Force, there is a wide gap between the executive agency and the distributed, frontline operational management and use of ICT. In addition, the act's language about technology acquisition and architecture may not be interpreted as including responsibility for more human issues such as best ICT practices and alignment between ICT management and organizational strategy.

During Y2K and as of the writing of this report, the Air Force CIO's office was divided among the Secretary of the Air Force and Department of the Air Force, the CIO in acquisitions (SAF/AQ), and the Deputy CIO in communications (HQ/SC). Units under acquisitions and communications, with a central focus on ICT, include: the Electronic Systems Center (ESC) and (under ESC) the Standard Systems Group (SSG) under AQ; the Air Force Communications Agency (AFCA) and the Air Force Communications and Information Center (AFCIC) under SC.

Additional background for non–Air Force readers will help them understand the lessons-learned sections. At the operational level, the Air Force is organized into nine major commands (MAJCOMs). Seven of these are functional (combat, space, mobility, materials, special operations, education and training, and reserves) and two are geographical (Europe and the Pacific). ESC and SSG are under the materials command (AFMC); AFCA and AFCIC are attached directly to HQ/SC. Another unit with particular focus on ICT is Information Warfare Defense (IWD), which is attached directly to operations in headquarters (HQ/XO).

Bases are attached to MAJCOMs and can house various tenants. For example, AFCA is a tenant at Scott Air Force Base (AFB), which is attached to the mobility command (AMC), while the 630th Air Mobility Squadron is an AMC tenant on Yokota Air Base in Japan, which is attached to the Pacific Command (PACAF). Base tenants may also be joint command units that serve the combined military services; for example, Scott AFB houses the U.S. Transportation Command (USTRANSCOM) and Yokota AFB houses the headquarters for joint services in Japan (USFJ). CINC refers to combined service units or operations under the Commander in Chief.

The overall Air Force management strategy can be summed up as centralized management with decentralized execution. In practice this means that central guidance from Air Force headquarters is interpreted by each MAJCOM for its particular functional situation. This continues down the line as bases receive guidance from their MAJCOM or a headquarters unit and interpret these orders for their local situation. The goal is a single point of contact (POC) for any given activity. But as this brief overview of relevant Air Force units implies, a single POC can be difficult to achieve for cross-functional activities such as ICT.

At times it is not easy, even for those directly responsible, to explain precisely where Air Force ICT policy resides within the organization and how it actually is managed. For instance, during the Air Force Y2K Lessons Learned Workshop, the facilitator asked, "Who sets IT policy, for example, the creation of a certificate to operate?" Because each participant's response was different, the conclusion was that "the answer is very complicated" (AFCA). Specifically, "where the policy starts and who owns it are two different things" (SSG), "especially when an organization always operates across boundaries" (AFCA). The cross-functional nature of ICT makes it particularly difficult to manage within an organization that is primarily organized along functional lines.

Funding is another complicating factor in Air Force ICT organization and policy management. The funding necessary to implement system modifications does not generally accompany the central guidance calling for those modifications. This issue is further complicated by the fact that changes to ICT systems do not occur in isolation. Rather, they require that an appropriate infrastructure be in place. This infrastructure

includes not only technical elements, such as an appropriate operating environment and sufficient bandwidth, but also human elements, such as appropriate personnel to field and maintain the change. Since all bases and units do not have the same level and type of ICT infrastructure, they will be in a better or worse position to make centrally specified changes. Where sufficient funding and support do not exist, bases can choose not to execute central ICT guidance.

There are many challenges to effective Air Force organization and management of its ICT assets. Some of the most difficult of these challenges involve striking an appropriate balance between the differing functions and perspectives of the various people and the units involved in ICT management and practice. Balances must be struck, among others, between:

- acquiring systems and linking networks
- functional and cross-functional needs
- central standardization and local flexibility
- managing more traditional aspects of the infrastructure and managing newer ICT components
- information sharing and information security

As discussed in the lessons-learned sections, the Y2K experience brought all these trade-offs to the forefront.

1.3.4 Personnel and Training

As Air Force leaders often emphasize, people are the most important element of USAF operations. This is true whether the technology they operate flies in the air or processes information on the ground. "The most important part of [the Air Force] vision is the people. We need to develop aerospace leaders who can take command of…information assets, which is going to be one of the most important things we do over the next two decades" (Peters 2000).

Air Force leaders also recognize that the tight market for ICT professionals represents a special personnel challenge, particularly with uncertain and uneven military demands. "We will size, shape, and operate the force to meet the needs of the nation. We must also manage the effects of tempo on our people. This is particularly important for those elements of the force currently in short supply, but in high demand" (USAF 2000b). There are many challenges to ensuring the consistent availability of experienced Air Force ICT personnel. These include appropriate job classifications and work conditions, effective training, improved retention, and adjusting these conditions to a rapidly changing environment.

Despite the complexities of their jobs and their critical importance to effective use and management of information and communication technology, frontline Air Force ICT personnel can often be undertrained and overworked. For example, personnel with previously unrelated job positions and training are retrained to IT (374th AW/LG). Others, such as wing system administrators, work extensive hours (for example, 5 a.m. to midnight) because of the complexity of their jobs (374th AW/XP).

Surprisingly, there is no formal Air Force job classification equivalent to system administrator (SA). This is particularly striking considering the critical role of an SA.

> [System administrators] perform activities which directly support the operations and integrity of computing systems and their use and which manage their intricacies. These activities minimally include system installation, configuration, integration, maintenance, performance management, data management, security management, failure analysis and recovery, and user support. In an internetworked computing environment, the computer network is often included as part of the complex computing system. (SAGE 2006)

In many cases, Air Force personnel with marginally related training receive short courses on specific aspects of their systems and then are expected to handle complex and varied SA tasks. These unofficial system administrators work long, intensive hours to maintain their systems, and many of those interviewed were tired and frustrated. They must cope on a daily basis with a growing number of system upgrades and security changes (AFCERTS) even as they work on ongoing major projects such as the Defense Messaging System (DMS). Yet they must often rely on on-the-job informal communications to acquire the necessary skills. This was particularly evident in the 374th AW/OG, where only one staff member had a background in medical network information, even though most of the staff worked on communications and system administration.

Whether formal or informal, the training Air Force ICT personnel receive is valuable. This contributes to another personnel issue—retention. Many Air Force ICT personnel look forward to retiring early to lucrative positions in the commercial sector once they gain sufficient experience. For example, SSG established permanent training centers at every installation and then lost trained personnel to such companies as Cisco Systems. Salary and competition from industry are key issues in attracting and retaining capable Air Force ICT professionals. In 1999, mean salary for U.S. system administrators was $64,271 and mean total cash was $70,565 (SAGE 2000). Whereas "…it was hard to keep staff in IT; a four-year senior airman made $18,000 a year" (374th AW/LG).

Turnover of ICT personnel comes not only from retirement but also from personnel cuts and the general practice of regularly shifting Air Force personnel to different bases (temporary duty, or TDY). Sometimes, personnel cuts stem from an assumed efficiency gain from the ICT itself: "We don't have the people that we had…There have been [numerous] aircraft maintenance cuts based on IMDS [a maintenance system]" (AFCIC/SY). Moreover, while there is obvious value to the wide experience and other benefits of regular TDY, the lack of consistent personnel can be particularly damaging to achieving good ICT practice and management. Given the dynamic and often idiosyncratic nature of most ICT systems, extensive and long-term practical experience with the various aspects of that system is a vital commodity. As discussed in the lessons-learned sections, the Y2K experience greatly impacted already stressed Air Force ICT personnel.

1.3.5 Geographic Dispersion

A final important set of Air Force ICT issues stem from the wide geographical dispersion of units and systems. These issues include important differences between the ICT situation at continental United States (CONUS) bases and at outside the continental United States (OCONUS) bases. Many differences between CONUS and OCONUS ICT are the result of general differences in non-ICT areas, such as organization, mission priorities, and dependency on local foreign infrastructure.

CONUS bases are attached to functional MAJCOMs, while OCONUS bases are attached to geographical MAJCOMs. This does not mean that the functional activities represented by the MAJCOMs do not occur on OCONUS bases. It does mean, however, that tenant functional units on OCONUS bases may be treated differently from their CONUS counterparts. There may be funding differences, or, as occurred during Y2K, functional MAJCOMs reaching out to their bases may reach only to the CONUS level.

In the ICT realm, these organizational differences can significantly impact the effect of central guidance, for example, efforts to establish common operating environments and to clear POCs and lines of authority. "The A[ir] F[orce] is moving towards having one IT [organizational structure]. The CONUS IT structure looks like the AF wants it. The OCONUS IT structure falls under the host unit" (AMC/SCP). In the ICT area, OCONUS units tend to have greater local autonomy than CONUS units, and this can lead to an even more idiosyncratic ICT infrastructure.

Because they are geographically and politically separated, OCONUS ICT personnel face additional challenges to fielding and maintaining state-of-the-art systems. There can be an almost rural aspect to OCONUS bases. Training is more costly and difficult to obtain, funding may be more difficult to obtain, and existing base infrastructure may be less up to date. "We're at the end of the…chain. Our computer systems are way behind those at stateside bases" (374th AW/CS).

Some of this difficulty is mission related. Being closer to the front lines, Air Force personnel at OCONUS bases see themselves as under greater operational urgency, with an accompanying reduction in time and attention for what can be perceived as secondary activities. "Operationally, a CONUS base is not that close to the enemy. The sense of urgency is greater at an OCONUS base because there is less time to do things, such as inventory" (374th AW/XP). In an OCONUS environment, ICT security issues are also complicated by geographical and political separation, which may mean less attention and fewer resources for other aspects of system maintenance and evolution.

Some OCONUS ICT challenges stem from base interdependencies with the local infrastructure of a foreign country. It is much easier to interact with the state government of Illinois, for instance, than with the government of Japan or Korea. Interdependencies with foreign systems most obviously involve power, transportation, and other traditional infrastructure elements, but technical elements of the ICT system itself can be affected as well. For example, in Japan, personnel cannot use the handheld scanners other bases use because they cannot get a frequency assigned (630th AMSS).

Some of the most difficult challenges for an OCONUS base involve cultural and political differences with the host country. These were especially visible during the Y2K experience and are discussed, along with other CONUS/OCONUS issues, in Chapter 3.

1.4 The Y2K Challenge

Just as ICT systems are complex, so was the challenge presented by Y2K. During Y2K there were a variety of perceptions as to what was occurring, and after Y2K the variety of perceptions persisted. To many people, Y2K was a pervasive threat to all ICT activities, with a firm deadline for averting that threat. "The difference between Y2K and normal day-to-day operations and software roles was that Y2K presented a problem that was going to affect everybody at the same time, whereas in the day-to-day world, random problems affect different people at different times" (MSG). To others, Y2K was more like a heightened state of the usual ICT activity. "These problems were not unique to Y2K. …They exist as part of the normal information technology day-to-day business. They just became more obvious under the intense spotlight that we saw with Y2K" (AMC/HQ).

Whatever the relationship between Y2K perceptions and realities, efforts to address Y2K challenged organizational ICT management in ways that it had never been challenged previously. For the Air Force, it was the equivalent of a test flight of their evolving prototype system for strategic and operational ICT management. To understand the lessons of this unique test, it is necessary to better understand the Y2K challenge itself.

1.4.1 The Y2K Problem

In Uruguay in the late 1960s, power engineers had trouble managing their power output, in part because of uncertainties in the water levels and flow of the river on which the power depended. They decided to write a software program to help predict river flow. In the Montevideo city records, the engineers discovered a wealth of historical data on river levels, weather conditions, and so forth, dating back to 1890. Unfortunately, their database used just two digits to represent the year. If they did not want to discard a decade of useful data, they needed a way of using two digits to distinguish between the years that began with an "18" and those that began with a "19." They did this using a coding scheme (for example, 01 = 1890) and created a useful predictive tool. Then they went about their business of power production and management.

The point is that in the late 1960s in Montevideo, Uruguay, a group of power engineers faced and addressed (for their situation) an instance of what, three decades later, came to be called the Y2K problem. In this case, it had nothing to do with the year 2000 or the closing seconds of a passing millennium. However, as with Y2K, it had everything to do with a range of dates that crossed a century barrier (in this case, the 19th) and a date representation scheme that used only two digits because it (incorrectly) assumed the two digits were preceded by 19.

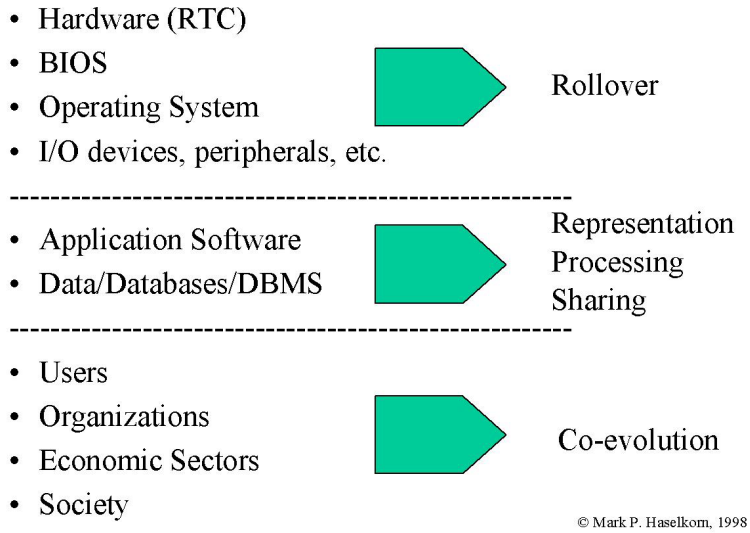
Despite the hundreds of billions of dollars spent on the problem and intensive media coverage of it, Y2K was a highly misunderstood event. Much of the misunderstanding stemmed from the popular linking of this event with the new

millennium. Such names as "The Millennium Bug" and "The Year 2000 Problem" were misleading, since they incorrectly implied a single, once-every-thousand-year event occurring at a specific point in time. People pictured a time bomb ticking away within computers and other date-dependent machines. Whatever the accuracy of these perceptions, they became an important aspect of the Y2K challenge.

The omission of the century digits in the representation of a year was neither unusual nor tied to technology. People always rely on assumed knowledge in the representation and interpretation of dates and time. For example, in the United States the date "10/02/00" is October 2, 2000; in other countries, it is February 10, 2000. To know what 10/02/00 represents, you need to know the country you are in and the schema that country uses to represent day, month, and year. To know what date is referred to in the phrase "The Spirit of '76," you need to know something about the American Revolution. Humans created computers, and humans working around the middle of a century did not see the need to keep repeating the obvious century digits.

As introduced in Section 1.1.3, an ICT system comprises a wide diversity of elements. Because dates can occur within any of these elements, Y2K was actually a set of different potential problems (see Figure 1-1). For example, such system elements as chips and operating systems are concerned with *system time* (that is, What time is it now?). These elements might experience a Y2K problem when "now" changed in such a way that the assumed 19 was no longer correct, that is, when 1999 rolled over to 2000 (namely, midnight December 31, 1999). However, system elements such as applications and databases are concerned with *functional time* (that is, What time range do I need to understand to conduct my business?). These elements might experience a Y2K problem whenever they needed to process a date that crossed the century barrier, whether that date was in the future—as with projected cargo scheduling—or in the past—as with the power engineers in Montevideo.

Figure 1-1. System Layers and Y2K Problems



The most difficult of the set of related potential problems that were called Y2K was concerned with sharing data among interdependent systems. This was especially true when those linked systems resided in different units, organizations, or even countries. In this case, the source of the date misinterpretation could reside not within any of the individual systems but *between* them. Since data shared between systems could include dates, what was correctly understood by one system might be misinterpreted when translated by another. Even more problematic, a change in date representation by the maintainers of one system, perhaps in response to a Y2K issue, could result in a problem within another system, even though there had been no previous problem with that system and nothing within that system had been changed. The only sure solution was careful understanding of and coordination across the system of systems. (The *Mars Climate Orbiter* failure, which resulted from the different interpretation of distance data across systems created by two different organizations, was similar to this type of Y2K problem.)

These and other complexities of the Y2K problem were not always understood. It was particularly difficult to craft a response that discriminated among the different types of Y2K problems, especially within the context of ICT management complexities and perceived insufficient time and resources. The following section provides a brief overview of various trends that played out over the course of the Y2K response period.

1.4.2 Y2K Response Trends

During the multiyear period during which organizations and governments were recognizing and responding to the Y2K challenge, the problem changed in several ways, in terms of both general perceptions and response strategies. Four significant trends could be seen in the world at large and in the Air Force in particular. There were shifts in focus from: (1) computers and ICT to chips and traditional infrastructure, (2) a technological to a mission perspective, (3) fixes to continuity planning, and (4) technology to political and legal issues.

1.4.2.1. From Computers and ICT to Chips and Traditional Infrastructure

For decades, selected computer professionals had recognized two-digit years as a potential problem. On January 27, 1988, the Federal Information Processing Standards (FIPS) Publication (PUB) 4-1 superseded the FIPS PUB 4, which had been established on November 1, 1968. The new FIPS PUB 4-1 stated that "for purposes of electronic data interchange in any recorded form among U.S. Government agencies, NIST [National Institute of Standards and Technology] highly recommends that four-digit year elements be used. The year should encompass a two-digit century that precedes, and is contiguous with, a two-digit year-of-century (for example, 1999, 2000, etc.)."

Why the previous FIPS PUB 4 had specified a two-digit year is part of another story. What is important here is that more than five years before most

organizations—including the Air Force—had a formal Y2K program, the issue had been clearly identified, at least as a need for a four-digit standard for date representation when sharing data. For most organizations, however, the cost of adjusting their data (and therefore the databases and processing software and the systems that shared the data) seemed to far exceed the threat.

Generally, computer professionals working on specific systems first brought to light the urgency of the two-digit date issue (at least in their immediate environments). In the Air Force, this happened in late 1993 at Cheyenne Mountain and again in early 1995 with the Airborne Warning and Control System (AWACS). As computer professionals recognized the complexity of changing what had been a widespread data standard, they were forced to seek additional resources from managers who neither understood the problem nor saw an immediate benefit to the bottom line or mission in addressing it.

> In 1995 at the Air Force level…there were three people working the issue…from the point of view of [researching] what industry was saying about it; not from what the Air Force mainly had to do. ... We felt [as if] we were vacuum cleaner salesmen. …[We would say to leadership] "We've got a problem here and this is what the problem is." And most of the leadership [viewed it as just] another program to throw on the burner. …It took quite a while, even within the SC community, to raise it to a level of the number one [issue]. … It was a very interesting mushrooming experience all along. (AFCA)

As awareness increased and the search for potential date-related problems gathered momentum, people realized that dates existed at many levels of the system, all the way down to hardwired dates on computer chips. The chips issue seemed particularly compelling: they could not be fixed, only replaced, and there were so many of them. The tiny time bomb, hidden in any machine with a date component, became the image of Y2K for many people.

In the first half of 1996, the Government Reform and Oversight Committee and the Science Committee began a joint review of the "Year 2000 Computer Problem," but by mid-1997 the focus was already shifting beyond the computer to a more traditional infrastructure. In her opening statement at a joint hearing on July 10, 1997, Chairwoman Constance Morella listed four specific concerns, the fourth being "that inadequate attention government-wide is being paid to other date-sensitive systems, such as the embedded computer chip problem." The media in particular was attracted to this issue, and soon these "other" systems became the major focus for many IT people, particularly those at the facilities level.

For ICT professionals this was a double-edged development. On the one hand, major attention was brought to the Y2K problem that might otherwise not have occurred. On the other hand, the focus on a more traditional infrastructure could be a major distraction from what they viewed as the central data issue.

> In August 1998 the first guidance was to look at computer-type equipment. …Three months later there was a shift from looking at interfaces to opening things up and looking for chips. …Not only did it increase workload but [also] it was another realm. (AMC/HQ)

> The chip was the focus. ...When we shifted away from the IT side…we put everything on the inventory that could possibly have a date problem with it. We had the traffic lights on

> it. We had railroad crossings outside the main gate. "Are the bars going to come down?" They had to test for that. (375th AW/Y2K)
>
> Generals had questions about embedded chips from what they had seen on *20/20*, *60-Minutes*. …That's what increased the workload—these kinds of external factors coming in. (AFCA)
>
> There needs to be a difference between IT and [traditional] infrastructure in the way they are handled. …There are 1,000 times more infrastructure items. AMC units were advised to let the bases worry about the infrastructure. (AMC/HQ)

The ICT-versus-chip issue is relevant to a number of the lessons learned presented in Section 2.5.

1.4.2.2. From a Technological to a Mission Perspective

Even as the increasing focus on chips took the Y2K response deeper inside the machines (though away from ICT), another trend was taking the Y2K response away from the technology itself and toward the organization and its mission. In part, this occurred because Y2K was getting too complicated for any one functional area, including the computing and communications people, to handle.

> We started out doing business as usual. "It's a COMS problem. Let the computer people deal with it." And as gradual knowledge came in of just how big this thing was turning out to be, we then started getting more people on-line and eventually we got operations to …look at it as an operational type of problem. (AMC/HQ)

Many computer professionals backed away from Y2K as their problem. They did not see it as being primarily about their systems (that is, computers and how they operated or were connected). Instead, many computer professionals saw Y2K as being about operational data and how it was stored and used or about chips in cars and alarm systems or about legal and political issues. To some people, this was an unexpected narrowing of the computer community's field of responsibility. For instance, "As we went through the Y2K process, I found that the original owners of equipment or policy or procedures or issues within the COM community were backing away from what I saw as their area of expertise. Once Y2K came into place, they stepped back from the area they were working on or their area of responsibility" (375th AW/CG).

Additional impetus for the shift from a technological to a mission perspective came from political and legal pressures (see Section 1.3.2.4.). "Prior to the Air Force Audit Agency coming through, it was a COMS squadron problem; after the AFAA came through, it was an operational problem because that's what the AFAA highlighted" (374th AW/CS).

Perhaps most importantly, the shift from a technological to an operational perspective occurred as part of a learning process. In response to the Y2K threat, more people than ever before were forced to face the complexities of ICT and the ways it is increasingly interwoven into the accomplishment of an organization's mission. Initially, most organizations attempted to address Y2K through a "technology first" approach. A

typical first step was to conduct an inventory of all information and communication technology with the goal of determining whether that technology was Y2K compliant or not. However, the limitations of this approach quickly became clear. For example, identifying all the ICT that was used in a large organization was no trivial matter, and even more difficult were complications of system complexity and ownership and responsibility for compliance.

> Who says whether it's compliant or not? If it wasn't owned by the Air Force, we called the vendor. …We have stacks upon stacks of compliance data from manufacturers. And they all say the same thing on the very bottom, "This is just what our compliance testing has proven. We in no way confirm that this product will continue as functional after the rollover." (375th AW/Y2K)

As the required testing phase approached, the impossibility of testing all systems for all possible glitches became increasingly clear, and operational test boundaries became necessary.

Given these issues, most organizations changed from a technical to an operational perspective over the course of their Y2K efforts. Instead of asking what technology they had and whether it was at risk, they asked what the critical activities of their organization were and what the role of information and communication technology was in those activities. Instead of placing a technical person in charge of Y2K, they placed an operating officer. By early 1999, as stated in the *Air Force Assessment Master Plan for Operations in the Year 2000*, "preparations for the year 2000 have now shifted to focusing on 'missions' rather than systems" (USAF 1999b).

We return to this trend in other lessons-learned sections, particularly in Chapter 2.

1.4.2.3. From Fixes to Continuity Planning

Related to the shift from technological to mission perspective was a shift of focus from fixing problems to preparing for continued function in the face of uncertain impact. For U.S. government organizations, this shift began in early to mid-1998 and gained momentum as both the complexities of the problem (particularly testing) and the demands of starting up contingency plans for ICT-dependent mission-critical activities became clear.

The evolving official government five-phase plan (Awareness, Assessment, Renovation, Validation, and Implementation) for managing a Y2K response program was initially developed in 1996; critical input came from Air Force planners at the ESC and the MITRE Corporation. The plan was disseminated in early 1997 by the Year 2000 Interagency Committee of the CIO Council (on an Air Force website) and by the General Accounting Office (GAO, now the Government Accountability Office) (OMB 1997 and GAO 1997). While contingency planning was mentioned, the plan initially focused heavily on the "massive undertaking" of finding, fixing (converting, replacing, or retiring), and testing all mission-critical systems, and perhaps even more. "Agencies must determine what systems are mission-critical and *must* be converted or replaced, what systems support important functions and *should* be converted or replaced, and what

systems support marginal functions, and *may* be converted or replaced later" (GAO 1997).

The early 1997 GAO assessment guide focused on project management and organized the five-phase plan into 52 key processes. Of those, only two (2.16, under Assessment, and 5.6, under Implementation) related to developing contingency plans. One year later, the situation was already viewed quite differently. GAO released a guide devoted entirely to business continuity and contingency planning that began, "Time is running out for solving the Year 2000 problem" (GAO 1998b).

As the Y2K response moved into its final year, complex efforts to complete and validate system renovations began to run up against equally complex efforts to develop and prepare viable contingency plans: "When we did the original studies in the spring of 1999, we realized the difficulty of fixing a serious, mission-critical problem within the time constraint for initiating the contingency plan" (Air Force Y2K Lessons Learned Workshop speaker). Many organizations shifted their primary focus from fixing and testing code to developing and monitoring contingency plans, or continuity of operations plans (COOPs) as they were called in the Air Force. (We return to the issue of COOPs in the lessons-learned sections, particularly in Chapter 4.)

1.4.2.4. From Technology to Political and Legal Issues

For ICT professionals, Y2K first came to light as a technology issue concerning date representation. For the many other people who were increasingly drawn into the Y2K process, however, the primary motivators were more likely to be legal and, especially for government agencies, political. This was particularly true for corporate executives, agency administrators, and their staffs. For the AFY2KO, the impetus was not from the scientific community. Instead, "it came from the political side. Senator Bennett and others had the foresight to make this thing the issue that it became" .

Given the huge potential for liability, early in the Y2K process corporations began sending queries about the readiness of their products through their legal rather than technical staff. By early 1998 this practice, in conjunction with the growing realization that Y2K preparation often called for high levels of coordination and cooperation across organizations, led to serious concerns that legal pressures would inhibit the flow of information vital to the success of these efforts. For example, the 375th AW/Y2K could not get any information from the vendors: "They just wouldn't say yes or no to the compliance status of anything because they didn't want to be held liable."

On July 30, 1998, at the request of the White House, Sen. Robert Bennett (R-Utah) introduced the Year 2000 Information Disclosure Act. This bill, passed early in October, provided liability protection from inaccurate statements made by organizations acting in good faith when sharing Y2K information.

While no additional federal Y2K legislation was passed, many organizations extended the focus on good faith beyond information disclosure to general Y2K response activities. The perception was that if good faith precautions were taken in addressing Y2K risks, legal protection would follow. There were calls for due diligence in

addressing Y2K, though the meaning of this term was not always clear. For example, it often was interpreted as "if you saw something you could do, you had better do it."

> The mandate came down under due diligence. … This was interpreted to mean that almost anything anybody could mention, you had to do that. … Because of the fear of being legally responsible… the only way you could not do something was if you could guarantee zero probability that there would be the possibility of an error. … Nobody could do that. (AMC/SCA)

In many cases, this trend led to the use of auditing agencies and other legally focused means of monitoring Y2K response efforts. "We did whatever we could but then we thought, what if they ask whether we have done enough? Well, we could call out the audit agency, which we did on three different occasions. … Then of course the DOD IG (Inspector General) [wanted] to get involved" (AFCA).

Government agencies were especially impacted by the increased political scrutiny of Y2K. In September 1997, Rep. Stephen Horn (R-Calif.) began issuing a congressional Y2K report card that produced such headlines as "Year 2000 Report Flunks 3 Agencies" and continued to get considerable attention throughout the Y2K effort, from the media and the agencies themselves (Barr 1997). The Department of Defense [DOD] received a C- on the first report. "Representative Horn probably did more to spur this whole process on than anybody" (AFCA).

GAO reports also had a major impact. While these reports often focused on technical aspects of the problem, they also emphasized the legal and legislative motivations. For example, "DOD's quarterly readiness reports do not fulfill the legislative reporting requirements under 10 U.S.C. 482 (the section of the U.S. Code that mandates such reporting) because they lack specific detail on deficiencies and remedial actions; as a result, these reports do not provide information needed for effective oversight of military readiness" (GAO 1998a).

As might be expected, there was a wide range of reactions to congressional involvement in the Y2K response effort including, among others, the following:

> A large part of what you are talking about…wasn't driven by any sort of need other than the political pressure. (AMC/SCA)

> External pressures caused us to have to report a lot of things we had never reported before. Some of which, now that we've come to grips with it, is not a bad thing. (AFCA)

> Is it rationally needed from a technical standpoint? No. But the measure of merit, in many cases, is you're doing things to satisfy the political institution and the political pressures. …Political pressure is why we spent our time looking at everything as opposed to looking at the really important things. (AMC/HQ)

> Politics is part of the environment. It's a reality of the environment that should not be put in pejorative terms. You know political leaders are not technologists; therefore, when these sorts of things happen, they naturally are not going to react with what is the engineering rational response. They are going to react with what is the politically rational response. It's just as rational in their decision-making frameworks. (AFXO/IWD)

We return to political and legal issues in other lessons-learned sections, particularly under the discussion of risk and response in Chapter 4.

1.4.3. How the Research Opportunity Changed

Just as perceptions of and responses to Y2K changed over time, so did Y2K as a phenomenon to be studied and an opportunity through which to learn important lessons. The NRC, working with the Air Force and with the support of the IEEE, began early in 1998 to position itself for a before-and-after study of lessons to be learned from the Y2K experience. Many of the early study aims were based on the assumption that there would be a number of critical, highly visible Y2K infrastructure failures. For example, one Air Force study aim was to use Y2K disruption as a surrogate for information warfare attacks. The hope was to develop a better understanding of how interdependent systems fail and then use that understanding to help make those systems more resistant to outside attack. The level of disruption assumed for this study goal did not occur. (Why it did not occur is addressed in Chapter 4 under lessons related to minimizing risk.)

Interestingly, that Y2K did not produce major sustained disruption to critical infrastructure actually makes it a more valuable source of long-term lessons for the operational and strategic management of complex ICT systems. Y2K studies evolved from a focus on fundamental flaws and cascading effects into an analysis of impact on overall strategic management of information and communication technology. This analysis included issues such as maintenance and modernization, life-cycle management of systems and software, functional interdependency and continuity, guidance policies and certification, system ownership and responsibility, training and organizational roles, and security and information assurance.

The worldwide Y2K response effort was of incredible magnitude and evolved over many years. It confronted organizational systems for managing ICT with situations they had never faced. People who played significant roles in this Y2K effort were changed in significant ways. Yet because little happened, the tendencies to return to business as usual were strong.

We hope that people and organizations do not ignore the valuable, if difficult, lessons gained from the expenditure of hundreds of billions of dollars and countless hours of human effort. We also hope the following sections of this report contribute significantly to the useful dissemination and application of these lessons.

Chapter 2 Managing ICT Complexity

> Modern technology and society have become so complex that traditional ways and means are not sufficient any more but approaches of a holistic and generalist or inter-disciplinary nature become necessary. (Bertalanffy 1976)

> Y2K is not about hardware, firmware, and operating software (platforms). It is not about application software and…data. It is not even about users, organizations, economies and nations—it's about all of them together. (IEEE 1999)

The previous chapter presented complexities associated with information and communication technology (ICT) systems in general, and within the United States Air Force (hereafter simply USAF, or Air Force) in particular. It also presented an overview of the Year 2000 (Y2K) problem and response efforts. This chapter and the two that follow bring these areas together by looking at the Air Force Y2K experience as a source of information for improving the operational and strategic management of complex and critical ICT systems. This chapter focuses on ICT management challenges stemming from system complexities. Chapter 3 focuses on organizational issues, particularly the role of organizational entities in the establishment and execution of ICT management strategies. Chapter 4 focuses on risk, response, and security issues. As will be seen, there is critical linkage across these three areas of "lessons learned."

On the surface, the whole Y2K story seems incredible: Between 1995 and 2000, a problem about assumed century digits in date representation came to be seen as the most significant challenge facing many, if not most, organizations in the world. For many people in the Air Force, it became "the #1 thing we've got going" (AFCA). Even more surprisingly (and far less well known) was that the problem with century digits ultimately taught those who worked on it more about their overall organizational operation than about their technology.

What follows is a discussion of the lessons learned by people and organizations as they attempted to address Y2K within the context of general ICT system complexities. These lessons are relevant to the ongoing management of other current and future ICT problems and opportunities.

2.1 The Need for New, Less Localized ICT Management Strategies

The magnitude of the Y2K response was greatly increased by less than optimal efforts to manage the situation. Y2K represented a class of ICT issues that go beyond the functional management of individual systems or localized clusters of technology. Thus, traditional localized management strategies were often defeated not only by the particular pressures of the problem at hand but also by the intermingling of that problem with other ongoing pressures stemming from the increasing complexity of and reliance on ICT systems.

It was difficult to break down Y2K activities into clearly bounded efforts under local control. The interdependency of ICT elements and the varying roles of ICT in achieving organizational missions meant that no single group could fully control the

issues. Enterprise-wide perspectives and nontechnical environmental impacts had to be considered. ICT managers recognized that these challenges were not unique and that the difficulties of Y2K management were symptoms of difficulties with the ongoing management of ICT: "These problems were not unique to Y2K. …They exist as part of the normal information technology day-to-day business. …We were doing business as usual, but we need to come up with a better business as usual" (AMC/HQ).

The ICT infrastructure of a large modern organization is extremely complex. The more an organization relies on information within that infrastructure to achieve its mission, the more complex its management task. In simple terms, a complex system is one in which the whole is greater than the sum of its parts. Traditional management strategies assume that the systems being managed can be broken down into discrete component parts and clear, causal relationships among those parts. However, this assumption is no longer valid for systems that have reached a sufficient complexity. "Compared to the analytical procedure of classical science with resolution into component elements and one-way or linear causality as basic category, the investigation of organized wholes of many variables requires new categories of interaction, transaction, organization, teleology, etc., …" (IEEE 1999).

Neither ICT systems nor the organizations within which they reside are closed systems; in other words, they cannot be understood and managed independent of their interactions with other systems and, particularly, with their environment. "To conceptualize an organization as an open system is to emphasize the importance of its environment, upon which the maintenance, survival, and growth of an open system depend" (Malhotra 1999).

Under the pressures of Y2K, the need to manage ICT systems as organized wholes was even stronger than during periods of business as usual. In addition to the general complexity of ICT systems, Y2K brought into play two additional major complicating factors. First was the perception that everyone would be impacted in the same way and at the same time. "During Y2K we were doing so much sharing because we had a common enemy and a common deadline" (MITRE). Second was the perception of a specific, fixed deadline for the effort. "Y2K was different. …We had a compressed time; we had some milestones that weren't going to change or move and [they were] related to coding and dates and what the impact would be if we didn't fix those problems embedded within the code. Out of that we've learned so much more about the way we really do business and rely on one another" (AFY2KO).

The perceived combination of a common enemy and a common deadline contributed to an increased awareness of the interdependencies and shared responsibilities of the various ICT efforts across an organization. (Additional elements of the Y2K experience that contributed to this awareness are discussed below.) This in turn helped foster the idea that these functional elements of the Y2K effort needed to be brought together under a single, more encompassing management perspective, at least for the duration of the effort.

Y2K helped teach organizations that ICT management was not a piecemeal effort. Under the added stresses of the Y2K situation, the limitations of focusing on localized clusters of technology became more evident. As efforts to respond to Y2K within business-as-usual management practices were found to be insufficient or impractical, new

strategies and tactics arose that were more representative of the complex, interdependent aspects of ICT systems.

The following lessons discuss many of the shifts away from traditional information technology (IT) management that were instigated or emphasized by the Y2K experience. Chapter 3 explores these shifts further in terms of specific organizational entities and roles.

2.2 The Need for Wider, More Integrated Efforts to Define and Stratify ICT Problems

During Y2K, breakdowns in traditional management of the situation began at the most basic, definitional levels. Efforts to decompose the Y2K problem and organizational responses into discrete components were largely unsuccessful. As a result, attempts to carry out a Y2K response strategy based on classification and stratification of ICT systems and problems, though not without some benefit, generally had minimal impact on frontline response activities. Difficulties in breaking down the problem stemmed not only from technical complexities but also from conflicting multiple perspectives and the impacts of nontechnical environments.

At different times during the Y2K response process, most organizations made efforts to stratify the various potential problems according to such identified criteria as criticality to mission, likelihood of occurrence (see the discussion of risk in Chapter 4), local conditions, and optimal response strategies. For example, a common component of strategies for dealing with Y2K (or any widespread threat that taxes available resources) was an attempt to classify systems by their criticality to the organizational mission and then focus efforts on those systems deemed most critical. In the Air Force, this "triage" strategy led to central guidance asking units to classify systems into categories C1, for most critical, through C4, for least critical. "Air Force Core Capabilities form[ed] the basis for determining critical missions and functions" (USAF 1999b), but complexities like those discussed in Section 1.1 meant that the translation from critical missions and functions to critical systems was not straightforward. As a result, Air Force Y2K activities found it difficult to tailor their response tactics to individual classes of Y2K problems or to local environments. Instead, Y2K was treated as a generic threat rather than what it was—a set of specific interdependent threats, each with varying factors of risk and impact and each best addressed using varying response tactics. "I've been doing this job for two and a half years. The Y2K orders have been…consistently 'check everything' with no real shift" (374th OG).

There were benefits from efforts to classify systems and problems, particularly at the most critical, "thin line"[1] level, as well as in focusing people's attention on organizational aspects of the Y2K situation. However, as a guide for the overall Y2K response activities, these classification efforts generally proved ineffective.

[1] "Thin line" refers to a cross-service operational thread at the Commander in Chief (CINC) level.

> Our only stratification really came along the line of thin line systems. But once you got past "is it a thin line system," for all practical purposes every system went through the same level of scrutiny. …You could look at the specific date-related type of errors that could occur and see that the impact would be negligible.… [It] didn't matter. (AMC/SCA)

The lack of problem stratification was particularly felt in the complex logistics area.

> We applied Y2K fixes evenly, although the problem actually is manifested asymmetrically. …If I print out on an in-transit visibility that I moved cargo by a C5 in 1949, that's not a big problem—it's…obvious and there certainly is a way to handle immediate mission impact. We shouldn't hold it at the same level of urgency as other programs, where miscalculation across a date, maybe miscalculation of fuel flow, would cause some severe problems. And for those we would need to give greater scrutiny. The point is that all scrutiny was equal, because you had to address Y2K first. (AMC/SCA)

At times, this lack of problem stratification could be extremely frustrating, especially given the effort put into classification.

> We spent all this time and effort categorizing stuff, then we promptly paid absolutely no attention to categorization and painted everything with the same paintbrush. … We did the exact same process for everything, from the most critical C^2 system that we have in the command to a system that is nothing more than a CD produced by a promotion company made to train people on how to run aerial cargo ports. We treated those two things the same way when it was quite apparent that they shouldn't have been. (AMC/HQ)

Why did efforts to stratify Y2K systems and problems have limited impact? Air Force efforts to categorize systems by their mission criticality were hampered by both technical and nontechnical factors. On the technical side, system complexities made it difficult to isolate ownership and roles of specific system features and elements. This complicated the task of determining both responsibility for and criticality of systems. Many were concerned about fragmentation of management responsibility. "What if we had had a bunch of Y2K failures? What kind of finger-pointing would have gone on initially between saying 'Oh, that was an application problem. No, that was an operating system problem. No, that was a hardware problem'" (MSG).

Even more significant, however, were the nontechnical factors. With the lack of clear technical criteria, political, financial, and other systems that composed the ICT environment became central to the definition of mission critical.

> What is mission criticality? A lot of our Y2K reporting got skewed or clouded by the fact that at first everybody was mission critical. But then the OSD (Office of the Secretary of Defense) requirements came down and said if you are mission critical you've got to do all the following by a certain date. Suddenly a lot of things were no longer mission critical. Then later on it came out that if you were mission critical we're going to prioritize how this money is used as it comes out from Congress. Whoa, then everybody's mission critical again. And then it came out that you weren't going to get money for certain things, and definitions changed again. So really it was a lot of oversight and funding that drove the mission criticality demands. (AFCA)

System criticality could not be assessed using purely technical or mechanistic means. Even as ICT complexity made it difficult to identify the boundaries and roles of any given system, the interplay between technical systems and their nontechnical environments dynamically affected basic definitions, such as the notion of what constituted a mission-critical system.

Similar to the difficulties in clarifying the definition of mission-critical systems were key definitional uncertainties surrounding the concept of "Y2K compliant." In other words, how was anyone to know when a system was okay or had been fixed? The certification of a system as Y2K compliant was seen as an essential step in the overall Y2K remediation effort, and the media used this phrase incessantly. Yet, despite its perceived importance and wide use, the interplay of multiple systems and perspectives made it extremely difficult to define and apply this critical concept.

Why was it so difficult to recognize the behavior of a system that was free of Y2K problems? Remember, compliance is not an abstract idea but, rather, is about complying *with* something (that is, a guideline or standard). Yet most people, particularly the media, used the phrase "Y2K compliant" simply to mean "fixed," without any notion of the guideline being met. The people responsible for certifying systems, however, required more precise definitions and test procedures for determining Y2K compliance. Specifically, they needed a clearly specified, testable definition of the desired behavior; a specified period of time (that is, range of dates) over which this behavior needed to occur; and specified conditions under which this behavior could be expected.

In the United States the most common definitions of Y2K compliance were adopted from language in the Federal Acquisition Requirements (FAR). Under FAR compliance, the desired behavior was "able to accurately process date/time data"; the period of time was "from, into, and between the twentieth and twenty-first centuries, and the years 1999 and 2000 and leap year calculations"; and the conditions were "to the extent that other information technology, used in combination with the information technology being acquired, properly exchanges date/time data with it" (FAC 1997). While this language was useful from an acquisitions perspective, definitions of Y2K compliance adopted from the FAR were not very useful for the testing and certification of systems. Acquisition is a critical ICT activity and organizational component, but it is only one of many perspectives that must be balanced in the management of ICT.

First, the FAR definition of desired behavior relied on such words as "accurately" and "properly," which were not sufficiently defined for use in testing and certification. Did "accurately process" mean "give correct answers" or "not break down"? ICT systems often give incorrect answers and often break down, independent of any Y2K issues. These vague words may have been useful in government contractual agreements, perhaps allowing for broad interpretation between parties, but they were not useful to ICT professionals seeking to test system behavior.

Second, the FAR language on the time period, while vague, could be interpreted as requiring systems to accurately process for two centuries (1901–2100). Again, this broad coverage may have made sense from an acquisitions perspective, but it made little sense from a technical one. The most common operating systems of that time could not meet this requirement, with the operating range of Windows beginning on January 1, 1980, and the operating range of UNIX ending January 19, 2038.

Third, the conditions under which accurate processing was expected to occur included "proper" date exchange with "the information technology being acquired." Again, the language was too broad to support specific testing. Even more important was the assumption that the technology under consideration was being acquired. This certainly made sense within the context of the FAR, but when this language was adopted in general definitions of Y2K compliance, it contributed to misunderstandings. Y2K was often seen to be primarily about modernization (that is, acquisition), when in most cases it was about maintenance (that is, keeping existing ICT functioning in a predictable manner). This is another example of how the multiple perspectives of people involved with ICT complicated not only the resolution of Y2K problems but also the understanding of the problems to be addressed.

Particularly during its early stages, Y2K was more about understanding the problem than addressing it. And throughout the dynamic Y2K experience, definitional complexities stemming from localized, loosely coordinated management strategies continued to make it very difficult for organizations to establish and apply precise problem definition and stratification. For these and other related reasons, there tended to be a generic, relatively uniform response to anything labeled as Y2K, even though Y2K consisted of a set of nonuniform problems occurring within nonuniform environments. Hence, Y2K helped teach organizations that even at the definitional level, ICT management can be more about balancing multiple perspectives and environmental impacts than it is about precise technical specifications.

2.3 The Need to Shift ICT Management Focus from Hardware and Software to Data, Knowledge, and Organizational Goals

In addition to definitional issues, Y2K highlighted other ICT complexities that challenged existing management practices. Many of these called for a shift in ICT management focus from hardware and software to data, knowledge, and organizational goals.
It is not surprising that traditional IT professionals and the organizations they work for see hardware and software as the central elements of their systems. These IT professionals come from an educational and training background where the difficult subject of computing (namely, hardware and software) has been their primary element of concern. This knowledge is critical, but people involved in Y2K remediation efforts found they could not limit their activities to issues involving computers, communication devices, operating environments, and application software (see Section 2.3.2.2.). Increasingly over the course of their Y2K experience, these people were called on to address issues involving the generation, capture, manipulation, sharing, and use of data and knowledge in the pursuit of organizational missions.

From the computer-centric perspective of traditional IT professionals, the operational use of data is separate from the system that is their primary concern: "Within AMC [mobility command] the SC [communications] organization actually does the command and control systems. We develop them; we operate them; we maintain them. We're not the ones who put the data in…we have an operational organization" (AMC/SCA). From this perspective, data simply "feed" the system. But Y2K reminded

us that data are more than numbers being eaten, crunched, and spit out by hardware and software.

Many complications in the Y2K remediation effort stemmed from the fact that data exist within a database and that databases do many things. Of course, databases specify data formats, which was a central aspect of the Y2K problem.[2] However, databases are also a compilation of the data types an organization considers worth capturing and specifying. In other words, databases represent the entities of interest to the organizations that use them. Databases also represent the relationships among those entities. They represent the questions that an organization wants to be able to answer and how they go about answering them. In the largest sense, a well-constructed database represents how an organization views the world and how it conducts its business.[3]

Over the course of Y2K, it became clear that changes made to hardware and software generally did not address the central Y2K data and database issues. Early on, Y2K was often viewed as a technology modernization issue involving older mainframes and legacy software created decades earlier. The problem was "a vestige from the bygone times of computer technology, when memory was expensive" (USA Today 1997). But organizations that took on Y2K within the context of general efforts to modernize technology found themselves facing two highly intractable and only loosely related problems. Arthur Gross, then Chief Information Officer (CIO) of the Internal Revenue Service, said that combining Y2K and modernization efforts reminded him of the scene in the movie *Butch Cassidy and the Sundance Kid* when Butch and Sundance find themselves trapped by Mexican soldiers on a high cliff overlooking a river. "I just remembered I can't swim," says Sundance. "It doesn't matter. The fall will kill you," replies Butch. While both efforts were critical, they were distinct and often incompatible. Y2K was about maintaining a consistent, predictable existing function, while modernization was about replacing old equipment or adding new technology and function.

While changes to hardware and software did not generally address fundamental Y2K issues, changes to data formats in databases required associated changes in any module that read, processed, or transferred the newly formatted data. For this important class of problems, the flow of data was the driver, not hardware, operating systems, or software. Thus, Y2K fostered a perspective in which data held the central position, with hardware and software needing to be adjusted to continue serving that data. (This perspective is consistent with the fact that hardware and software change rapidly, while data and databases change rarely and only at great cost.)

Furthermore, Y2K reminded us that problems with data can have disastrous implications independent of whether the hardware and software are performing as intended or not. Data corruption could be a greater concern than system failure. "JACAL is a warning system, and if data [are] intentionally corrupted…and then sent to an installation—that's what we do our maintenance on. If it's the wrong information—a

---

[2] It had become common practice in databases to specify the calendar year as consisting of two characters defined as the last two digits of a year in the twentieth century. Such a specification needed modification (directly or indirectly) in order to handle years outside the twentieth century.

[3] It was largely on this basis that many consulting companies (for example, SAP) saw Y2K not as an opportunity to modify existing code and to plug in new machines but, rather, as an opportunity to convince clients to adopt an entirely new system for handling their data and information processing.

slight miss torque on an egress line on an A-16, that could kill a pilot. …I'm concerned about somebody getting bad information into a system that we rely on for operations" (AFCIC/SY). Here, the central driver goes beyond the data to see how people use data to generate information that is essential to accomplishing an organizational mission. Over the course of the Y2K effort, the central focus shifted from hardware and software to data and information and, ultimately, to how people use information to achieve organizational goals.

Y2K encouraged organizations to reverse the commonly held perspective of computer-centric IT management by emphasizing the central nature of data as they are used in the accomplishment of organizational missions. Data and the databases within which they reside represent the core knowledge of an organization, and an organization faced with saving either their processing systems or their data will choose the data. For many IT professionals this represented a new perspective on their systems. Data, databases, and the knowledge they represent were increasingly seen as holding a stable central position, with computers and software constantly evolving to assure that people could use the data and knowledge to achieve organizational goals.

2.4 The Need to Align ICT Management with Operational and Strategic Goals

The increasingly information-centric perspective of ICT fostered in part by Y2K did not just mean that traditional IT professionals began to view data, information, and knowledge as holding a more central position in their world. It also meant that many operational and strategic managers who had previously seen themselves to be on the periphery of the ICT world (if not completely outside it) suddenly found themselves thrust into its center. This coming together of operational and ICT managers was one of the most significant outcomes of Y2K. For many organizations (including the Air Force), Y2K instigated the first large-scale, formal effort to align ICT management with operational and strategic management.

Generally, IT management and the strategic management of an organization have differed significantly. IT management has focused on acquisition and keeping technology working within an imperfect world where failures and fixes are a common occurrence. In this world, correct decisions about hardware and software, based primarily on technical knowledge, result in relatively short-term system improvements, such as restored or improved functionality, increased compatibility, and easier maintenance.

On the other hand, strategic organizational and business decisions are seen as being more pervasive, with longer-term impact on a wider range of the enterprise. Strategic decisions are generally the result of a negotiated consensus process within a dynamic context of shifting economic, legal, and political forces. The goal is to achieve an accepted best direction based on appropriate trade-offs and compromises. While the nature of this decision is complex, once it is made there is little tolerance for error and miscalculation. To a strategic planner, failure is a career-threatening event; to an IT manager, failure is part of the job. This is one example of the differences in perspective, focus, and knowledge that can result in a gap between ICT and strategic management, and both sides can help create this gap. "Managers have often delegated or abdicated

decisions to information technology professionals… [while] poor specification of strategic objectives often leads to the information technology group setting an information technology strategy in isolation from the business" (Weill and Broadbent 1998). Where gaps between ICT and strategic management existed, Y2K highlighted both the difficulty of bridging them and the critical importance of doing so.

As Y2K evolved from a primarily technological to a primarily mission-oriented issue, IT and operational personnel were drawn together in new ways. These two groups, generally with differing backgrounds, perspectives, and corporate cultures, found themselves sharing responsibility for what had become a complex, dynamic, high-priority, organization-wide project. Not surprisingly, this coming together of IT and operational managers under difficult and stressful conditions was not without its problems. "Y2K was not just a common computer problem but also a mission problem. …When we got all the different functionaries involved in it, that tended to complicate things. There were times when coordination between the different functionaries was difficult, at best, or lacking, at worst" (AMC HQ).

Coordination issues were complicated by the fact that IT professionals and operational managers had differing perceptions of the Y2K situation and response effort. Of particular relevance was the considerable difference in their understanding and acceptability of risk and error. As mentioned earlier, IT professionals were in an environment where risk, and even breakdown, was far more prevalent and acceptable. For these professionals, any change raised the possibility that, even with testing, catastrophic problems could follow. "Everyone who's dealt with software knows that [but] senior leadership…has an absolute unawareness that this is the reality…we live in every day" (AMC/SCA).

Over the course of Y2K, the wide range of perspectives on ICT caused different people to have very different responses to the same situation. For example, when Y2K was still seen primarily as a technical problem, frontline Y2K workers found it extremely difficult to obtain resources from higher-level IT managers who were used to dealing with potential failure and whose primary focus was on keeping their technology functional.

> Why would or should a CIO or MIS (Management Information Systems) director with a two-to-four-year life expectancy at any one organization…say, "Give me $40 million and I'll disrupt our whole information infrastructure, put all of our current operations at risk and, if I'm lucky, do something no one else has ever done and prevent a problem many people think is not real and will not in any case happen for years, and otherwise contribute nothing to our bottom line?" (IEEE 1998)

Later, as Y2K evolved into an operational issue, another set of differences developed—this time between these same IT managers and the more mission-focused operational managers who gradually took over leadership of the Y2K process. The far lower tolerance for uncertainty of operational managers contributed to a far greater availability of resources devoted to Y2K. But this reduced tolerance for risk could be extremely irksome to IT managers, who lived on a day-to-day basis with the development, operation, and maintenance of highly sensitive and often unreliable ICT systems (see Section 1.1.4). "During Y2K there was zero tolerance of risk because of ignorance on the part of people looking for certainty. An engineer knows that there is

always a probability that things might not work" (AMC/SCA). (Risk and response are discussed in more detail in Chapter 4.)

While the differences between traditional IT managers and operational managers could be significant, something even more significant was strongly emphasized by the Y2K experience: the absolute necessity of bringing together these two groups under a single strategic umbrella. This recognition became clear even to those who most experienced the difficulties of trying to make it happen. As sAMC/HQ stated: "We need to take the information sharing we had—take the things that we learned from getting the operational people involved in it and looking at it not just as an IT problem but, everybody uses it, it's a problem throughout the business that we do—and we need to manage it that way. And we need to make that business as usual."

The growing perception of Y2K as a mission problem served to emphasize the cross-functional nature of ICT and the increasingly central role of the new information infrastructure in achieving the strategic goals of an organization. The overriding lesson was that the organization had to incorporate its management of ICT within its overall operational and strategic management: "The entire information technology portfolio…must be managed by a partnership of business and technical management to create business value. …In most businesses, deciding on information technology capabilities is far too important a strategic decision to be left to the technical people or, worse, to the outsourcer with its own business objectives and need to make a profit…" (Weill and Broadbent 1998). To align ICT and operational management, organizations need an effective enterprise-wide information strategy based on achieving organizational goals.

As Y2K evolved from a primarily technological to a primarily operational effort, it brought home the need to align ICT and strategic management. The experience of addressing Y2K reminded organizations that the ultimate goal of ICT was not the continued functioning of local clusters of technology but, rather, was the effective use of information in support of strategic goals. This lesson was particularly important to government and military organizations less driven by the demands of private enterprise and more likely to think of ICT as secondary support rather than as a major component of their operational product. The USAF was a prime example of an organization that faced this lesson as its Y2K effort evolved from IT leadership to operational leadership.

2.5 The Need to Manage ICT Cross-Functionally

Differences between traditional IT managers and operational managers were not the only organizational gaps that needed to be bridged in order to effectively address Y2K (or, more generally, to effectively manage ICT). The complexity of ICT makes it easy for people with differing perspectives to view the same system very differently.

Probably the most common perceptual barriers that had to be overcome during the Y2K effort stemmed from the organization of most corporate, governmental, and military entities into functional units. A worker's functional location impacts nearly every aspect of her or his organizational life. Information flow is a major component of this impact. In most organizations, information sharing "is usually up and down the structural hierarchy—up to superiors and down to subordinates—within functional boundaries"

(Davenport 1997). While there are many situations where it is entirely appropriate for workers to focus on their particular functional niche, most high-level operational and strategic objectives require integration across functional lines. In these situations, "stovepipe" perspectives can result in damaging operational and communication barriers. The Y2K situation emphasized that ICT is one such critical cross-functional activities, in which success often depends on overcoming stovepipe perspectives and actions.

Because of their structure and culture, military organizations are particularly susceptible to the problems that can result from the stovepipe effect. Fortunately, when faced with achieving cross-functional goals, leaders at the highest levels of these organizations recognize the importance of getting people to look and act beyond their particular area of the overall operation. For instance, "the integration of our aerospace forces and people is a critical element of our plan. This process will break down stovepipes between air and space, leading to integrated solutions with air and space systems that are more effective and efficient than separate systems" (Peters 2000). Nevertheless, even with this high-level recognition of the issue, cross-functional management of enterprise-wide projects can be extremely difficult to achieve.

During Y2K, the need to overcome functional barriers in the management and operation of ICT was particularly evident. As Y2K progressed, issues initially viewed as isolated within a particular technology under the control and responsibility of a particular functional area became increasingly intractable as those issues cut across technologies and functions. These cross-functional complications generally began at the level of ownership and responsibility issues and progressed to operational, strategic, and legal issues.

For example, most organizations began their Y2K efforts with a unit-by-unit inventory and assessment of at-risk technology (for the USAF this was called the Air Force All Systems Inventory, or AFASI). Yet, even at this early step, it could be difficult to maintain a functional unit perspective, particularly where ownership of and responsibility for systems were unclear. Whose name went into the inventory as owner of a given system that was paid for and developed (in conjunction with an outside vendor) by one functional unit, used by a number of different functional units, and supported by yet another functional unit? Who was responsible for certifying this system as Y2K compliant?

Given the pervasiveness and interdependency of system elements, tensions could arise that were difficult to resolve through central guidance. For instance, "[AMC] had an argument with ESC (Electronic Systems Center) that lasted for months over who the 'owner' [of certain software] was. Other systems have had the same argument over ownership" (AMC HQ). Or, "In AFASI there was a Sponsor, Owner, and PMO (program management office) field. Folks sorted out who these were on their own" (AFCA).

During Y2K, functional unit perspectives were further blurred by the central role of data. Section 2.3 discusses how changes to data formats were greatly complicated because databases not only contain instances of data but also represent how an organization views the world and conducts its business. Beyond this, database change was further complicated by the fact that data are commonly shared across systems. This meant that changes to one database owned by one functional unit could lead to the need for coordinative changes in other databases owned by other functional units (as well as

coordinative changes in all the software that read, manipulated, and transmitted that data). Another complicating factor could occur when one functional unit owned a system, but another unit owned the database (SSG).

All of these interdependent complications contributed to a highly uncertain atmosphere wherein no single functional unit could declare with absolute certainty that its systems would work in the face of Y2K. When these units turned to the makers of their system components to provide some answers, the same uncertainty, again stemming from the interdependencies of those components, was evident in the highly qualified statements of Y2K compliance that were provided.

> All CCRP controls and servers rely on services provided by the underlying operating system. While we have observed the behavior of CCRP controls and servers with dates above and below the Year 2000 rollover, as well as during a simulated rollover, it is not possible for us to fix bugs in the compiler, that compiler's run-time library, or operating system. Therefore, the accuracy of this, or any other product claiming compliance, may be affected by the operating system in use. (CCRP 1999)

> We had to assume that we would be operating in uncertainty. (374th AW/LG)

> The fear of the unknown is what drove the way business was conducted. (AMC HQ)

(Chapter 4 looks more closely at the impact of this atmosphere of uncertainty on Y2K risk assessment and response tactics.)

Another complication of the Y2K effort was the common occurrence of multiple sources of guidance. This complication stemmed from the application of functional perspectives to what was a cross-functional issue. Stovepipe Y2K management efforts often meant that Y2K workers had to be aware of and respond to numerous overlapping sets of directives. In many cases, this contributed to a significant increase in workload.

> There was an awful lot of redundancy from the stovepiping within the different functional communities for data gathering and reporting. …AMC had three reporting chains—the MAJCOM, the Air Force, and the unified command—each with their own unique reporting requirements, their own unique reporting format that covered a lot of the same data. We'd get guidance on the same issue from all three chains at different points in the process. We were continually having to stop, go back, and look at what we'd already done. We had to try and match the latest set of guidance with other guidance that we already had. If there were any problems, we had to figure out what to do about it and how to deal with it all. (AMC HQ)

One medical division was particularly impacted by underbudgeting man-hours for Y2K. As of December 1999, this division estimated more than 4,000 hours of additional Y2K-related effort. More importantly, they indicated that they had to respond to guidance from five different units, and they estimated that approximately 50 percent of their effort was spent in dealing with multiple guidance and policy. This was not an isolated situation nor was it limited to the Air Force.

"A lesson from Y2K is that we have underestimated the workload, the amount of tasking involved in communication, and the work involved in keeping up with directives and changes to the directives" (USFJ). In part, multiple Y2K guidance occurred because no single functional unit could adopt a response strategy

that adequately addressed the spectrum of uncertainties stemming from cross-functional interdependencies. For this reason, many large, multifaceted organizations found it necessary to establish a temporary cross-functional entity to oversee Y2K efforts (for example, the President's Council on Year 2000 Conversion). These entities tended to be operationally oriented, focusing more on mission capabilities than on specific technology within functional domains. As stated in the Department of Defense Year 2000 Management Plan, this meant that "progress will be measured not in terms of numbers of systems fixes, but in terms of warfighter mission readiness unimpeded by Y2K glitches" (USAF 1999b).

Through the use of these temporary cross-functional entities focused on "mission threads," attention could be paid not only to the functional nodes of an organization's information system but also, more importantly, to the links between those nodes. In the Air Force, this temporary entity was called the Air Force Year 2000 Office (AFY2KO). Chapter 4 looks more closely at the role of the AFY2KO and other Air Force organizational entities involved in Y2K, including examination of the issue of whether such a cross-functional entity is desirable on a more permanent basis.

There were many reasons for the often fragmented, piecemeal organizational perspective on Y2K. Faced with a complex, uncertain situation, people tended to fall back on what they understood best—their own particular corner of the organizational and ICT world. In addition, day-to-day operational issues and functional demands made it extremely difficult for individuals to keep in mind the cross-functional interdependencies of their systems as well as their roles in the overall flow of data and information to achieve organizational goals. Finally, organizational territorial issues and the mechanisms for funding systems worked against a cross-functional perspective, as with MSG: "We really didn't understand the configuration of our system of systems. That problem is exacerbated by the way systems are viewed and, more importantly, by the way systems are funded. They're funded individually as a system, and so there is no real impetus to look at it as a system of systems."

In many cases, these same issues continue to contribute to a fragmented approach to the ongoing management of ICT in general. "The Air Force's [information] efforts may not be as well integrated as they should be, which may result in duplication of effort and inefficiency" (USAF deputy chief of staff for air and space operations, reported in USAF 2000c).

Fortunately, the Y2K experience confronted many key people with the limitations of relying on piecemeal, functional perspectives to manage information and communication technology. Managers of the overall Y2K effort came away realizing they had been forced to fill in gaps that existed in the business-as-usual management of ICT. They realized that, from a mission-oriented perspective, ICT management was more about sharing ideas, developing appropriate trade-offs, and balancing competing "goods" than it was about making correct technology decisions. In other words, people need to be taught about teaming, sharing ideas, and working with one another cross-functionally as they enter the business. To do this: "we have to break down the barriers and walls both organizationally and procedurally, from a policy standpoint and from a security standpoint. There are some things that we've created over the last 50 years…that will keep us from being flexible in how we adapt to this kind of business in

the future" (AFCIO/AFY2KO). Thus, Y2K helped teach organizations the necessity of breaking down functional barriers in the strategic management of ICT.

2.6 The Need for an Overall Information Strategy Centered on People, Information, and Mission

The media portrayed Y2K as an issue centered on computer technology,[4] but managers on the Y2K front lines knew that far more was at stake. Previously, they had focused on specific components of their technology; now they were being called on to consider the role of that technology in the overall organizational operation. They were seeing that the interdependent elements of the ICT infrastructure were not fully under their control and could not be addressed in isolation. They were seeing that data issues could not be adequately understood independently of the interpretation and use of that data.

As this more holistic perspective grew (and as the new century approached), a change occurred in specific Y2K project goals. Whereas early on the goal had been to fix every possible glitch, the approaching deadline and increased focus on mission meant that glitches with little or no impact on operational goals could be ignored.

> **Issue:** The Real Time Operating System (RTOS) embedded on the Tadpole Technology SBC (system bus controller) does not recognize that the year 2000 is a leap year.
>
> **Resolution:** The only CompuScene SE application software that is affected by this issue is the DBLOAD off-line utility. Any files created or modified on 29 Feb. 2000 will have an incorrect date stamp. The data contained in the file [are] not affected. Since there is no operational impact due to the date stamp error, LMIS (Lockheed Martin Information Systems) plans to take no action on this issue. (LMIS 1999)

As organizations increasingly put their Y2K efforts within an operational context, they were doing more than simply changing specific Y2K project goals. They were also shifting the role of ICT managers from a support activity into the operational mainstream of the organization.

As Y2K progressed, ICT managers were increasingly placed in positions where their efforts were meaningful not so much because their technology worked, but because they enabled people to use data and information to accomplish operational missions. With this came a growing recognition of how the systems they managed fit into the larger organizational picture: "People saw for the first time that this information does fit together. Systems do support missions and missions do rely upon certain things. So that at least at a very high level the operational system world…suddenly came together—central management, mission funding, personnel, all these kinds of things" (AFCA). Despite this recognition, it remained a difficult proposition to develop and implement new long-term strategies for managing ICT systems.

For most technology managers, Y2K was a new organizational experience. Under previous business-as-usual practice, the investment in ICT had been essentially uncoordinated across the enterprise. During Y2K, the ICT community was called on to

[4] For example, the representation of Y2K on the cover of the June 2, 1997, issue of *Newsweek* depicted a computer screen breaking into pieces.

play a major role in a coordinated, strategic, mission-oriented activity. As with any new role, it was not always easy, as illustrated in the following excerpts:

> For the first time the SC community ran a command and control effort. We didn't do that real well in the beginning. We didn't understand how to do command and control the way other operators do it. And that is something we are going to have to evolve into if we are going to do what SSG is talking about, an active monitoring and command and control of this network asset. (AFCA)

> We do it now but it's fragmented. … We're doing it in bits and pieces. It needs to be…uniform. (SSG)

> There's a huge amount of confusion at the bases and MAJCOMs. …We're not consistent. Not just at…[our] level but across the rest of the Air Force. (AFCA)

The fragmentation and inconsistency of ICT management stemmed in part from the operational community having a strategic perspective the ICT community lacked and needed. The Y2K experience emphasized the need for an integrated ICT strategic perspective that started not with technology but, rather, with the people in the organization who created and used information, with the nature of that information, and with the missions that people accomplished through the use of that information. "Information and knowledge are quintessentially human creations, and we will never be good at managing them unless we give people a primary role" (Davenport 1997).

Y2K taught many ICT leaders that they needed to develop an enterprise-wide information strategy that would be aligned with the overall organizational strategy. "Leaders who were actively engaged in this process, they essentially 'saw the light.' I think those individuals in leadership positions will carry that throughout the rest of their careers" (AFCIO/AFY2KO). This recognition among organizational leaders helped stimulate efforts to develop an overall information strategy centered on people, information, and missions.

In the Air Force, steps toward developing such an overall information strategy began shortly after the New Year.

> Recognizing the importance of information superiority, Air Force leaders from a variety of functional areas met [on] March 7 [2000] to chart the future course of Air Force information operations. …Currently, the Air Force's efforts may not be as well integrated as they should be, which may result in duplication of effort and inefficiency. Creating an integrated Air Force approach to information operations is the goal of the Air Force IO (information operations) steering group [Headquarters USAF]. …Representatives from many functional areas were invited to participate. …This was the first time the [Air Force] Office of Special Investigations, weather, space, intelligence, surveillance, and reconnaissance, legal, communications and information, public affairs, Reserve, Guard and other key area representatives met at this level to develop a plan to integrate all of their individual information operations efforts. We didn't want to exclude any significant information operations stakeholders. …The representatives also discussed the legal issues—domestic, international and intelligence oversight laws—that affect the planning and execution of information operations. (USAF 2000c)

Clearly, the lessons of cross-functional management and attention to system environments were not lost on this group of Air Force information leaders.

Similarly, on April 14, 2000, the Air Force held a workshop on the lessons of Y2K for ICT management.[5] Again, cross-functional managers who had previously not come together found that they shared important pieces of the ICT management puzzle. They also found that these pieces would continue to be important for ongoing issues beyond Y2K. "There are some things we can do with CIP (critical infrastructure protection) and with information assurance… that will carry forth from the lessons that we learned from Y2K. Prior to this workshop that discussion really hadn't taken place" (AFCIO/AFY2KO).

It is no simple task to keep ICT technology functioning effectively on a daily basis, and it is not surprising that ICT managers must often focus on the continued functioning of local clusters of technology. However, Y2K helped remind organizations that ICT was an enterprise-wide activity and that ICT management needed to focus on more than technology. It needed to focus on the effective use of information by people in support of overall organizational missions.

Unfortunately, the struggle to understand and manage the critical relationships among technical, human, and organizational aspects of ICT systems is a difficult and never-ending process. Not surprisingly, there are strong tendencies to revert to a less comprehensive business-as-usual approach.

2.7 Do Not Return to Business as Usual

Many middle-level managers learned the lessons of Y2K firsthand, but some doubt the long-term impact of those lessons on the organization. "Those of us at mid-level management will carry forward the lessons that we learned during Y2K, but I'm skeptical about how we will carry these things forward as an organizational enterprise. Because I don't feel that we had the full buy-in throughout the organization on this problem" (AFCIO/AFY2KO).

There were a number of reasons why people who were not on the Y2K front lines would continue to view ICT management as a loosely connected, technology-focused business-as-usual activity. For one thing, most people not directly involved with the issue saw Y2K as a nonevent or, even worse, as a hoax. There had been threats of catastrophe, yet "nothing" happened. How could it be viewed as a watershed event with important lessons to teach?

Perhaps even more significantly, the crisis of Y2K forced people to grapple with complex issues that were not fully under their control. This is not a particularly comfortable position for most people. With the passing of the crisis came a natural tendency to seek a return to more familiar methods and roles. "Y2K made people do some uncomfortable things. Now that Y2K is over there will be a tendency to go back to doing it the old way" (MSG). Despite this tendency, one of the most important themes of this work is the need to retain and build on the lessons of Y2K, to resist the seemingly easy path of a return to business as usual.

Air Force ICT managers involved in dealing with the complexities of Y2K saw that existing business-as-usual practice could not deal with the situation, even

[5] This workshop was part of the National Research Council study that produced this report.

as they experienced the benefits of changing that practice. Furthermore, they recognized the "need to take some of the things we've been talking about [in the Y2K Lessons Learned Workshop] and make that the new business as usual" (AMC HQ).

This call for changes in ICT management practice did not suggest an absence of useful procedures in place before Y2K. On the contrary, at the tactical level, staff complained that the new processes they were pressed to use for Y2K duplicated existing structure (374th AW/CS).

At the strategic level, however, Y2K leaders saw a clear need for change. They had struggled to fill the gaps in the overall management of ICT. They had developed an organizational context for what had been an essentially fragmented management activity. With the Y2K effort complete, they grew concerned that their newly developed context would not result in ongoing benefits, specifically, that the enterprise as a whole was not being considered. Even with a new management and policy, the strength from an enterprise standpoint was being lost, and the momentum gained through Y2K was rapidly falling away. In short, they were "losing…[their] opportunity to maintain the enterprise perspective" (AFCIO/AFY2KO).

A critical issue was that temporary organizations and money had been used to guide the Y2K effort, and as a result, no permanent homes had been established for the arduously developed policies and practices.

> We get into this issue of spinning up special organizations to deal with problems with unclear integration plans. Once we know that organization is going to go away, what happens to the policy that came out of that program? What happens to the funding that was tied to that program? What happens to requirements that were associated with that program? I know for a fact that in the case of Y2K none of that was put in place. (AFCIO/AFY2KO)

Despite the barriers to implementing an ongoing integrated plan for managing ICT systems, some leaders saw the lessons of Y2K to be both compelling and even inevitable.

> We now recognize the interrelationships between organizations and functional areas … we would be remiss in our responsibilities if we turn around and go back to doing business as usual. … Organizations have to … see changes as they occur and make adaptations … learn from the mistakes they made and the things they did right. … To turn around and try to go back to business as usual is not only impossible, it's the wrong thing to do. (AFCIO/AFY2KO)

The general lessons of Y2K were felt strongly by many who participated in the experience, and these lessons are critical to the successful management of ICT. Nevertheless, without accompanying organizational change, these lessons cannot provide ongoing benefits. It is far simpler to call for an enterprise-wide ICT management strategy than it is to make it happen within a complex, dynamic organization. The next chapter examines organizational aspects of the Air Force Y2K experience, with a focus on institutionalizing the general lessons of Y2K.

Chapter 3 Aligning Organizational and ICT Strategies

> While the organization as a whole is becoming more and more *interdependent*, the parts increasingly display choice and behave *independently*. The resolution of this dilemma requires a dual shift of paradigm. The first shift will result in the ability to see the organization as a multiminded, sociocultural system, a voluntary association of purposeful members who have come together to serve themselves by serving a need in the environment. …The second shift will help us see through chaos and complexity and learn how to deal with an interdependent set of variables. (Gharajedaghi 1999)

Chapter 2 focused on general lessons of the Year 2000 (Y2K) that establish a need and indicate an overall framework for an integrated, enterprise-wide information and communication strategy. This chapter focuses on more specific lessons of Y2K that can be used to translate that general framework into organizational practices and tactics. This can be an extremely difficult task. Like information and communication technology (ICT) systems, organizations are dynamic open systems consisting of "organized wholes of many variables" (Bertalanffy 1976). Anyone involved in managing the coevolution of these two highly complex, fundamentally different yet interdependent systems (that is, ICT and the organization itself) is engaged in a never-ending effort to improve a situation, not a grand scheme to achieve final victory.

Given the complexity of managing ICT within the context of a specific organization, the notion of an organization's "information ecology" has been gaining visibility (Davenport 1997).

> Complete alignment [between the information technology portfolio and the business strategy] is usually nonsustainable because strategic context constantly changes and because information technology portfolios are assets that take a long time and significant investment and expertise to develop. … Alignment is dynamic—a change in any one of the ingredients usually requires another shift elsewhere. The goal is for information technology investments and the portfolio to be heading in the right direction to maximize the value of those investments to the business. (Weill and Broadbent 1998)

Although this is a business school perspective, it nevertheless sounds more like tending a garden than balancing a financial spreadsheet.

Many United States Air Force (hereafter simply USAF, or Air Force) leaders already share a vision in which major elements across the service will operate within a single integrated system. This vision acknowledges the open nature of commanding such an integrated environment, calling it an art. There is even the recognition that achieving this vision requires organizational change, as stated in the Air Force Vision 2020. "We operate aircraft and spacecraft optimized for their environments, but the art of commanding aerospace power lies in integrating systems to produce the exact effects the nation needs. To meet this need, we've modified our command organizations to take full advantage of air, space, and information expertise."

With slight modification, this Air Force vision statement could serve equally well as a vision statement for managing ICT: We operate ICT systems optimized for their environments, but the art of managing ICT lies in integrating systems to

produce the exact effects the organization needs. To meet this need, we will modify our organizations to take full advantage of mission and information expertise.

When most people hear the phrase "system integration," they think of technical issues, such as machine compatibility and achieving common operating environments. From this computer-centric perspective, two systems are integrated if they are electronically linked and can communicate with each other. However, the Y2K experience demonstrated that cross-functional ICT challenges, particularly those involving the interpretation and use of data and information, cannot be defined solely or even primarily in terms of technology. Like Y2K, current ICT management challenges such as system integration, information assurance, security, and life-cycle management cannot be met on purely technical grounds. Because ICT is pervasive, yet personalized; affects everyone, yet has no single owner; and is intimately tied to organizational missions, broad-based ICT issues inevitably generate tensions across various organizational boundaries. Y2K was a warning that technical solutions to broad-based ICT problems that fail to consider these tensions are unlikely to succeed.

Under the added strain of Y2K, the impact of cross-organizational tensions on Air Force ICT policy and practice became increasingly evident. While the tensions and related issues were exacerbated by Y2K, they are a fact of organizational life even during periods of business as usual. In most cases, these tensions represent competing yet mutually desirable "goods" (for example, additional functionality versus tighter security), each of which needs appropriate representation within the organization. For this reason, attempts to solve these problems by eliminating the tensions that caused them are generally unrealistic and even undesirable. One-dimensional cures aimed at establishing enterprise-wide ICT uniformity can be worse than the problem. Rather than seeking to eliminate ICT tensions, management strategies and tactics need to carefully consider and appropriately balance these dynamic multidimensional demands. Such strategies and tactics must be based on an enterprise-wide view of the varied ways that information is used to achieve organizational goals.

The remainder of this chapter explores specific organizational lessons of the Air Force Y2K experience that clarify and expand on the art of managing integrated ICT systems. These lessons are discussed under the following general headings:

3.1 Balance Central Management and Local Execution
3.2 Consider Evolution of the Problem over Time
3.3 Clarify Ownership and Responsibility
3.4 Consider the Impact of Local Diversity
3.5 Consider the Role of Local Autonomy
3.6 Build Trust Between Local Administrators and Central Managers
3.7 Strengthen Horizontal Relationships across the Organization
3.8 Overcome Funding Disincentives to Working across Organizational Boundaries
3.9 Clarify the Appropriate Level of Central Guidance and the Role of Central Administrators
3.10 Address Cross-boundary Issues in Life-Cycle Management of Systems
3.11 Tackle the Huge Informational Effort Needed to Support Management of Integrated Systems
3.12 Address Issues of Organizational Culture
3.13 Empower Permanent Organizational Entities Focused on Cross-boundary Issues

These organizational lessons of Y2K can help guide not only the Air Force but also any organization seeking to integrate ICT systems and to align management and use with organizational goals and strategies.

3.1 Balance Central Management and Local Execution

Probably the most pervasive organizational ICT issue is the intricate and dynamic tension between central management and local units or departments. Neither the central nor the local perspective is right or better, and it would be neither feasible nor appropriate to attempt to eliminate the differences between them. Achieving an effective balance between central management and local execution is a critical component of any organizational information strategy. During Y2K these tensions were especially evident and had significant impact. In fact, nearly all the lessons discussed in this chapter relate in some way to tensions across the horizontal layers of an organization.

The Air Force is well aware of the desirability and complexity of balancing these tensions, since its overall management strategy, commonly referred to as "manage globally, execute locally," depends on it. This popular strategy extends far beyond the Air Force. At many organizations in the public and private sectors, top-level managers use some version of this strategy as they simultaneously attempt to coordinate action toward a common goal while freeing individual groups to adjust tactics to their specific conditions.

In the Air Force, the manage globally, execute locally strategy is implemented by designating a single point of contact (POC) for each major action or issue. The POC provides general guidance to local units who act on that guidance within the context of their individual situations. Y2K demonstrated that ICT presents special challenges to this strategy.

Over the course of its Y2K effort, the Air Force found it very difficult to establish consistent guidance under a single POC. This was evident across numerous levels, functional areas, and locations. For instance, ICT staff received guidance from and were accountable to several POCs, or bosses. The difficulties with this arrangement included a lack of organization and format (AFY2KO), the dynamics of dealing with multiple bosses (AMC/SCA), and demands for the same data in different formats (375th AW/MDG). In some cases, this resulted in excessive use of man-hours: "We put in about 20,000 man-hours overall. It should have been about 12,000" (375th AW/MDG). During Y2K, many complicating factors made it difficult to implement and effectively employ standard Air Force management practices based on central guidance and local execution. These factors are important to understand as part of a postmortem to Y2K, but far more importantly, they are general facets of ICT that continue to complicate ongoing management of this critical resource. As lessons learned from Y2K, they must be taken into account in the implementation and maintenance of any enterprise-wide information strategy. These lessons are discussed in the following sections.

3.2 Consider Evolution of the Problem over Time

One set of factors that complicated the effort to manage globally, execute locally stemmed from tensions generated by the way Y2K evolved over time. Chronologically, Y2K's evolution ran counter to this standard management strategy. Rather than evolving from central awareness and management to local execution, the Y2K experience—as with most large ICT problems—evolved from local identification and action to central awareness and management (AFCA). For instance, MITRE first became involved in the Air Force Y2K effort in 1993 (Cheyenne Mountain) and then again in 1995 (AWACS), before the organizational issues with Y2K were prominent. This process was similar to the evolution of Y2K in industry.

Once the Y2K problem reached a certain critical mass, management efforts rose up the chain of command and out across the military and government. Specifically, "in October 1997 there was no Y2K policy or guidance; in November 1997 the original guidance was that everybody should report to the host units; …[by] spring 1998 the policy was that everyone should report up the chain of command. This caused problems" (AMC/SCP). As higher levels of command became involved, so did Congress and accompanying oversight staff, each with "their particular view of [Y2K]" (MITRE). For AMC/SCP, the process for Y2K fixes was "(1) MAJCOM discovers the problem and finds a solution;… (2) policy is created; (3) three months later the Air Force comes out with a [different] policy…to fix the problem;… (4) three months later the DOD [Department of Defense] comes out with a policy that again forces us to do Y2K checks but in a different format….Those after-the-fact policies…led to the MAJCOM being hesitant to put out policy." Similarly, from the perspective of the 374th OG, "We couldn't tell who was asking what. We just had to do things again and again."

From the local perspective, the gradual upward and outward shifting of problem management produced a changing and, at times, redundant policy, making it difficult for local Air Force Y2K managers and staff to find a way of coping with the situation. Even as local Y2K staff struggled with the uncertainties of an evolving policy environment, central managers were experiencing their own growing uncertainties. In this case, uncertainty grew over time as managers became increasingly aware of how Y2K risk was complicated by the cross-functional, interdependent aspects of ICT. These managers saw the need to achieve consistency and accountability in the service-wide Y2K response, but this was greatly complicated by the diversity of local ICT activities. "Numerous places…[use] Air Force personnel to do systems development. They have their CDA (central design activity); we have our CDA. They don't use our tools; we don't use theirs. We don't talk to them—maybe at conferences sometimes. MAJCOMs do their own development. Even the National Guard does its own development in some small part" (SSG).

The difficult task of managing interdependencies was often heightened by a lack of global information at the local level. "There was a lack of understanding in the functional community of how…systems…worked together. The functional world understood the processes their systems went through, but because of manpower downsizing and people changing jobs,… the people who really understood that System A passed its information to System B through System C weren't there" (MSG).

Although problems at the local and central levels were different and could therefore lead to tensions, they were both related to the ways Y2K evolved over time. In this context it is instructive to compare large ICT problem-solving activities to large ICT central initiatives. While problem-solving activities such as the Y2K effort tend to evolve from local recognition and activity to central management, large ICT initiatives tend to follow a reverse evolutionary pattern, one that more closely resembles the manage globally, execute locally principle. Nevertheless, the initiative's pattern of central management to local execution generates its own set of tensions between central and local units.

With Y2K we saw that local identification and execution existed before global management was established (or even seen as necessary). On the other hand, with large ICT initiatives, such as the Defense Messaging System (DMS),[1] the concept is usually generated centrally, while the reality of that idea is subsequently identified and tested locally. "Usually ideas come from top down… but feasibility must filter up from the bottom" (375th AW/NCC). In addition, at any given time there are generally numerous overlapping system initiatives, forcing bases to "just field [them] and then try to figure [them] out" (374th AW/SC).

In this situation, local executors become testers for centrally developed projects, often bringing to light unanticipated problems that then filter back up the layers of the organization, perhaps leading central managers to adjust their initial plans. This not only occurs with big programs but also with relatively small, highly frequent changes. For example, patches are function-specific, but when loaded onto a local system, they often introduce a new problem, one that may not be easily resolved. In some cases, unanticipated local problems can force central management to abort a patch load altogether (374th AW/OG).

Bases do not generally like to see themselves as a testing ground for central ICT initiatives. Local units are focused on their functional missions; they expect that those missions will be enabled, not disrupted, by their ICT. Thus, when the central idea does not match the local reality, it can generate strong responses and loss of support at the local level (375th AW/NCC).

ICT issues can evolve across organizational layers in two directions: large problem-solving activities evolving up into centrally managed initiatives, and centrally managed initiatives evolving down into locally driven problem-solving activities. Each related pattern has the potential to generate tensions across those layers. In addition, given the often rapid pace of ICT change, central ICT management can face a difficult task just in keeping up with the current version of these dynamic issues.

While Y2K was primarily a problem-solving activity, the tensions associated with central initiatives were also visible in the Y2K response effort both because Y2K itself evolved into a centrally managed initiative and because Y2K efforts became closely interrelated with ICT initiatives in such areas as version control, certification, configuration management, testing, continuity planning, and security. (The first four of these areas are discussed in Section 3.10, the last two, in Chapter 4.)

Despite the various tensions from differences at the local and central levels, it is important to keep in mind that each represents critical and compatible strengths. Local

[1] DMS is an initiative led by the Department of Defense to establish secure e-mail throughout the department.

units more quickly recognize and respond to specific evolving issues, while central units more easily understand and respond to the need for compatibility and coordination of effort over time. For these strengths to be integrated, the tensions that can arise between central and local perspectives must be constantly and creatively managed.

3.3 Clarify Ownership and Responsibility

Another source of the organizational tensions that complicated the management of Y2K (and continues to complicate ongoing ICT management) was a lack of clarity in the ownership of and responsibility for ICT systems. "It's never one person who owns a system" (374th AW/XP). Generally, local units attempt to assert control over the systems they rely on. During difficult times such as Y2K, however, central ownership of these shared systems could be seen as desirable, since it lessened local responsibility for assessing and addressing the problem. The 374th AW/CS, for instance, viewed "70 percent of systems…[as being] out of local control; that is, the managing unit…[was not] on base. Therefore, 70 percent of assessment was already done." Central ownership could be viewed as meaning central responsibility for a system's functioning. "We have no access into C2IPS (Command and Control Information Processing System), so we have to take [central's] word on Y2K compliance" (374th AW/CS).

If other units owned their systems, then local units were free to interpret central Y2K policy as best suited their needs. This was especially visible at overseas (OCONUS) bases, where stressful frontline conditions and limited resources increased the incentive to minimize the demands of the Y2K response. This is illustrated by such statements as: "It was a moot point to freeze our systems because systems are centrally controlled," and "We didn't have to do most DOD tests because we're at the end of the…[system] chain" (374th AW/CS). Yet even at major stateside (CONUS) bases, unclear ownership and responsibility could be a complicating factor. "We argued with the Audit Agency over who is responsible for making sure the base has updates—the base or PMO (Program Management Office)" (375th AW/CG). In addition, like their OCONUS counterparts, CONUS bases could interpret central ownership as meaning that primary responsibility for assessment was not with the local units. "C2IPS is on the infrastructure spreadsheet. Systems like this that are used but not owned appear on the database … but aren't inventoried" (375th AW/CG).

In actuality, neither central nor local units alone can be fully responsible for shared ICT systems. Even when central units are solely responsible for development and fielding of organization-wide off-the-shelf systems (whether government or commercial), these systems invariably require ongoing adjustment for implementation, operation, and maintenance under local conditions and needs. For this reason, a comprehensive assessment of shared ICT requires an appropriate integration of central and local evaluation.

Another aspect of unclear ownership of and responsibility for ICT systems is that different components—and even parts of components—can be viewed as being owned or under the responsibility of different units. For instance, "the last 50 feet of wire belongs to AMC (Air Materiel Command), and anything that belongs to AMC is reported through

AMC channels" (AMC/HQ). This can result in potentially confusing arrangements that impact ICT management practices.

In particular, local users of ICT systems can face a confusing picture when deciding with whom responsibility lies. For a system problem, users may contact the functional system administrators; for a Windows problem, they contact another technical group. Each group has a local expert who discerns whether problems have resulted from commercial off-the-shelf (COTS) hardware or the system itself. The result of having different agencies responsible for different parts of an end user's system is less than optimal (374th AW/CS).

One of the important benefits of the Y2K experience was that it forced diverse owners of systems and overlapping system components to communicate with each other in an effort to coordinate responsibility. Unfortunately, much of this valuable information and communication is being lost. (See Section 3.6 for further discussion of information needs in support of integrated ICT management.)

3.4 Consider the Impact of Local Diversity

Closely related to ownership and responsibility issues are issues that stem from the diversity of local ICT environments and resources. Multiple ownership and guidance may confuse individual users as to who is responsible for the different parts of the complex systems they rely on, but central owners and maintainers of those systems face the equally confusing task of understanding and managing a complex system of systems that spans significantly different functional and geographical environments.

During Y2K the effort to provide central guidance was greatly complicated by the diversity of local ICT conditions. Even central management of a specific piece of software with a common function had to account for complications that could stem from differences in local and mid-level management. "For Scott [Air Force Base], supply is under AMC; at Yokota, supply is under PACAF [Pacific Command]. But each base uses the same system, SBSS (Standard Base Supply System)" (374th AW/CS).

These differences in ICT management contributed to diversity in response activities as central guidance filtered down to local execution. The divergence of interpretation of central guidance sometimes began at high levels and involved cross-service entities, creating potential confusion well before it reached the even greater diversity of frontline conditions. In one instance, the Commander in Chief (CINC) and PACAF received the same guidance, but by the time a base (under PACAF) and a tenant at that base (under CINC) received it, the guidance was different (USFJ).

In addition to management differences, local diversity of ICT resources was another important complicating factor for central managers. These differences occur across many units and at many levels, but they were particularly evident during Y2K within the operating environments at OCONUS bases. Even though systems staff had been "told that all bases had new equipment," old equipment (for example, copper wires and low-bandwidth modems) was still in use and could not support many of the new systems. Updating all the bases was a six-year project, which meant that some bases would not receive new equipment for several years: Yokota, for instance, was the second-to-the-last base to be updated. Differences

like these mean there is great variability by location in the demands during a large ICT problem-solving activity such as Y2K. This issue continues to impact such service-wide ICT efforts as DMS (374th AW/SC).

Complications that arise from the diversity of local environments can be greatly exacerbated by the way systems are viewed. The risk of disruption from local diversity greatly increases when systems are developed and fielded in isolation rather than as a piece of a larger system of systems. "Ideally, programs should be tested higher up. The programs are time line driven rather than event driven, so the engineering and installation ends up happening at the bases" (374th AW/CG).

This is more than just an Air Force issue. The success record of large ICT projects throughout government and industry is very poor (see Section 3.13), and many of these difficulties can be traced to a failure to anticipate the impact of local changes on the overall system. This occurs even within the most technically perceptive organizations: for example, in 2001 the isolated test of a WorldCom employee "crippled NASDAQ's network" (Weinraub 2001). (This issue of cross-boundary interdependency is discussed further in Section 3.10.)

3.5 Consider the Role of Local Autonomy

Local diversity issues can be further complicated by a high degree of local autonomy. This autonomy stems from facets of the organization and of ICT itself. In the Air Force, local autonomy is fostered in part by the ways ICT is funded or, as is often the case, not funded. Many times, "systems are fielded without funding in hopes that bases will find their own funding for them" (375th AW/CG). As a result, regardless of certification or policy, if a base lacked the funding to implement a system, implementation did not occur.

Without accompanying funding, there can be only limited confidence in the effectiveness of central guidance. However, the wide diversity of local conditions and infrastructure greatly complicates any effort to centrally fund ICT guidance. (See further discussion of ICT funding in Section 3.8.)

Where central funding does not accompany central guidance, local units may be unable or unwilling to follow that guidance. On the other hand, the existence of flexible money can enable local units to do what they want outside of central guidance. Thus, International Merchant Purchase Authorization Cards (IMPACs), military credit cards for flexible purchases, represent the other financial side of local autonomy. In the case of ICT purchases, local initiatives outside of central guidelines can greatly complicate the central management effort. For instance: "folks use IMPAC cards to buy stuff and hook it up to the network. … We have no central way of knowing what's on the network" (374th AW/CG). In addition, because the use of IMPAC cards bypasses the standard purchasing process—and therefore the standard approval process—security problems may be detected after the fact (if at all).

> There is a problem with the use of IMPAC cards and not using the standard process. Operational commanders listen to the local IT expert in their units, and he says, "We really depend on the network and if we put a modem on this box we can go out and back up the network on the Internet." And the commander signs off on it. Next thing you know I detect a security problem and I'm investigating it. And then I'm asking them where their approval is. … (375th AW/CG)

On the other hand, the use of IMPAC cards to support local ICT initiatives can be seen as a local user's response to rapidly changing needs within the context of a slowly changing bureaucracy. "Government tends to be very slow and makes it very hard to change direction, yet the entire information technology field is characterized by very rapid change. … So users go off and do their own things—that's why IMPAC cards came out. People couldn't do what they wanted quick enough through our means, so they purchase and build…miscellaneous little [utilities] on their own…because that meets their needs" (MSG).

While funding is a critical contributor to local autonomy, it is not the only one. Inconsistent ICT guidance, quite evident during Y2K, also frees local units to choose their own courses of action. For example, "last year we refused to install [a business system]… because [we] got conflicting guidance from SSG and PACAF" (374th AW/CS).

Sometimes, questions about central guidance are raised by the use of less formal, individualized communication channels that appear to be quicker and more reliable to local ICT managers. This occurred frequently during Y2K as local managers sought additional information and clarification of central policy that was often changing or unclear. For instance, "[Our] guidance came…through PACAF. However, I was part of the AFCA newsgroup so I'd get to see their spin was on what PACAF said" (374th AW/SC). These informal communication channels could be very helpful, but they further increased the likelihood that local units would find their own ways to interpret central guidance.

Another issue related to local autonomy is the creation and use of locally developed software and systems. Because these systems are motivated by and tailored to specific situations they can often better address local needs, including ease of use, at least in the short term. However, these systems can easily result in duplication of effort, such as double entry of data, and difficult maintenance problems when the local developer leaves the unit (374th AW/CG).

Locally developed software was a particular concern during Y2K. Date formats could be idiosyncratic, and data processing and flow could be difficult to understand, especially if the developer was no longer available. In addition, many Y2K fixes came from commercial providers, not in-house staff, so they did not address these "homegrown" systems.

Addressing the concerns about locally developed software became another side benefit of the Y2K effort in that less visible problems were noticed and potential long-term problems were identified. For example, AMC/SCA was required to upgrade a program written in an old version of Access to be Y2K-certified. Fortunately, this coincided with the imminent retirement of the staff member who had written the program.

3.6 Build Trust Between Local Administrators and Central Managers

For many reasons, including those already discussed, local system administrators can develop considerable skepticism about central ICT guidance. This can make it difficult to predict the outcome when central guidance meets local execution. During Y2K a master sergeant at an OCONUS base was under additional pressure to deliver administrative system reports. He preferred to use an alternative software package to generate the reports rather than the approved package he was told to use in central guidance received through his major command (MAJCOM). (See discussion of system certification in Section 3.10.) He had experienced considerable problems in working with the approved software, problems that he attributed to insufficient bandwidth on his local network. He concluded that this was yet another case of central managers not understanding his local conditions. There was no one he could turn to for support of the approved software, so he went to people he knew within the local systems group and got them to sign off on his use of the alternate system, and he got his reports in on time.

While the master sergeant's general concerns—that is, lack of local support for the system, too-low bandwidth, and generality of central guidance—are important to consider, there is another version of this story as told by a captain in the systems group responsible for system configuration. From the captain's perspective, a master sergeant has invested in learning a software package that facilitates his work. He then is told he should be using a different package. The sergeant halfheartedly tries the approved package and experiences a variety of problems. He receives a quick approval from some systems staff to use his preferred package, without the knowledge of the captain, who is responsible for network configurations. (One office within the Network Control Center [NCC] provided one level of approval without the other office being informed.) In addition, the captain disagreed with the sergeant's view of the specific problems, attributing them not to insufficient bandwidth but, rather, to incompatibilities between the approved and non-approved software packages.

A number of possible issues are involved in this scenario. The approved package may or may not be the best option for the local environment. There are cases where local personnel appropriately consider critical aspects of their unique situation that global management does not anticipate. In such cases, it is important to consider whether central guidance is being issued at an appropriate level, focused on enterprise-wide organizational goals that allow for a greater diversity of local execution to achieve those goals. (For further discussion of this issue, see Section 3.9.)

On the other hand, there are less desirable (though no less important) reasons for local resistance to central policy, including lack of communication, failure to develop local investment in desired changes, lack of training, and user investment in existing successful practices. Local management and staff recognize their accountability to central authority; sometimes, however, new policy or procedures are counter to accepted practices or legacy versions at a particular base. Therefore, local staff may refuse to implement them (374th AW/XP). At other times, local system administrators may consider new policy a less than optimal solution for their situation, and in these cases, they develop their own solution or work-around (374th AW/SC). Other relevant issues to address include:

- Was the approved package too difficult to install?

- Was NCC's role as a mediator between the MAJCOM and the local user clear and effective?
- Was there sufficient training and local support?

From one perspective, staff who circumvent central policy are likely to create difficulties for others; from another perspective, people like the master sergeant (trained in logistics, with only occasional short courses in system administration) are showing initiative in the face of an expanded mission.

One conclusion is clear, however: within ICT, numerous conflicting and interrelated factors make it difficult to anticipate what will happen when central policy meets local execution. This unpredictability greatly complicates central ICT management activities in such areas as configuration management and version control. This became clearer during Y2K, when central software managers had a greater need than usual to track the version of software packages in use. "'Versions released' does not always equate to 'versions in use,' especially in the client-server environment. Some versions were…not installed. Some were installed wrong. Some of the program offices were allowed to release their own software, …[which was] almost impossible to install…" (SGG). (Version control and related ICT life-cycle issues are discussed further in Section 3.10.)

Because of the many tensions that can arise between central ICT management and local execution, the complications associated with the way ICT problems and initiatives evolve over time, and the diversity of conditions and rapid rate of change, it can be extremely difficult for central managers to stay current on a given overall situation. In many cases, central management finds itself grappling with what are actually earlier issues that have evolved into new challenges at the local level. This can result in further rifts between local administrators and central managers. Trust between local and central administrators is needed to break this potentially destructive cycle.

While problems with communication and trust between local administrators and central managers were evident during Y2K, they extend far beyond it. Any broad-based ICT initiative or problem-solving activity runs the risk that centrally driven activities will break down into a set of local tests and solutions. To minimize this risk, organizations need enterprise-wide information strategies and tactics that mediate the tensions between central and local ICT personnel. In particular, stronger relationships across vertical organizational boundaries can reduce risk and unpredictability by increasing trust, facilitating communication, and focusing decision making on shared organizational investments, goals, and missions rather than on individual and diverse technologies or conditions.

3.7 Strengthen Horizontal Relationships across the Organization

In addition to vertical tensions across hierarchical organizational layers (for example, Headquarters [HQ], MAJCOM, base), there are equally critical horizontal tensions across functional organizational lines. During Y2K these horizontal tensions also worked against effective global management and local execution of Air Force ICT. In fact, some managers who went through the Y2K experience and faced the many ongoing ICT issues

discussed in this chapter considered horizontal issues to be even more problematic than vertical ones. In many cases "…the vertical structures for management and policy…[were] being maintained or strengthened to a certain degree, while the horizontal relationships…[were] not. The investment…[was] not clear. …[There was no] strategy for relating that investment across the enterprise" (AFCIO/AFY2KO). Given the overall focus on functional groupings in most organizations, the lack of strong horizontal relationships is an extremely common barrier to effective cross-organizational ICT policy and practice. Communication paths generally run up and down functional lines, the well-known "stovepipe" problem. (This issue resurfaces throughout the remaining lessons of this chapter.)

However, while some aspects of horizontal tensions are unique from vertical ones, both are generally intermingled within the context of a given ICT issue. In addition, both require a common integrated solution based on an organization-wide ICT policy that increases cross-boundary trust, facilitates cross-boundary communication, and focuses decision making on enterprise-wide goals and missions.

Who owns ICT policy? How is it promulgated and maintained throughout a complex organization? How does this policy change as it travels across horizontal (and vertical) organizational boundaries? A large, diverse, ICT-dependent organization such as the Air Force can find these kinds of questions extremely difficult to answer, as is illustrated in the following interview:

> **Interviewer:** Who sets IT policy? Let's take a specific example—that there will be a certificate to operate[2] and that it will be negotiated between SSG and the MAJCOM. Where did that guidance come from?
> **MSG:** The CIO?
> **SSG:** I think it probably started with General ___.
> **Interviewer:** It sounds like the answer can be complicated.
> **AFCA:** The answer is very complicated.
> **SSG:** Where it starts and who owns the policy are two different things.
> **AFCA:** It's very complicated, …especially where an organization has to always operate across boundaries, which we do. It's chaos. It's almost anarchy.

The Air Force Communications Agency's (AFCA's) sense of "almost anarchy" when ICT policy must operate across organizational boundaries is revealing, particularly in light of an analysis of the continuum of organizational approaches to controlling information (see Figure 3-1).

[2] It was proposed that no software be run at a base without a certificate to operate issued by the MAJCOM in consultation with SSG.

Figure 3-1 The Continuum of Information Control

Source: *Information Ecology,* by Thomas Davenport, p. 69

In his research, Thomas Davenport (1997) found a continuum marked by four general states of information control in organizations: (1) monarchy—"one individual or function controls most of a company's information"; (2) federalism—"representative democracy, a weak central government, and a high level of local autonomy"; (3) feudalism—"business unit managers control their information environments like lords in so many separate castles"; and (4) anarchy—"every individual fends for himself or herself." These descriptive states are neither good nor bad by themselves. Different combinations and states of control can work well in different organizations and under different circumstances.

If the Air Force attempted to articulate its overall ideal information strategy along this continuum (a highly beneficial activity), it might fall closest to federalism. Anarchy would likely be an undesirable state. Yet during Y2K, as AFCA points out, anarchy nearly resulted when central policy broke down under the strain of working across organizational boundaries. Few formal mechanisms existed for developing and maintaining a shared cross-organizational vision of ICT policy and practice. Such mechanisms are needed to support strong horizontal (and vertical) relationships and communication.

During the April 14, 2000, Y2K Workshop, a discussion among managers from a wide range of functional units (from MAJCOMs to HQ) revealed some of the multifaceted strain that results when ICT policy makers attempt to work across organizational boundaries without strong existing relationships and cross-functional communication mechanisms. Without such mechanisms, it is extremely difficult to develop clear, shared enterprise-wide strategies and tactics. While the people who took part in this discussion impact each other in their organizational roles, they had rarely interacted as in the workshop and, in many cases, were meeting each other for the first time.

The discussion centered on policies for assuring that Y2K problems (or problems resulting from Y2K fixes) did not surface during 2000 and covered a number of tactics. These included: (1) block releases—requirements for releasing software on a fixed schedule (for instance, once a quarter) rather than as the individual system is ready; (2) code scans—applying an automated tool to check code for errors; (3) certification—formal approval after certain defined criteria (which could include code scanning) have been met; and (4) continuity of operations plans (COOPs)—which are discussed in detail in Chapter 4.

The participants began with a well-intentioned effort to explore new ways of working together across functional boundaries; however, local considerations quickly

took over, complicated by unclear policy, vague practices, funding barriers, disputed definitions, and the impact of players outside the organization. Tensions arose during the exchange, which is paraphrased below.

> Air Force policy states that for every block release throughout calendar Year 2000, those systems would be re-code scanned and re-Y2K certified. Could we use this as an opportunity to move a little further toward an enterprise view and find homes for these activities?
>
> It would kill us if you told us we had to do that.
>
> Well, that's a signed policy.
>
> That's for users. I can tell you right now we're not doing it.
>
> That was my question—are we going to do it?
>
> If the Air Force were to mandate this to us, then the Air Force would have to come up with the money to pay for it, because US TRANSCOM isn't going to pay for a requirement that isn't on a joint command.
>
> Maybe you can refresh my memory, but I thought that was a mandate. Here we go with mandates and funding.
>
> I think it was, but I'm not sure. I'll have to go back and check it. We need to clarify which policies were to be carried through the Year 2000.
>
> Re-code scanning and Y2K certification of block releases were signed off and were supposed to go through the Year 2000.
>
> I think that's half correct—the policy does state that you will code scan block releases throughout Year 2000 or well into the Year 2000, but the part about certifying is not there.
>
> We were not going to re-certify, I know that.
>
> The code-scanning requirement is still there by Air Force policy.
>
> What do you mean by code scanning?
>
> Just what you did before when you gave it to SSG.
>
> Determining whether you inadvertently introduced a bug that would now make it non-Y2K compliant.
>
> [Lots of simultaneous discussion, at which point the moderator stepped in and asked for additional clarification as to how Y2K policy had been established.]
>
> Let me explain why there is some confusion about that. At times, half of a policy would get signed off and half of it wouldn't. We put the plan together and sent it up and they never signed. Yet MAJCOMs took the guidance and followed it—how to use the database, how to use the Air Force spreadsheets, how to use all those kinds of things. It was a mechanism for people to do something but it was never signed. The COOP guidance 10-232 was signed, but in other cases there was a lot of confusion because policies would go up and sometimes they would be signed and sometimes they wouldn't be. Yet they'd still be followed to a certain extent.
>
> When you say that part of the policy isn't fully developed or doesn't have clear funding, that's got far-reaching impacts. For example, we just fielded an emergency release of our in-transit visibility system about a week ago, and I know it didn't go through code scanning because we fielded it in the space of about a week or two.
>
> I can speak to that. We were working on the latest version of our system and got results back on the code scan from two or three versions ago. We were asked to respond to these comments, but it's kind of pointless when you're already two or three versions later. We offered to send a new version down and have it scanned. The answer we got back was "we're out of money so don't bother." So even though we may have a bug and even though there may still be Air Force policy out there that says scan every 6 months through the end of 2000, it isn't going to happen because there's no money.

As discussed in previous sections, some of the tensions manifested in this exchange are between central policy and local execution (although earlier we often saw

the base in the local role and the MAJCOM as representing central guidance; here we see the MAJCOM in the local role and central guidance generally at the HQ level). However, this discussion also reveals tensions that stem from a lack of cross-functional communication and ongoing horizontal relationships. This is visible in a number of ways—in the lack of shared understanding of how policy is enacted, interpreted, and maintained, in the way managers focus on their local objectives and funding, in the strong local autonomy and great degree of latitude in the way each group chooses to interpret and follow (or not follow) unclear ICT policies and goals.

This discussion reveals many factors that can complicate and distort ICT guidance. These factors include inconsistent assumptions, locally motivated interpretations, misalignment, confusing practices, and considerable leeway for local response. Factors like these need to be addressed through formal mechanisms for cross-boundary communication and interaction. Without clear mechanisms for coordination and communication across both horizontal and vertical organizational boundaries, ICT policy cannot be fully developed nor clearly funded.

3.8 Overcome Funding Disincentives to Working across Organizational Boundaries

As shown in Section 3.7, funding is one of the more visible sources of ICT tensions. As with other ICT-related tensions, funding issues generally represent competing desirable ends. For example, accounting practices, which are driven by the need for fiscal responsibility, call for projects that can be defined, tracked, and managed through a clearly identified owner. However, cross-functional ICT projects and activities often do not have an easily identifiable owner. Nevertheless, funding is often used to identify ownership of ICT projects, even though those projects serve a range of purposes for a wide variety of users and units. "Ownership of systems is driven by resources as opposed to day-to-day operations" (375th AW/ CG).

Unfortunately, identifying complex ICT projects on the basis of narrower funding practices can lead to a piecemeal view of these highly interdependent systems. During Y2K this piecemeal view added to the complexity of tackling a problem that existed not only within functional and hierarchical units but also across those units. Since funding is usually attached to functional activities, there generally are clearly identified owners of the functional nodes of an enterprise-wide ICT system. Y2K was a reminder that problems also occur along the links between these nodes and that it is far less clear who owns and is responsible for those links. This uncertainty contributed to the complexity of addressing the Y2K problem and continues to complicate numerous aspects of ICT management.

In addition to this central perspective, funding issues also complicated the Y2K effort at the local level. "The functional users' imperative was to make sure they got their functional changes in, and they sometimes saw Y2K as an annoyance or as an absolute roadblock to being able to do their job. The functional users…had to pay for the work being done, so in many cases they saw Y2K as siphoning off funds to fix problems that the…[technology] world created and that weren't going to help them in the long run… this problem [may] still exist today" (MSG).

In this example, competing demands for funds exacerbated the tension between local users and central ICT managers. Local users did not readily see Y2K as directly linked to their functional mission. Even worse, following central Y2K guidance would shift resources away from those missions. Organizations need to bridge the gaps between central efforts to achieve technology consistency and local efforts to use information for specific purposes. Unfortunately during Y2K, local funding issues served to widen these gaps.

Additional complications can occur when ICT funding practices are not uniform across the organization. Many Air Force units "are funded to do their business over and over again," whether or not they can demonstrate improvement, "but that's not true for the whole Air Force. I'm in an organization that puts out a profit and loss statement every single year. That impacts whether we're going to have some people working next year or not" (AMC/SCA). Distinct differences exist between those parts of the Air Force that operate on a fee-for-service basis and those that do not, and these differences can complicate efforts to achieve consistency of ICT management.

Perhaps the biggest funding lesson of Y2K, however, can be seen in how this issue was able to attract sufficient attention, critical organizational mass, and significant funding such that, although it was temporary, it was tied specifically to addressing an enterprise-wide ICT issue. In this sense, Y2K set a precedent in ICT funding. When it ended, many who had been involved were concerned that since Y2K turned out not to have as great a negative impact as anticipated, it could be more difficult to get the senior levels to recognize and fund other large, cross-functional problems such as critical infrastructure protection (CIP) (AF/XOIWD). (Of course, the subsequent events of September 11 have eliminated any concern in this area.)

Whether or not there were negative impacts from the perception that Y2K was benign, the experience of having gained such a high level of public and political visibility, and the funding that went with this visibility, left a strong impression on many ICT leaders. They realized that in order for other broad ICT efforts to be successful, a very high level of leadership, support, and funding was necessary. "The real lesson of Y2K was gaining a very high level of visibility, support, and, ultimately, funding" (AMC/SCA).

3.9 Clarify the Appropriate Level of Central Guidance and the Role of Central Administrators

While funding issues tend to be visible, other, less visible issues can be equally critical to effective ICT management. One such issue is the need to gear central ICT guidance to an appropriate level: if too high, there may be a disconnect with local execution; if too low, local executors may be overburdened and have little room to adjust for individual circumstances. During Y2K, the subtleties involved in gearing central guidance to an appropriate level were further complicated by the increased involvement in ICT decision making of higher-level administrators with little or no ICT management experience.

Once the focus of Y2K efforts moved beyond technical performance to the ability to complete missions, higher levels of review were seen as necessary. This

increase in levels of review and approval could be dramatic, often involving high-ranking officers with experience and responsibility in operational, rather than infrastructure, areas. "For all…major systems and some…characterized as fairly minor, the review process for certification got to a very high level. … the norm being 5-7 levels of review on every change with final approval by an O9 (lieutenant general)" (AMC/SCA).

Despite the increased burden and opportunity costs associated with higher-level review, many ICT managers saw this growing awareness and involvement of upper management in ICT decision making as positive, overall, and an indication that the Air Force view of information technology (IT) had matured (375th AW/CG). These managers knew that Y2K was not their only cross-boundary ICT effort and that other ICT initiatives (such as DMS) required them to address issues that extended beyond their ability to control. To these managers, an increased involvement of upper-level administrators in ICT management meant an increased focus on cross-boundary and organizational goals rather than technical objectives.

Before Y2K, system problems were in the domain of system or program managers and generally stayed there. But because of the importance of identifying and resolving mission-related problems, the imperative with Y2K was to involve upper management. "And since top levels of management are the ones primarily concerned with customer satisfaction, …the service organizations had to be more sensitive to satisfying their customers and assuring that the senior management of those organizations was able to address customer concerns" (MSG). In this way, Y2K helped stimulate not only the awareness of upper management to the importance of ICT but also the integration of ICT goals with organizational goals.

While these potential benefits are critically important, other managers viewed Y2K as demonstrating that at the tactical level, the impact of higher-level administrative scrutiny could be burdensome. "In one extreme case, our developers had to add a carriage return to one line of code on a [certified] program that had about 500,000 lines of code in it. And we went through that entire [recertification] process. We did Y2K testing and had it independently verified, all the way up to the O9 [level] to get approval for that release. And that's a lot of work" (AMC/SCA).

These managers expressed concern that the higher level of scrutiny during Y2K would be extended into other ICT areas. In the Air Force, good leadership generally means pushing decisions down to the lowest level possible and delegating responsibility. Many managers felt critical concerns such as systems breaking networks and programs spamming a network could be handled at functional levels. "Senior-level review of all the changes to every system is not efficient problem solving" (AMC/SCA).

Central management of ongoing ICT practice is a highly problematic activity. The layers of review and approval needed to achieve such control are extremely resource intensive, and the benefit from this additional review is often unclear. For instance, based on the success of Y2K, AMC/SCA felt pressure to carry forward a procedure much like that proposed for Y2K; that is, a higher-level organization would review their configuration charts. In this case, decisions normally made by an Air Force captain would be made by a brigadier general, including all the layers needed to staff the effort.

According to personnel at one AMC/SCA: "We had no history…of…having fielded something that broke the defensive transportation system or caused an interface problem with anything…in TRANSCOM. So…what is the value added?"

Generally, the demands of ICT management do not require tactically specific central orders, but during Y2K there were times when the increased central control manifested itself in specific, relatively low-level guidance that could leave little room for individual adjustment to local conditions. For example, as the new millennium approached, central guidance called for a demonstration of mission readiness by putting planes in the air across the New Year time boundary. "Directions came down from MAJCOM that they wanted all planes up at 00:01. Local folks here said they wouldn't do it because all their flying is done with handheld GPS systems" (374th AW/CG). In this case, the local environment did not support the centrally defined tactics.

What were the higher organizational goals behind the guidance calling for planes to be in the air during the century change? Could this guidance have been geared to a level that allowed individual bases to meet this higher goal using more individualized tactics? Whatever the answers to these questions, the Y2K experience demonstrated that effective central guidance on a cross-organizational ICT problem could not be focused on a blanket policy covering individualized technical issues. Instead, central ICT management needs to focus primarily on common information strategies and their alignment with organizational missions.

Beyond Y2K there are numerous other ongoing cross-organizational ICT problems that need this level of central attention. "I would love to see greater senior-level involvement, not trying to solve the individual problem, but taking on the basic problem as a whole. For instance, if…[the Air Force is] serious and really want[s] to operate on a common backbone as a weapons system, then let's do it reliably. We haven't gotten very good at it" (AMC/SCA). Nevertheless, this central focus must be balanced by the awareness that central guidance is limited in managing a distributed, individualized ICT system. Those who oversaw the Air Force Y2K effort came to understand that the lessons of Y2K could be realized only through the combined actions of empowered local organizations.

> Don't rely on headquarters to tell you what to do or how to do it with regard to the Y2K experience. There are too many things that each individual organization has learned that could benefit you in your own situation. … You're the ones who know how to do your jobs. You're the ones who know where the needs are. You're also the ones who are going to be responsible for funding those changes in the way you do business. I can only think that is the proper approach. (AFCIO/AFY2KO)

Thus, central guidance needs to strike an appropriate balance between generating and maintaining an enterprise-wide information strategy and fostering individualized local execution of that strategy.

3.10 Address Cross-Boundary Issues in Life-Cycle Management of Systems

The need to balance enterprise-wide information strategies with individualized local execution is particularly evident in life-cycle management of systems and software. During Y2K there was a heightened awareness (even within upper administration) of the need to know that systems were okay (testing and certification), that systems were current

(version control), and how a given subsystem fit into the larger system picture (configuration management, or at least an area that configuration management should include but often does not). In raising awareness of the importance of these ongoing life-cycle management concerns, the Y2K experience also helped emphasize the importance of addressing cross-boundary organizational issues in these areas.

3.10.1 Certification and Testing

Y2K provided a strong incentive to take control of the myriad ICT systems that proliferate over time throughout a technology-dependent organization. The Y2K response effort involved a wide range of tasks that were generally organized into a five-phase program: (1) awareness, (2) assessment, (3) renovation, (4) validation, and (5) implementation. As this effort progressed, the validation phase loomed as increasingly daunting.

> Once systems have been renovated, testing in a controlled environment is required prior to placing them into operation. The reader should be aware [that] testing and validation is projected to be a time-consuming and extremely expensive phase in the resolution process. The Gartner Group estimates testing and validation will encompass 40 percent of the total Year 2000 effort for most organizations. Through the years, testing has often been looked at as an area where money and time could be saved. To do so with Year 2000 testing may make for a very unhappy New Year's Day in 2000. (USAF 1997)

Despite the perceived importance and magnitude of the validation phase, the complexity of testing and diversity of local conditions made it difficult to generate specific central guidance on validation.

> Most organizations will already have a validation process in place for ensuring [that] systems operate as designed prior to being placed in production. As a result, little guidance will be given in this area other than recommending [that] each organization closely evaluate test beds and processes to ensure [that] the infrastructure exists to test systems on a large scale. (USAF 1997)

Much of the difficulty of Y2K testing was tied to the complexity of the ICT systems themselves, particularly the interdependent nature of components and subsystems. In its November 1998 testing guide, the General Accounting Office (GAO) outlined four types of validation testing:

1. *Software unit testing* to "verify that the smallest defined module of software ([namely], individual subprograms, subroutines, or procedures) work as intended."
2. *Software integration testing* to "verify that units of software, when combined, work together as intended."
3. *System acceptance testing* to "verify that the complete system ([that is], the full complement of application software running on the target hardware and systems software infrastructure) satisfies specified requirements (functional, performance, and security) and is acceptable to end users."

4. *End-to-end testing* to "verify that a defined set of interrelated systems, which collectively support an organizational core business area or function, interoperate as intended in an operational environment (either actual or simulated)." (GAO 1998c)

These four test types run the gamut from the workings of an individual, isolated component to the intricacies of a full-blown, cross-functional, cross-organizational mission thread. Thoroughly covering this wide range of tests was extremely difficult, particularly in the relatively short time available.

To facilitate this daunting task, most organizations, including the Air Force, turned first to the use of testing tools. These tools existed primarily at the unit testing level, generally scanning code to identify problematic occurrences of date formats and date-based calculations. Even at this level, these tools required significant human analysis. "We code scan … it pops up thousands of instances … then it's necessary to eyeball and go through and pick out things" (MITRE). In addition, the tools lacked the specialized knowledge about particular systems and environments that was needed to augment tool-based testing. "A commercial vendor is selling the silver bullet Y2K fix. The reality is he's going to find a few real issues, but very often he's going to raise more questions than he's going to solve. …For example, we used windowing[3] [to fix dates] but the testing software, rightly, would say 'You've got a two digit year here.' Well we knew that" (AMC/SCA).

The use of code-scanning tools revealed not only disconnects between Air Force units and their vendors but also disconnects among Air Force units themselves. When these tools were employed at Air Force central ICT facilities, the need for specialized system knowledge was demonstrated again.

> SSG tested our software for Y2K issues and … they did find some. But they needed to know more about the program. So that required further resources on our part to help them in order to get it to run [and] to make sure they knew what they were looking at. In some cases they would say "you have these issues" but when we looked, it wasn't really a problem. (AMC/SCA)

In addition to specialized system knowledge, the use of code-scanning tools needed to incorporate the environment in which the code operated and its interdependencies with other systems. Without these, Y2K certification based on these tools was highly problematic: "We didn't trust ESC's (Electronic Systems Center's) certification. AMC looked at certification from a systems view" (AMC/SCP).

Given the short time frame, the limitations of unit testing, and the complexities of integration and acceptance testing (for example, How do you measure whether systems are acceptable to end users?), attention soon shifted to the opposite end of the testing spectrum—end-to-end testing. This was an extremely involved effort requiring the coordinated interaction of a wide range of people across various inter- and intraorganizational boundaries. In particular, "GAO's Year 2000 guidance recommends that in planning and managing end-to-end tests,

[3] A technique for converting two-digit dates to four-digit dates without explicitly changing the date format.

agencies define test boundaries, secure the commitment of data exchange partners, prepare test procedures and data, define exit criteria, and document test results, among other steps…" (GAO 1999).

Not surprisingly, the required interaction among professionals from across organizational boundaries was difficult and produced its share of surprises. "Designing…end-to-end testing became a very excruciating process of sitting down with a lot of people. And even…[with] the experts in the room, literally just before…test…[kickoff]," someone would discover that the system worked differently. As a result, the tests had to be reconfigured (MSG).

Nevertheless, end-to-end testing was the most direct way to address the basic issue; namely, could technology-dependent critical missions be carried out after the change of century? To coordinate across the Air Force and with other military branches, a cross-organizational Y2K entity had to be established—the Air Force Year 2000 Office (AFY2KO) (see Section 3.13). As the century change approached, considerable confidence was gained through the activities of this coordinating entity and the shift of focus to end-to-end testing. Nevertheless, as the deadline approached, there always seemed to be more to do.

> Overall end-to-end test efforts within three of the four functional areas were reported to be largely on schedule and expected to be completed by October 1999; however, at the time GAO briefed the Communications functional area on the results of GAO's review, it could not provide complete progress information; and while information was subsequently provided by Communications, it showed that the functional area had not yet developed plans to test 31 mission-critical systems. (GAO 1999)

Testing and certification were two of a number of software life-cycle management activities that became increasingly centralized during Y2K. Coding, testing, distribution, and support functions were moved from the program offices into a so-called software factory, which included the Communications Environment Test Laboratory (CETL). "Code that is released goes through a test process before it is certified. …One of the major benefits of Y2K was that we built up the CETL" (SSG).

A risk of centralized testing and certification is that it may not adequately account for the impact of diverse operating environments—a risk exacerbated by the fact that system components do not operate in isolation. To address this risk, CETL began testing in a laboratory network environment instead of testing the software solely for functionality. For this testing, software is run against other programs, across routers, and through firewalls. Testing scenarios cannot duplicate all possible cases, but CETL activities were fairly comprehensive (SSG).

Some ICT managers see the increased focus on centralized testing and certification that came out of Y2K as positive, and they want to build on it. For instance, the Standard Systems Group (SSG) envisions that the CETL testing will evolve first into a certificate of net worthiness and then into a new "certificate to operate" that would be granted by the MAJCOM. "No software will be allowed on ACC bases without the ACC certificate to operate. AMC promises to do that, and we hope that all the rest will do that as well" (SSG).

While some ICT managers are attracted to the idea of certification of worthiness for systems and acceptable operating conditions, others are less sure about this trend toward higher-level, centralized certification. They worry that an expansion of the Y2K certification philosophy means that the level of authority making decisions will be higher than pre-Y2K, when the different levels within the configuration control boards addressed different problems. With certification, "you need to set up some threshold or criteria to escalate the level of leadership. Changing the screen from blue to green will require an O7's (brigadier general) review. In the past there was no certification…" (AMC/SCA).

As with other areas of ICT management, numerous perspectives on ICT testing and certification need to be balanced. For example:

> The only good part of negotiating with the MAJCOM for a certificate to operate is [that it is]… subject to a very high level of scrutiny, testing, and verification. We still use the IV&V [Independent Validation and Verification] tools; the code scanning is still part of the process; and the certificate to operate puts everything out in the open and makes everything very controlled. The problem is…bureaucracy and paperwork. …FTP [file transfer protocol] is a problem for some programs because we can't verify secured channels. FTP is required for remote administration, and that probably results in…having to get waivers to a certificate to operate. (SSG)

> [At]…Scott Air Force base…USTRANSCOM has their own network because they could not [operate]… the DTS (Defense Travel System) under Air Force rules. And the certificate of net worthiness, certificate to operate, and so on just exacerbates that problem further. So they…got their own network…separate from the base. To send e-mail from them to us, we go outside the base…and come right back on, even though it is just across the street. (AFCA)

> From the base level, we…like [the] process of getting the MAJCOM certification…because…we also have to task out the users who are complaining that they've already got too much to do. …[So] it helps a lot to move that to the MAJCOM level. (374th AW/CS)

> From my perspective, the big problem comes when either operational need or some external force drives you—maybe the aircraft industry or FAA wants things done differently. We now suddenly have to get…[a lot] of other people to agree, and… it takes months [to reach agreement], even if it's a waiver. …We find that they're not binding…a MAJCOM will say, "Here's what it is." Then you'll get to some base and they'll say, "No, we're not the same thing at all." So you can't install. (AMC/SCA)

> Too many folks…have to "bless" the software before its release. AMC and GATES (Global Air Transportation Execution System) have about 150 geographical sites with hardware and software. Does a change require all sites to agree? We'll never lose local authority. (AMC/SCA)

Like many other issues raised by Y2K, the topic of certification and testing likewise calls for ongoing organizational mechanisms that support cross-boundary communication and coordination.

Certification and testing issues are also tied to issues of acceptable ICT risk and appropriate response, which are discussed in Chapter 5.

3.10.2 Version Control and Configuration Management

Not only did the massive effort to assure that systems were Y2K certified increase an organization's focus on testing and certification, it also increased its awareness of the need to track which versions of software and configurations of components were currently in use. Software fixes and system certification would mean little if the approved software and configurations were not actually implemented. Under this increased scrutiny, numerous difficulties were revealed in the mechanisms for tracking and controlling software versions and system configurations. For example, when systems had been Y2K certified and fielded, but were not yet installed everywhere, confusion and problems occurred during audits, configuration assurance, and so on (AMC HQ), and the only way to verify whether people were using patches was to receive verbal confirmation (375th AW/ CG).

While these difficulties were particularly visible during Y2K, they are an issue for ongoing ICT management.

> We send things out with certain configurations, and when we distribute them to the units, we don't know if they are loaded or not. So we need to do a lot more work in terms of assuring that configuration is managed right down to the end site. Version control is part of our major business function, so Y2K probably didn't change us that much, though it did allow us to identify some issues and problems. Some of the resources allowed us to get better and build capacity. (SSG)

As with certification and testing, the increased focus during Y2K on version control and configuration management contributed to an increased effort to centralize these activities. One approach was to work toward a single, electronically based distribution mechanism: for instance, access to the latest software versions from a web page (passive) or electronically distributed (active).

> We've set up a single point source for distribution. So if you want the latest version, you go to the [web] page. That's where all the latest versions are. (SSG)

> We are responsible for version control. We used to send out a live person to do this; now we are trying to push it all out electronically. (AMC/SCA)

The effort to centrally track and electronically manage software and system configuration is complicated by an extremely diverse and hectic environment of system change. Some of the factors that contributed to this diverse change environment included the many types of changes that were occurring (for example, Y2K fixes, security patches, new software releases, user-requested changes), the high rate of change, the variety of ways in which these changes occurred, the variety of units involved, and the variety of roles these units played. Both local and central units saw difficulties in this diversity.

> Y2K is a symptom of configuration management. There are too many hands in the pot. (374th AW/CS)

> Updates happen different ways: at log on, posted at a website, some are done by a team of guys who go out to each base. Nobody and everybody owns it. (AFY2KO)

Change management at the local level could border on the chaotic. "Specific groups were responsible for specific programs, and they had to make sure that patches were loaded. In one case, Logistics didn't load a patch. …The functional versus operational chain of command had issued conflicting instructions. Operational commanders aren't aware of SSG tasking…so they won't enforce it" (374th AW/XP).

Central units could be equally frustrated, which often led to tensions between central guidance and local execution. In some cases "there were complications in the extension configuration management…some folks having six configuration messages each week, and others having only two. Basically, it's a struggle between local autonomy and central management. We're looking for 'positive' control with configuration management" (AMC/HQ). In another case, "MSG knew the configuration of its application software but did not necessarily know the configuration of the mainframe that ran that software, as well as all the other software in those domains. … So there was not one big picture…and we found…domains [that] were configured differently because there were different applications running…depending on who the customer was and who they were serving" (MSG).

Since change management is an ongoing issue, the situation was further complicated by related problems that extended beyond Y2K. For example, AFCA saw configuration management of COTS infrastructure to be something the Air Force was either willfully behind on or not focusing on well. However, "with the Nortel switch, fiasco configuration management came to the forefront for many senior leaders because [it] caused people to have to backtrack up to two years into configurations and pay for it" (AFCA). In another case, the Cargo Movement Operation System (CMOS) was a problem for SSG because multiple versions were not being completely installed and the program office was releasing patches off their own web page, which was not known to the version control staff.

As we have seen in many other areas, often the tensions between central guidance and local implementation can be traced to differences in perspective that need to be continuously balanced. From a central perspective, the key issue during Y2K was assuring that local installations were using the approved, Y2K-compliant release or configuration. However, local users were far more focused on completing their many functional and strategic projects, not on whether they had the approved version or configuration. End users wanted change to be as quick and smooth as possible. They wanted to continue to use their software and systems in the manner to which they had become accustomed. In short, ICT was there to facilitate their tasks, not to replace them as the central focus.

An approach to managing change control that potentially benefits both local and central units is to reduce the hectic and unpredictable pace of change. One way to accomplish this is to hold changes for a set release date, that is, to block release. "With block releases we would have once-a-month releases where everything gets approved, certified, …tested and goes out in a single release package from SSG. That… would fix a lot of the version control problems…" (SSG).

During Y2K there was the additional pressure of assuring that the great pace of change did not inadvertently undo already completed Y2K fixes or introduce new Y2K-related problems. Therefore, central Y2K managers went a step beyond block release and instituted a freeze during the latter half of 1999 and into 2000. This meant that once systems were declared Y2K compliant, additional changes before the century rollover required considerable justification and additional layers of approval. This increased level of oversight considerably slowed the pace of change. For instance, before Y2K, AMC/SCA "averaged more than one software release per week on an AMC critical command control system. …[With the freeze, the average decreased to] less than one change every three to four months."

The high level of review that accompanied the freeze frustrated many software managers.

> Some oversight is good, but it should be at the Program Manager level, not at TRANSCOM or in D.C. We probably would have made 2 new version releases by now. We won't submit the paperwork for certification because it wouldn't get through until March, which is when the freeze is going to be over anyway. (AMC/SCP)

These managers viewed the high degree of change as being responsive to user and system needs. Some predicted that putting off these changes would result in future difficulties.

> The impact of a slowdown in software releases is a backlog of changes. … And as they are delayed, the changes become larger, which in turn increases the risk we're going to have problems with the changes. We're trying to field these things all around the globe. It's not easy to do. So that creates greater integration issues. That impacts life-cycle management. (AMC/SCA)

These predicted difficulties apparently did not materialize, however.

> In terms of the configuration and certification freeze that was in effect from November through March 15, that bothered all the program offices—that put them off schedule. We were worried that on March 16 all of these programs were going to be dumped on the field and we were going to have a huge support tail. And it turns out that hasn't been a problem. (SSG)

Perhaps slowing the pace of change means that new versions and patches are more thoroughly tested. Or perhaps all this change is not so clearly beneficial to users. Perhaps the drive to stay current with technology through constant change is driven more by the ICT industry and central ICT managers than by obvious benefits to local operations and users. Whatever the reasons, the Y2K experience emphasized the need to balance the many competing perspectives on ICT life-cycle management issues—for instance, version control, certification, documentation—as well as increasing the focus on these activities (SSG, 374th AW/XP).

Change management activities also have a clear impact on such issues as security, critical infrastructure protection, and information assurance (which are discussed in further detail in Chapter 4).

3.11 Tackle the Huge Informational Effort Needed to Support Management of Integrated Systems

Another key set of issues—related to change management and highlighted by Y2K—was the difficulties faced by people attempting to acquire and maintain necessary information about the organization's ICT systems and information environments. It is difficult to manage, protect, or fix a system when its components and configuration are not clear. At the outset of Y2K, as organizations decided they were facing a widespread, generic threat, their first impulse was to inventory what was in place, who was responsible for it, and whether there was a problem that needed to be addressed.
Seemingly basic information, such as the state of the installed equipment base and how it is used, was not readily available nor being constantly maintained.

Unfortunately, in a large, complex, and diverse organization, it is extremely costly and time-consuming to meet comprehensive ICT informational needs—so much so that these activities are often limited to local databases for local purposes. Maintaining the big picture is an extremely difficult task complicated by rapid change (for example, constant upgrades from the highly dynamic ICT industry, often exacerbated by an organizational focus on staying abreast of the latest technology) and distributed ownership.

> The big hang up is that data go out of date very quickly. Since the Y2K rollover, I haven't made one update to the [comprehensive inventory], and we were making them on a daily and weekly basis in many cases. The data are already starting to get out of date. (AMC HQ)

> Since we've gone to a distributed client server environment and everybody at every base can run their own systems, they dropped a centralized inventory and it just wasn't tracked any more. (SSG)

Y2K provided the incentive to tackle a huge ICT information inventory, and considerable ICT information with potential long-term value was generated. Air Force efforts initially focused on two comprehensive databases: the Air Force All Systems Inventory (AFASI) and the Air Force Evaluation Database (AFED). Later, in support of "mission thread" tests, these databases were augmented to capture how the various systems worked together to accomplish operational tasks.

From many different perspectives, the huge Y2K informational effort was seen as capturing critical information that met several ongoing ICT management needs. Specifically, those needs were: (1) understanding the relationship among systems (AMC HQ); (2) building a permanent operations reporting status for information systems (SSG); (3) knowing the infrastructure and how to work with it (AFCA); and (4) generating a cross-functional inventory and incorporating all the inventories onto one spreadsheet (375^{th} AW/CG). Many people thought this effort should be maintained beyond Y2K.

The pressures of the Y2K threat, however, coupled with ongoing operational demands, left little time or energy for leveraging this effort into an ongoing means of addressing comprehensive ICT informational needs. "The databases could possibly be used for version control, configuration management, and information assurance, but…[staff]…don't have time to keep it maintained" (AFCA). In addition, "the level of information exchange will go away. …There will only remain documents documenting

the details of the process. Motivating causes will not be recorded, because there's no time to do so" (USFJ).

In addition to basic time pressures, the Y2K informational effort remained focused on short-term benefits because of numerous other difficulties and barriers that further complicated such a large job. One issue was clearly establishing the usefulness of the collected information and incorporating that usefulness into ongoing activities. Thus, to ensure that the data are maintained accurately, the organization must provide an incentive to the owners of the data.

> Having data collection is great, but if we don't have something useful to do with the data, we are never going to get people to keep them updated. We proved this during Y2K—asking people to gather information for information's' sake is a waste of time and effort. (AMC HQ)

Other complications were related to the lack of organizational homes, operational structures, and ongoing funding in support of a comprehensive ICT information effort. Over time, without a structure in place, much of the information becomes out of date or is lost (AMC HQ). Some people see critical infrastructure protection and information assurance activities as the natural homes for these informational efforts (see further discussion in Chapter 4). As with many ICT issues, however, no single, natural home covers all aspects of the situation, and funding cross-functional resources remains an issue.

> I have tried to look for a home for AFED. Do you guys want it? (AFCA)
> Somebody needs it. Actually I would argue that AFCIC/SY needs it more than anybody else. If the CIP program is not going to take ownership of it, we'll figure out something. (AF/XOIWD)
>
> We're using AFASI right now. I just used it yesterday. And actually AFASI and AFED probably need to be used together. (AFCIC/SY)
>
> If you want to get to the mission tasks and war fighter needs, the AFED starts to map that out. (AF/XOIWD)
>
> Yes, we probably need to get that. …Sometimes I wonder why the XO hasn't stepped up here. (AFCIC/SY)
>
> I agree… this needs to be an operational concern as opposed to a COM community concern. … The problem is it's a resource-intensive activity to do properly, and no one has got the resources committed to it like we did with Y2K. (AF/XOIWD)

Despite the generally perceived value of ICT information, without clear organizational homes, accepted information structures, and dedicated resources, it was difficult to maintain a coherent, comprehensive data-gathering effort following Y2K.

Another important challenge to Y2K, or any large informational effort, is maintaining consistency in data-reporting practices. One of the Y2K problems was inconsistent terminology across the numerous units and users. "Systems were identified in a variety of pet names, acronyms, codes, verbal descriptions. …The Fusion Center… had as much work identifying [information on] tickets as … taking the tickets and following up on them" (SSG). In addition, "the [inventory] databases were hard to manage with multiple users [because] the inputs were too variable" (AFCA).

Technology issues also affected the consistency of data-gathering practices. During Y2K, bases lacked the software other organizations used to gather data; the AFASI interface was difficult to use, which resulted in inaccurate data; the functional managers experienced problems in accessing the database; and the capacity problems in Excel were not anticipated (AFCA).

Equally critical were issues of organizational politics and information control that led to inconsistencies in the execution of data-gathering plans. For instance, 130 people from different communities developed a plan for reporting Y2K information to the Fusion Center. They used large group process techniques to create an acceptable reporting structure and vetted the plan across various other groups and organizations—some liked it and some did not. One MAJCOM "told its world, 'Don't report directly to the Fusion Center. Report to us. We'll massage the information and give it to the Fusion Center'" (SSG).

Geographical and cultural differences, especially between CONUS and OCONUS bases, could also impact the consistency of information-gathering efforts. OCONUS bases were required to go through the State Department—specifically, the embassies—to obtain information from host governments. The information received from these sources was much different from the information received from stateside sources. Other information originated from intelligence and similar networks that pooled information (374th AW/CS).

The barriers to effective data gathering were not limited to the Y2K effort; they continue to complicate ICT informational activities to the present. Despite these challenges (including additional information security issues discussed in Chapter 4), this huge and complex effort is necessary to support effective high-level ICT management. The Y2K exercise gave the Air Force a much-improved grasp of the systems it has, the purpose and functions of those systems, and the systems and organizations with which they interface. The next step is to develop processes and procedures that maintain that data and use them constructively (AMC HQ). To do this, organizations need to give information issues a proper home (see Section 3.13), sufficient priority and organizational visibility, and adequate resources. Continuity over information inventories developed during Y2K must be retained (AFCIO/AFY2KO). Over time, organizations need to make information gathering and maintenance part of their ongoing communication culture.

3.12 Address Issues of Organizational Culture

Beyond technology that is well designed and appropriately used; beyond data that are current, relevant, and readily manipulated; even beyond information that is alive and useful, there is communication among people and the culture within which that communication occurs. Information is not neutral. Existing relationships with an information source, for example, can mean more than the specific message content. In the Air Force, receiving information from one organization rather than another (for instance, OPS [operations] versus COMS [commands]) can determine whether the issue is dealt with by the base or delegated to one functional group (374th AW/XP).

Similarly, existing informal patterns of interaction can mean more than formal plans of operation. While formal communication plans were in place, verbal agreements among the program offices assured them that if a critical Y2K failure occurred, everyone would "get a call" (MSG). Because of its pervasive effect on how people perceive and practice communication, organizational culture impacts all aspects of ICT management, from specific tactics to overall strategies.

Y2K was neither the first nor the last ICT project in which cultural issues played a central role. This is generally the case for any major, cross-organizational change in ICT such as occurs during mergers or strategic realignments. In 1995, when changes in the economics of health care forced Johnson & Johnson to move toward a more integrated delivery system involving doctors, hospitals, patients, and insurance companies, the president of their customer support center found himself in a countercultural effort: "Johnson & Johnson has over 100 years of history authorizing operating companies to manage all business facets to maximize their brands' [profits and losses]. …We are learning how difficult it is to break those paradigms and work together to leverage the strength of the firm with larger retail customers" (Weill and Broadbent 1998).

The Air Force, too, has a long history of functional autonomy, and Y2K similarly brought out the need to break down cultural barriers, to balance differences, and to work together while maintaining the benefits of that autonomy.

> There has been a tug of war between the network view and the systems view. Y2K taught us that both are good. … The AF needs to continue to have folks be cross-functionally focused while maintaining stovepipe functionality. (375th AW/SC)

Some cultural traits are generally pervasive throughout an entire organization. The Air Force, for example, has a common "culture of perfection" that impacted the organization's tolerance for risk during Y2K (see Chapter 4). Most cultural issues, however, involve differences among organizational subcultures, for instance, those that are information or commission driven (AMC) versus those that are not (ACC); those focused on system capabilities and performance (acquisitions) versus those focused on compliance and version change issues (computing operations). These subculture differences were especially visible during Y2K.

Perhaps the most visible cultural differences during Y2K were those between acquisitions and computing. Even at the top level of management, the Air Force Y2K effort was split between these two perspectives. The Air Force Chief Information Officer (CIO) came from acquisitions (SAF/AQ), while the deputy CIO came from computing and communications (HQ/SC). Within these two areas, units that were particularly active in providing Y2K leadership included, on the acquisitions side, the Standard Systems Group (SSG) and the Material Systems Group (MSG) and, on the computing side, the Air Force Communications Agency (AFCA) and the Air Force Communications and Information Center (AFCIC).

On the one hand, the acquisitions culture fostered a more hierarchical approach to Y2K. Those with an acquisitions orientation focused on centrally administered correction and testing of large systems acquired and maintained through contractual agreements. As discussed in Section 3.10.1, they saw Y2K as a demonstration of the need for more uniform, centralized software development and testing. The key to this was an increased emphasis on contractually based ICT management. On the other hand,

the computing culture fostered a more distributed response to Y2K, with local SC units working at each base. The emphasis was more on networking and managing nodes of activity focused on local, ongoing operational and maintenance issues. During Y2K, SC provided leadership and support to the various Y2K working groups that tackled the frontline efforts at bases and facilities across the service. Counter to the acquisitions' perspective, those with a more computing perspective saw Y2K as a demonstration that central developers often fail to adequately consider the realities of local conditions and ongoing operational and maintenance issues (374th AW/XP, AFY2KO).

Different perspectives, combined with the complexities of ICT systems, led to some confusion during Y2K over ownership of systems, responsibility for assuring compliance, and guidance on how to achieve it. However, it is neither surprising nor disturbing to discover that SSG primarily saw Y2K as an Air Force–wide acquisitions and fielding problem, while SC units primarily saw Y2K as a functional, operational support and maintenance problem. Each of these activities is highly complex and equally critical, yet each is fundamentally different. Even when acquisition decisions do consider maintenance, it is only one of a large set of other equally compelling issues (for example, cost, platform, function, training, scheduling, past performance, existing agreements, future acquisition plans). This is very different from the ongoing activity of maintaining systems under local conditions and needs with dynamic operational demands. In the current operational and organizational environment, acquisitions and computing could not be accomplished without the distinct cultural mechanisms that each activity has developed to support their differing relationships and practices.

Nevertheless, acquisitions and operational support and maintenance are interrelated ICT management activities. Central acquisitions decisions impact the operational support effort, and the operational support situation impacts acquisition decisions. These activities need to be integrated, and for this to occur, bridges must be built between the two cultures that support them. It is critical that there be formal organizational mechanisms for supporting communication across these cultures, as well as regular occasions for that communication to occur. (For more discussion on this, see Section 3.13.)

Other cultural differences also surfaced during Y2K. Users have their own culture, too, which is different from that of either system developers or computing support personnel. An analysis of user needs and environments is a complex activity, generally associated with the design phases of software and other information products. Although a detailed analysis of Air Force system users is not within the scope of this report, it is important to note that user backgrounds, purposes, perspectives, and environments differ from those who acquire, develop, or support the systems. Unique relationships and practices lead to a distinct user culture, and this can contribute to tensions that make it difficult to work with other interrelated activities, such as acquisitions and support.

For instance, what works for system developers in the development stages does not necessarily work for users in day-to-day operations. "From the 600,000-foot view, C2IPS works. But in the trenches it doesn't work. The real test is day-to-day operations. It takes a while to make a system run consistently" (374th AW/OG). While users can see developers and high-level managers as out of touch with the realities of frontline system operations, developers and system maintainers can see users as untrained and

unpredictable, prone to individualized actions that can defeat carefully conceived central plans (375th NCC).

Some Air Force managers even see conflicts between the culture of technology users and that of government itself as contributing to the tensions they experienced with users.

> Government tends to be very slow and makes it very hard to change direction…yet, the entire information technology field is characterized by very rapid change—change in the technology, change in terms of our users' needs. …Everyone else looks to information technology as a solution to their own internal problems. So they're trying to do more things with information technology. That creates an inevitable conflict because as part of a government bureaucracy we can't always do the things that we would like to do, so we tend to be unresponsive to those users. (MSG)

It is vital to understand and link user culture to the other cultures that impact ICT management activity. Users are not only the system's reason for being but also the first to notice (and are most affected by) ICT problems. For the 375th AW/CG systems, customers find 99 percent of system degradation. During Y2K, for example, users were in a far better position to recognize certain data corruption issues than were developers and others working on the central Y2K effort. AMC/HQ asked its users to monitor any special processing that occurred infrequently to be sure that the results made sense. Only thoughtful and alert users could catch these kinds of data corruption issues early.

As with the acquisitions and computing cultures, the user culture is complex, functionally beneficial, and an inevitable part of ICT use. High-level ICT management needs to balance tensions stemming from cultural differences and to provide bridges across these various interrelated cultures so that users become part of the conversation and part of the solution.

Like cultural differences, geographical differences in both physical and organizational location also impact ICT management. During Y2K these differences were particularly visible between stateside and overseas bases. For OCONUS staff, a major challenge was presented by the cultural differences of the host government: "Too many people wanted to ask too many questions and it damaged relations" (USFJ). In addition, Air Force ICT managers located in non-U.S. environments were generally more concerned about the impact of Y2K on the foreign culture they depended on than on their own ICT systems. Given the extensive DOD, MAJCOM, and system group scrutiny generated by Y2K, OCONUS staff were confident that their own system's potential problems would be identified and fixed. Their concern was focused on the host country's reaction and ability to provide dependable utility support. To that end, they spent 1999 preparing for the worst case (374th AW/CS). "The experience was more challenging because of our unique situation to be dependent on an electrical power source outside of U.S. territory. Your main power source may not be there no matter how prepared your systems are. Host country data/parts were not readily available when needed. The base prepared higher-level contingencies because of these limitations" (374th AW/MDG).

Another geographical factor that impacted ICT management was physical proximity to major organizational units. This impact could be both positive and negative. On the one hand, Air Force units on a base that hosts a MAJCOM headquarters, for instance, increase their likelihood of informal interaction with that unit and, therefore, access to central guidance and related communications. "It was nice to have AMC next door. We looked at reports sent up to the MAJCOM that other folks didn't get to see. We were

guinea pigs for inspectors so they could get a first run-through for inspections" (375th AW/CE). On the other hand, the impact of organizational proximity to major commands could preclude certain activities, such as total blackout tests (375th AW/CG).

Finally, cultural and geographical issues impact ICT management at the highest, most strategic levels. Like Johnson & Johnson, the Air Force had a deep-rooted history of functional autonomy that had to be overcome in order to address the cross-functional aspects of Y2K. Those who went through Y2K, especially from a leadership perspective, were profoundly impacted by this experience. They acknowledged the difficulty in implementing change; however, they also recognized the potential for making a significant difference in the way ICT is managed, and that to do so was their responsibility (AFCIO/AFY2KO).

> It's going to be difficult to change some of the perspectives of the current leadership. … We won't recognize what really happened culturally to us individually and to our organizations. The potential is there for us to do some significant things. But it's going to be incumbent upon those of us who participated in this process to continue to bear the flag. … We're facing a tremendous amount of cultural change in the way we go about tackling problems, and the way we go about finding solutions and executing things is going to change. It changed with the way we dealt with Y2K. (AFCIO/AFY2KO)

At the top level, ICT management is about the space between functional areas. It is about fostering cross-cultural communication and balancing the dynamic tensions that arise across organizational boundaries. It is therefore critical to recognize and address the many organizational subcultures that sustain these various functional homes. To accomplish this, the "space between" requires an organizational home as well.

3.13 Empower Permanent Organizational Entities Focused on Cross-Boundary Issues

Once Y2K was perceived to be a general, widespread threat to ICT infrastructure, many organizations found it necessary to establish temporary organizational entities to spearhead their Y2K response efforts. Efforts to solidify central management of Air Force Y2K activities culminated in the creation of the AFY2KO in mid-1998. This temporary office not only faced a large problem with a short deadline but also came into being at a time when a variety of Y2K activities and levels of management had already existed for several years. Thus, while the AFY2KO was well positioned to provide coherent leadership to culminating activities, such as the final CINC-level assessments of mission threads, there was little time, resources, or incentive for establishing itself as the single POC responsible for providing consistent Y2K guidance across the myriad of Air Force Y2K activities.

Similarly, numerous other organizations established temporary Y2K management entities, such as the President's Council on Year 2000 Conversion and the United Nations' International Y2K Co-operation Center. These entities were created not so much because the problem was large and important, but because existing entities did not encompass the cross-functional, cross-hierarchy, cross-organizational, and cross-system issues involved. During Y2K, temporary organizational entities were used to gain perspective on interdependencies across units and subsystems, as well as to foster

communication where existing channels did not exist or were insufficient. The President's Council, for example, focused much of its energies on leading a series of meetings that brought together key people from various sectors, as well as creating an International Communication Center to gather and distill information on national and international Y2K incidents.

Were such temporary entities filling a need for integration and communication that existed only during the Y2K situation? Based on everything discussed previously in this chapter, the answer is no. The creation of these temporary entities represented a missing element in ongoing ICT management: "There are a large number of IT-related issues that need to be worked similarly to the way we did it in Y2K. … It's been looked at as unique in a number of ways, but it shouldn't be" (AMC HQ).

Organizations already have permanent homes for functional parts of their ICT system of systems; they also need permanent homes for the space between those parts. Complex systems such as ICT are more than the sum of their parts. Partial perspectives are often sufficient for day-to-day operational activities, but as has been shown in this chapter, high-level, strategic ICT management needs to integrate and balance the ongoing, dynamic tensions between the various parts and perspectives. This holistic perspective represents a different kind of knowing than knowledge of the parts. Both are essential to the understanding of a complex system. "More than one way of knowing is possible. …Without the development of an over-all perspective, we remain lost in our individual investigations. Such a perspective is a province of another mode of knowledge, and cannot be achieved in the same way that individual parts are explored. It does not arise out of a linear sum of independent observations" (Ornstein 1975).

Many ICT managers who went through the Y2K experience came to recognize the necessity of permanent organizational entities focused on enterprise-wide, holistic aspects of ICT systems. They saw that the toughest problems occurred not so much within areas under their responsibility but, rather, within areas that cut across those responsibilities. These more holistic problems were not so much about technical issues—they involved integration of and communication across the entire system of systems, that is, the overall infrastructure (AMC/SCA).

> There are a number of areas that are very soft and it would be wonderful if they got a greater emphasis. The programs have their problems, but largely those are being worked. What isn't being worked is the overall infrastructure. (AMC/SCA)

Yet, as difficult as it had been to focus on enterprise-wide ICT management during a crisis situation, managers knew it would be even more difficult to maintain this focus under normal conditions, especially since funding and other mechanisms for institutionalizing change had not been put into place. "Y2K was a hybrid organization and it was set up to run for this period of time. … Now we step forward past the rollover and …[nothing] has changed within our own organization. …Y2K has imploded itself back into the organization…" (AFCIO/AFY2KO).

ICT has become a less visible issue, resulting in a return to business as usual with normal (namely, pre-Y2K) funding. Therefore, mandates to solve information assurance and security problems will not be fulfilled (MITRE). (Of course, the events of 9/11 have changed this.) Because Y2K was not expected to have a long-term effect or enterprise-wide impact on the Air Force, professional financial managers were not brought into the

program. Such a group could have been carried over into a new ICT management environment (AFCIO/AFY2KO).

As Y2K ended with seemingly little long-term impact, ICT managers worried that the critical cross-boundary focus was rapidly being lost. "The enterprise as a whole is not being looked at. We may have management and policy, but strength from an enterprise standpoint is lost. … Momentum… that we gained through Y2K is rapidly falling away—we're losing our opportunity to maintain the enterprise perspective" (AFCIO/AFY2KO).

Even a cursory look at the ongoing state of ICT management leads to the conclusion that organizations should not need a crisis to stimulate cross-enterprise ICT coordination and communication. There are staggering organizational losses every year that can largely be traced to incomplete and ineffective ICT management. Overall, ICT projects have an extremely poor completion and success record. The following describes the situation immediately prior to the Y2K effort (1994/95):

> In the United States, we spend more than $250 billion each year on IT application development of approximately 175,000 projects. The average cost of a development project for a large company is $2,322,000; for a medium company, it is $1,331,000; and for a small company, it is $434,000. A great many of these projects will fail. Software development projects are in chaos, and we can no longer imitate the three monkeys—hear no failures, see no failures, speak no failures.
>
> The Standish Group research shows a staggering 31.1% of projects will be canceled before they ever get completed. Further results indicate 52.7% of projects will cost 189% of their original estimates. The cost of these failures and overruns are just the tip of the proverbial iceberg. The lost opportunity costs are not measurable, but could easily be in the trillions of dollars. ...
>
> Based on this research, The Standish Group estimates that in 1995 American companies and government agencies will spend $81 billion for canceled software projects. These same organizations will pay an additional $59 billion for software projects that will be completed, but will exceed their original time estimates. Risk is always a factor when pushing the technology envelope, but many of these projects were as mundane as a driver's license database, a new accounting package, or an order entry system. (Standish Group 1994)

Since these ongoing estimated losses are comparable to expenditures during Y2K, the need for a central home of ICT management appears not to be limited to times of crisis. Because so many ongoing ICT issues were interwoven with the Y2K effort (for example, version control, certification, system ownership and responsibility, configuration management, system maintenance, continuity planning, security), there was a relatively brief time during Y2K when the AFY2KO became the Air Force's home of enterprise-wide ICT management. As a temporary office, however, the AFY2KO had no mandate for developing and implementing long-term approaches to these ongoing ICT challenges. However, it did recognize the importance and complexity of these evolving issues and that permanent homes were needed for managing them. "We need to find homes for issues like configuration management and certification and version control and we need to put them into policy and procedure" (AFY2KO).

While the AFY2KO and similar Y2K-focused entities have disappeared, there are legacies of Y2K aimed at addressing this ongoing situation. Most significant are the rapid growth of a relatively new corporate position, the Chief Information Officer (CIO), and the creation of an even newer cohort, the Chief Knowledge Officer (CKO). "Agents

of change are…rewiring corporate culture one technology project at a time. These direct descendants of Y2K crisis management teams are more highly disciplined and closely managed than past IT teams. …The CIO has emerged as the driving force behind these collaborative implementations of technology" (McCartney 2001).

While CIOs and CKOs have increasingly been charged with managing an organization's information and knowledge systems, there has been considerable uncertainty as to the exact nature of and appropriate skills for these positions. What is enterprise-wide management of an organization's information and knowledge systems? What does an entity devoted to this activity do?

As with the Air Force, many organizations initially saw the CIO's office as an extension of already influential acquisitions and development functions. This fostered two related perspectives: (1) technology was the central component of an organization's information and knowledge activities, and (2) the CIO's primary role was as owner and manager of that technology. Thus, many CIO offices centered their information and knowledge management activities on standardizing and keeping up with new information and communication technology. This focus was not only aligned with existing ICT units but also was economically beneficial to the many technology companies with products in this area. "Technological perspectives of knowledge management are popular because of the power and resources often held by technology departments. Furthermore, some of the most widely distributed knowledge management periodicals (*KMWorld* and *Inside Knowledge* magazine, for instance) are sponsored almost exclusively by the advertising dollars of technology companies marketing their products" (Wick 2000).

As Y2K demonstrated, enterprise-wide ICT management is not primarily about functionally organized technology. If the CIO owns anything, it is the space between these nodes of responsibility, the conversation and interactions that link the functional parts into a strategic whole. As such, one of the primary activities of the CIO's office must be team building. "It's no longer the case that companies are just forming teams within their own walls. Now they're doing teams across company lines. So you have teams that are cross-organizational, cross-company, cross-culture, cross-hierarchy, cross-technologies, cross-languages, cross-functional—cross-everything" (Jessica Lipnack, quoted in McCartney 2001).

Team building was a critical issue during the Air Force Y2K response effort. In addition to the AFY2KO, Y2K spawned unique working groups at bases across the service. These working groups took cross-functional interaction to a lower level than most workers had ever experienced. The working groups, where the decisions were made, were composed of the organizations' labor forces, which do not usually work with each other. Consequently, people from the various organizations came to recognize that they have a mutual dependency (375th AW/Y2K, 375th AW/CE).

However, team building and coordination are difficult tasks, especially when teams operate out of the normal channels. Many saw these lower-level working groups to be impaired by a lack of leadership and traditional rank. "We had a COMS Tech Sergeant running the [base] Y2K program…not only didn't he have the rank but he didn't have the experience or background of taking all the players on a base and getting them involved" (374th AW/CS). Therefore, "it was… difficult to get [Y2K work group] members involved…the effort's success depends on the level of involvement. It depends on each functional commander's opinion; if they are behind the effort, then there is good

involvement. While the strength of the effort was the cross-functionality, there was no central, formal power behind it" (AMC HQ).

Others gave a far more positive appraisal of the Y2K working groups, though even these people acknowledged the critical role of high-ranking leadership and authority behind the groups. For example, before Y2K it could take up to three weeks for information to be routed up through the wing chain of command. But during Y2K, "the worker bees could take the raw data, streamline it just a little bit, and present it right to the wing commander. And we did that weekly at the stand ups. … I don't think it's something that's ever happened before" (375th AW/Y2K). Perhaps this occurred because "wing commanders were personally called to task for Y2K. …That's why the low-level organizational matrix worked" (375th AW/ CG). For others, cross-functional teams could be advantageous if they had a defined function. It was noticeably effective to have cross-functional problems addressed by people from different parts of an organization (AMC/HQ).

Whatever the success of the Air Force Y2K working groups, cross-functional team building is a complex activity, one where organizational CIOs charged with enterprise-wide ICT management need to play the central leadership role. This, alone, impacts the desired skill set for the CIO position. "Given the high risk for failure of teams, the CIOs who lead [collaborative] groups require business, technology, team-building, project management, and communication skills to be effective" (McCartney 2001).

What else must the CIO do? The CIO needs to distinguish functionally bound ICT issues from enterprise-wide ones. Where the issue resides within a functional responsibility, the role of the CIO is greatly minimized or nonexistent. But the CIO needs to be extremely sensitive to the interdependencies of the overall system. When an error is made, it is likely to be the incorrect assumption that a cross-functional issue is bounded within a particular functional responsibility.

When an ICT issue is identified to be enterprise wide, the CIO must take ownership. While this means assuring that there is a single point of contact providing consistent guidance at the appropriate level, it does not mean the CIO's office should be that POC or should own the problem parts. The CIO owns the space between the parts—the space that makes it a cross-enterprise, strategic issue. In this case, his or her primary role is to identify the relevant organizational perspectives, to determine the best available representatives of those units and perspectives, and then to link, guide, and empower those people and units to manage the issue. Under the CIO's guidance, a cross-boundary entity defined to represent the relevant organizational perspectives on an issue becomes the POC. Only such an entity, acting with the guidance and authority of the CIO's office, can take on the delicate task of balancing the competing organizational goals that surround a cross-boundary ICT issue. The CIO is the fulcrum in this balancing act—team building, facilitating cross-boundary communication and activity, assuring that ICT activities are aligned with organizational goals and strategies, and institutionalizing desired change.

Sometimes, however, the CIO must go beyond the fulcrum role to one of greater authority and stronger leadership. Specifically, during times of critical activity like Y2K or security threats, the CIO may be required to assure speed and flexibility in the face of traditional methods for doing things. "There are bureaucracies that are designed to slow

down decision making and there are places where you want to do that—but in this case [Y2K], because of time urgency, the bureaucracies were either pushed aside or stepped aside and allowed that rapid reaction to take place. And you need to be able to adapt your organization to do some of those things" (MSG).

For an organization such as the Air Force, the CIO would be responsible for assuring whatever ICT flexibility was required for national defense. In addition, the CIO's office should serve as the single point of contact for ICT coordination outside the organization. This was a successful aspect of the AFY2KO effort but may be less clearly achieved in noncrisis cross-service initiatives. For instance, "the Y2K strategy was to develop the relationship with DISA (Defense Information Systems Agency) early on…create a service-level agreement. …We probably worked on that relationship as much as anything else to make things function smoothly. …[However,] DMS is…not being run that way…" (AFCIO/AFY2KO).

Finally, the CIO must foster the use of ICT systems themselves as part of the solution to the problems they generate. These systems are increasingly the primary medium for the cross-boundary conversation and activity the CIO must establish and guide. During Y2K much of the sharing of information among the Air Force, the services, the federal government, and other governments took place over the World Wide Web, which was not business as usual. In the future, "similar approaches will be needed for other equivalent issues" (MITRE). In this vein, the AFCIO/AFY2KO is working with the Air Force Materiel Command to develop a knowledge management website to host the Y2K lessons learned.

Given the ability of modern ICT to empower individual users and groups of users, some wonder whether decentralization is an inevitable feature of ICT activity. They wonder whether we must focus on the strengths of local flexibility to achieve our goals, even under crisis conditions. For instance, IT support during the Gulf War was essentially a kludge; that is, a flexible and decentralized system composed of very different parts was organized into a working system that successfully served a critical yet temporary need. "And that's effectively how we're going to do it in the future" (AF/XOIWD).

Even though there is considerable validity and strength to this perspective, it must be coupled with the strengths of enlightened central leadership. A recent Pentagon study of the Gulf War found that Army logistics and support units "were hard-pressed to keep up with the rapid pace," and if the victory had not been swift, "maneuver forces would have outrun their fuel and other support" (Rosenberg 2001). As difficult as it may be to achieve, without a single point of responsibility for the overall ICT system, without the cohesion an appropriately focused CIO's office can provide through central authority and the creation and use of formal cross-boundary entities, we may not be as fortunate in the future.

Managing ICT systems means managing risk. In battling the risks of Y2K, there were lessons for the current struggle with risks associated with information assurance, critical infrastructure protection, and security. "What we did during Y2K is going to continue into the information assurance and the CIP program as we move toward better and better ways of managing IT" (AFCIO/AFY2KO). Chapter 4 focuses on applying the lessons of Y2K to managing ICT risk.

Chapter 4 Managing ICT Risk

> Out of Y2K we've learned so much more about the way we really do business and rely on one another. …We have to find a way to flow this into the next level of what we're going to work on. And whether it's CIP (critical infrastructure protection) or whether it's information assurance, they're all part of the same problem. We need to maintain that continuity. …It's going to be up to those of us who participated in Y2K to see to the success in critical infrastructure protection and information assurance and information warfare... that's the future for our organization and, in a sense, for our country. (AFCIO/AFY2KO)

Many managers saw considerable linkage between their Year 2000 (Y2K) response efforts and ongoing efforts to manage other widespread, generic threats to critical infrastructure in general and information and communication technology (ICT) systems in particular. The central aspect of this linkage was the recognition that these efforts were more about managing risk than they were about fixing things.

Not every threat to the security and accuracy of information systems can be eliminated or anticipated; they must be managed as an unavoidable cost of increased reliance on these systems. "Military operations today are heavily dependent on globally shared critical infrastructures. Technological advances have interconnected these infrastructures, better enabling mission accomplishment anywhere in the world. While this connectivity better enables mission accomplishment, it also increases our vulnerability to human error, natural disasters, and physical or cyber attack" (USAF 1999a).

Similarly, the Y2K effort evolved from a focus on fixing ICT systems to a focus on how to manage an uncertain risk to critical information infrastructures. The unpredictability of Y2K stemmed from numerous interrelated sources, including the complexity of information technology (IT) systems and lack of clarity as to exactly how they worked, uncertainty surrounding the nature of the problem itself and how it could be identified, and uncertainty concerning the effectiveness and secondary impact of preventative measures. "Fear of the unknown drove the way Y2K was conducted" (AMC).

Given this high degree of uncertainty, much of the Y2K effort evolved into a massive risk management project. For nearly five years, people across the entire organization worked not so much to eliminate the Y2K threat as to limit the risk of its anticipated impact. "Every effort under Y2K was done to lower risk. … That drove all the decisions we made" (AFCA).

Yet, despite this overlap between Y2K and ongoing security and information assurance efforts, little formal effort was made to leverage the Y2K "investment" to improve management of these related critical ICT issues. "That's a fundamental flaw…a matter of the Air Force's priorities. …We're missing an opportunity to invest wisely… [so as to] sustain some of the good that we had from Y2K" (AF/XOIWD).
This chapter clarifies and analyzes potential benefits from the Y2K experience for ongoing management of ICT security, CIP, and infrastructure assurance (IA).[1] It does

[1] IA more commonly refers to "information assurance," but as discussed throughout this work, the Y2K experience argues for an expanded notion of "ICT infrastructure" that includes not only hardware,

this in two parts: (1) a discussion of the nature of the Y2K risk and the relationship between that risk and the responses it engendered, and (2) the drawing of lessons from Y2K for ongoing management of ICT risk and vulnerability.

4.1 Understanding the Relationship Between Y2K Risk and Response

During Y2K, organizations had great difficultly clarifying the risks they faced. This had a major impact on the nature of the response to those risks. One striking aspect of the Y2K response was a highly reduced tolerance for risk.

4.1.1. Reduced Risk Tolerance

As discussed in Chapter 2 (in particular, see Section 2.2), much of the difficulty in clarifying the risk to ICT from Y2K stemmed from issues involving the complexity of ICT systems and their environments. This complexity contributed to uncertainties about the nature of the Y2K problem itself. "The problem wasn't understood. We had to assume that we would be operating in uncertainty" (374th AW/LG). In turn, uncertainties surrounding the nature of Y2K led to uncertainties about the threat to critical systems and the operations they supported. "People couldn't quantify the risk" (AFY2KO).

Faced with an uncertain threat to highly critical operations, organizations significantly reduced their tolerance for Y2K risk—in some cases, to zero. This occurred "not just within the Air Force but DOD [Department of Defense] wide, and probably even government wide" (AMC/HQ). The difficulty of quantifying a complex, multifaceted problem with a fixed deadline, coupled with an extremely reduced tolerance for risk, led to a response that approached anything associated with Y2K with a broad effort to eliminate as much risk as possible. "If you could identify a problem you had to fix it. If you could theorize a problem you had to go after it" (AMC/SCA).

This broad and exhaustive effort led to frustration among those ICT managers who saw a need to distinguish specific Y2K threats by their likelihood and criticality. For example, the AMC/SCA "instituted a review board to have the programs in a technical sense try to defend why they should be certified. …[The board probed] the changes and how the program worked to determine the probability from the technical standpoint that they'd missed something or created some other problem…" (AMC/SCA). In other words, based upon an understanding of its programs and of the nature of the problem, the board could have made a specific response, but because of other reasons—specifically, the inability of senior leadership to accept less than zero risk—it had to apply a general, zero risk response. "I found it very difficult to explain [differing levels of risk] to more senior leadership. … I can't tell you how much time I could have saved. They basically said 'Any risk at all, forget it'" (AMC/SCA).

Most ICT managers had never operated under a policy of zero risk tolerance, and they saw it as inappropriate for their situation. "Because of the atmosphere of paranoia, any kind of information that appeared would generate [exaggerated responses]. . . ." If

---

data, and information,but also its use and management. Therefore, unless specifically noted otherwise, IA stands for the more encompassing notion of "infrastructure assurance."

completion percentages were less than 100 percent, offices would "spend the next several weeks writing current reports on all the bases…and providing twice-a-week status reports to senior management listing every single piece of infrastructure that wasn't complete, where it was, what the expected due date was, what the fix action was, and who the POC working it [was]. And most of that…was category 4 [lowest priority]." This was considered wasted time; they could have been working on more important problems (AMC/HQ).

ICT middle managers were sometimes caught between the broad requirements of senior leaders and the efforts of local workers to minimize efforts by focusing on high priority systems and issues.

> We spent a lot of time categorizing all of our systems according to the mission criticality categories. … Nevertheless, on several occasions I spent two or three days answering questions from OSD about category 4, non-mission-essential systems. … I had to call the people who manage these systems for this information and they said, "Who cares? If it breaks we get out a pencil and piece of paper and nobody knows the difference." I'd say, "I understand that, but I have to put this information together so it can go up to OSD next week for a big conference that's going on." (AMC HQ)

Clearly there were differences between the risk tolerance of ICT managers and that of senior leadership.

4.1.2. Risk Tolerance of ICT Managers versus Senior Leadership

To a great extent, the frustrations of ICT managers stemmed from fundamental differences in their tolerance for risk versus that of senior leadership. As discussed in Section 2.4, ICT managers and senior strategic managers have significant differences in training, experience, work environment, and perspective. These differences led to very different responses to the uncertainty surrounding Y2K risk.

On the one hand, to the more politically motivated senior administrator, failure can be a career-threatening event. Senior managers saw Y2K as a predictable risk. From this perspective, the clear response was to anticipate the worst-case scenario and work to eliminate as much of this risk as possible. On the other hand, ICT managers saw failure as part of their job; something they understood and dealt with every day. As engineers, they viewed senior decision makers as trying to force an unrealistic level of software reliability and assurance on Y2K (AMC/SCA). ICT managers found it difficult to understand why levels of risk they routinely accepted were now unacceptable and, even worse, causing a considerable drain on their time and resources. One manager reported being required to go through a week's worth of effort to recertify a system after a minor change, despite having informed his senior officer that it had virtually no chance of causing a Y2K failure, because he could not *guarantee* that a failure would not occur.

As senior managers took responsibility for Y2K, however, they also became frustrated. In their case, frustration stemmed from the inability to get clear, concrete answers to what they saw as basic questions, such as, "Is this system Y2K compliant?" or "Can you assure me that this will not experience a Y2K failure?"

4.1.3. IT Industry Compliance Statements

Given the uncertain atmosphere surrounding Y2K and its accompanying risks, most organizations (including the United States Air Force, hereafter simply USAF, or Air Force) sought assurance from the IT industry itself. In developing their operational definition of Y2K compliant, these organizations relied heavily on Y2K compliance statements provided by system component manufacturers. Y2K workers either obtained these statements from individual system points of contact (POCs) (a highly duplicative effort) or found them posted in organization-wide inventories, such as the Air Force All Systems Inventory (AFASI).

Unfortunately, whether industry Y2K-compliance statements were applied bottom up or top down, they generally failed to reduce the uncertainties surrounding Y2K risk. Specifically, compliance of parts, components, and subsystems carried no guarantee of reliability when interacting with other components of the larger system, and industry Y2K-compliance statements were careful to state this. For example:

> Our products depend on many aspects of your computer system for their correct operation. They will not be Year 2000 Compliant if the rest of your computer system, including software, hardware, firmware, and other aspects of the system or service including the operating system and BIOS, is not Year 2000 Compliant or is adversely affected by the Year 2000. (QLogic Corporation 1999)

In addition, component manufacturers could not be viewed as fully objective, since noncompliance of older products could lead to increased sales of newer ones. Here again, senior managers could not find the assurances they sought.

4.1.4. Legal Factors

Another set of factors that greatly impacted senior management tolerance of Y2K risk and further fueled the broad and exhaustive Y2K response was legal concerns related to faultfinding if disruption from Y2K occurred. The Federal Y2K Act, passed in July 1999, specified that

> A defendant who wishes to establish the affirmative defense of Y2K upset shall demonstrate, through properly signed, contemporaneous operating logs, or other relevant evidence that—(A) the defendant previously made a reasonable good faith effort to anticipate, prevent, and effectively remediate a potential Y2K failure. … (Y2K Act of 1999)

The Air Force's good faith effort was couched under the even stronger phrase "due diligence." "The responsible individuals, in this case…leadership, had to take an attitude of due diligence and awareness" (AFCIO/AFY2KO). However, due diligence was not formally defined; rather, it became a general sense of doing everything possible to assure operational capabilities. Nevertheless, due diligence became a fundamental aspect of the Air Force Y2K response, filtering down from senior leadership to all participants in the effort.

> Due diligence will probably be the most important tenet after the dust settles. If your mission-critical or mission-essential system should fail due to a Y2K problem, you may find yourself testifying in court. Without evidence of due diligence, those involved could be held liable for the damage created by system failures—this is the case in the Air Force because the certifier must sign documentation to certify the system is Y2K compliant. (Ashton 1998)

Unfortunately, people charged with addressing what was already an unclear Y2K threat now had the added vague legal threat of due diligence to consider. This led to even more extreme efforts to eliminate what was viewed as a nonquantifiable risk. In other words, the only time workers were allowed not to fix a problem was when they "could guarantee zero probability that there would be the possibility of an error," which was impossible to do (AMC/SCA).

These due diligence concerns made it difficult to control the scope of the Y2K response. "Because of due diligence, there was a fear that if we didn't try something, then somebody could accuse us of not doing everything possible if anything at all went wrong (AMC/SCA). The legal (and political) pressures of due diligence drove certification approval to higher levels, involving more auditing and inspection groups. These groups further advocated a broad response that treated all potential aspects of the Y2K problem equally, whether they were mission critical or not. According to the 375th AW/LG, the AMC Audit Agency's position was, "If it's got power, check it."

4.1.5. Politics and the Media

Even when not directly linked to due diligence, outside political and media pressure further heightened the level of Y2K response. On the one hand, this pressure was beneficial in helping to bring together the critical mass of people and resources needed to address the cross-functional, cross-organizational Y2K problem. On the other hand, this outside pressure, particularly in the form in which it came from the media, helped fuel the broad nonspecific response and zero tolerance policy. "In the beginning, there were basically two types of press coverage on Y2K." These were one, the kind that predicted disaster, and two, none. "In that kind of environment…the only information…[being disseminated is about] the next disaster that's going to destroy western civilization. …That brought to bear all the political pressure that helped drive the zero tolerance policy and guided everything we did from there on" (AMC HQ).

Reports from the media could particularly affect senior administrators who lacked the familiarity with ICT that would allow them to discern media hype from accurate reporting. "Generals read press reports and called down, wondering about their cars" (AFCA). Whether or not it was the media who brought non-ICT infrastructure to the attention of senior leaders, this focus also had a major impact on Y2K risk management.

4.1.6. The Inclusion of Non-ICT Infrastructure

The inclusion into Y2K of non-ICT infrastructure was another significant factor in the heightened effort to eliminate Y2K risk. The 374th AW/LG "spent months going through inventory…[including checking] if a Toyota Land Cruiser was Y2K compliant." This

expansion of Y2K to include more traditional infrastructure went far beyond cars to include power generators, alarms, refrigerators, traffic lights, air conditioning, and sprinklers. The uncertainty that drove this expansion stemmed from a tiny but legitimate risk from hardwired dates in embedded chips. The likelihood of having an embedded chip relying on a hardwired date was small; the likelihood of that date having a Y2K error was even smaller; the likelihood that the chip's function required sensitivity to the century was even smaller (a sprinkler, for example, might be sensitive to the day of the week or hour of the day); the likelihood of a century-sensitive chip failure having a critical cascading functional impact was even smaller. Yet, because a faulty chip was so difficult to locate and impossible to fix (it required replacement), this issue became the public focus of Y2K, the so-called ticking time bomb widely reported in the media and discussed in Congress.

In the context of zero risk tolerance, meeting the embedded chip threat required a huge, almost never-ending effort. ICT managers recognized that this was a fundamentally different issue from the Y2K data and ICT systems issues they had been dealing with. Since traditional infrastructure items varied greatly by location and were generally managed at the local level, many Air Force ICT managers passed this burden on to the bases. Not surprisingly, delegating the chip issue to the bases had a significant impact on the Y2K effort at the local level. For some bases, this meant checking "anything with possible date ramifications. We received inquiries about refrigerators and sprinklers" (375th AW/CG). Even though one base may have had the same systems as another base, each chip was considered unique and therefore was checked. Thus, the effort was extremely arduous ("I wasted 10 months of my life" [374th AW/LG]) and could require what appeared to be considerable duplication. Were there existing organizational mechanisms for managing risk that could have brought greater order to this effort?

4.1.7. COOPs and ORM

An organization such as the Air Force has considerable experience with conducting operations under risk conditions. How did existing mechanisms for managing risk impact the Y2K effort? Two related mechanisms that came into play to varying degrees during Y2K were Continuity of Operations Plans (COOPs) and Operational Risk Management (ORM).

Risk of disruption from a predictable threat can be reduced not only by addressing the threat itself but also by addressing its potential impact. As the perceived deadline for Y2K approached, the response effort shifted focus from fixing systems to preparing for continued function in the face of uncertain impact (see Section 1.3.2.3). In August 1998, GAO released its Year 2000 report on "Business Continuity and Contingency Planning," which stated:

> Time is running out for solving the Year 2000 problem. Many federal agencies will not be able to renovate and fully test all of their mission-critical systems and may face major disruptions in their operations. …Because of these risks, agencies must have business continuity and contingency plans to reduce the risk of Year 2000 business failures. Specifically, every federal agency must ensure the continuity of its core business

> processes by identifying, assessing, managing, and mitigating its Year 2000 risks. (GAO 1998b)

As an organization familiar with operating under threat of disruption, the Air Force already maintained plans for assuring continuity of operations if a disruption occurred. Faced with the need to establish Y2K continuity plans, Air Force leaders looked to its existing COOPs (as well as, to some extent, its ORM, as discussed below).

> Review and exercise your continuity-of-operations plans: A Y2K test at Keesler Air Force Base, Miss., showed we couldn't simply rely on assurances that systems are Y2K compliant. During that May 11 and 12 test, compliant systems—including commercial off-the-shelf software, encountered Y2K anomalies. Ensure your COOPs cover your mission-critical processes—the ones you can't afford to shut down. Use operational risk management to assess which of your critical processes are most likely to be affected and how they would be affected. Review your COOPs to ensure you can get the job done even if computers fail. Ensure [that] your COOPs are resourced, particularly if you're depending on goods or services you don't control. Finally, ensure [that] you've thoroughly tested your workarounds. Think of Y2K as ability to survive and operate. (Ambrose 1999)

The effort to apply COOPs to Y2K continuity planning revealed inadequacies in the COOPs as plans for minimizing uncertain risk of widespread disruption. First, given the high degree of personnel turnover and reassignment in the military, COOPs tended to be more about job continuity than consequence management. The focus was on individual unit activity, not overall mission operation with the possibility of uncertain disruption. There was little uniformity in the various unit or even base plans and little attention to interdependencies outside a given unit's control. "Each squadron and group had a COOP, but we needed an overall plan for the base" (374th AW/CS).

Second, given reductions in personnel and the accompanying increased effort to meet ongoing operational needs, COOPs were given extremely low priority and were rarely reviewed; in some cases, they could not even be located during base visits. In most cases, the backup plan was "just do things like we were doing them using pen and paper" (374th AW/OG).

Nevertheless, Air Force Y2K leaders made a concerted, though initially ad hoc, effort to build on the existing COOP structure to develop a cross-organizational plan for continuity of critical missions while facing uncertain Y2K disruption. The focus of this centralized effort was interdependency—how to continue mission accomplishment with the possibility of disruption to mutually dependent, separately controlled entities. Over time, this focus was extended to include organizations and communities outside the Air Force. For example, a logical extension of a COOP was a community outreach program based on the president's program (AFCA).

Once Y2K managers began looking at interdependencies, it became difficult to delineate where these interdependencies stopped. Like other aspects of the Y2K response, the effort to use COOPs to reduce the risk of disruption became exhaustive, especially as the new century approached. To help prioritize the ever-widening range of continuity efforts, some Y2K leaders looked toward another Air Force mechanism for managing risk, namely, ORM. "Operational Risk Management was applied to contingency planning" (375th AW/SC). In the Air Force, ORM had been a recent development focused on predictable risks to safety. "The [Air Force] always deals with

risk, but…the culture has become not to take any predictable risk. Aircraft crashes are predictable, so the [Air Force] will try to reduce them to zero. …ORM…[is] a systematic approach to get the risk out in the open for evaluation" (AFCA). Since Y2K was considered a predictable risk, it made sense to attempt to use ORM as a tool to guide response efforts by evaluating the various levels of risk.

Unfortunately, efforts to guide the Y2K response strategy based on such ORM classifications as criticality of impact and likelihood of occurrence, though not without some benefit, had minimal impact. As discussed in Section 2.2, these efforts were hampered by the technical complexity of ICT systems and nontechnical factors of the ICT environment. Other than at the highest level Commander in Chief (CINC) thin line systems, it became too difficult to discriminate different levels of Y2K problems and responses; thus, "for all practical purposes, every system went through the same level of scrutiny" (AMC/SCA).

While complexity issues were central to the difficulties in applying ORM to Y2K, there were organizational issues as well. ORM was seen as a process applied by specific offices associated with safety. It was difficult to suddenly turn ORM into a general way of thinking that could guide a cross-organizational risk reduction effort. "The Office of Primary Responsibility (OPR) is usually responsible for ORM training. Safety and Manpower usually apply ORM to most things to assure a common understanding in the case of, for example, accident investigations. ORM should be decentralized. It's a concept, not an application" (375th AW/SC).

Though little formal effort was made to apply ORM to addressing potential Y2K problems in ICT systems, there was a more formal effort to apply ORM to Y2K continuity planning.

> We told people in the guidance for making COOPs to go through an ORM process. Deal with your safety guys and find out how to do [it]. We didn't do that in the software; we didn't do that in the infrastructure; we did it basically in the COOPs. (AFCA)

However, since ORM categories and procedures were not clearly defined or understood, the uneven application of ORM to COOPs could actually confuse rather than clarify the continuity planning effort. AFCA asked bases to use an ORM approach to COOPS using prioritized risks, such as complete loss of service and generation of bad data, but "the development of COOPs occurred at different levels, some of them very high and some of them very low. And what we found on a lot of our strike teams was a marrying of those levels [that] became a cloud [of general assumptions that everything would work out]" (AFCA).

In fact, some local units used ORM to justify a reduced focus on their ICT systems. Since central management was already working on most of the systems on a base, an ORM analysis could lead a base to focus more on traditional infrastructure, such as power and telecommunications, especially when those systems were not under their control (that is, they were provided by off-base facilities).

4.1.8. Effectiveness and Appropriateness of the Response

Many lessons for ongoing management of ICT risk can be drawn from the overall story of Y2K risk and response. Before drawing out the most important of these lessons, however, it seems appropriate to briefly address what was once a highly visible issue—the effectiveness and appropriateness of the Y2K response. While this study was never geared toward formally assessing the effectiveness of the Y2K response, this section on the relationship between Y2K risk and response might be viewed as incomplete without a few general comments on this complex and potentially controversial subject.

At the most basic level, the question could be asked, Was the Y2K response effective? If "effective" is defined simply by outcome, than the answer is yes. There was a complex problem; changes were made; in the end, there was little impact. If "effective" entails a sense of how much change was made, however, the answer would depend on how change is defined and counted. The anecdotal evidence indicates there was far more change to IT equipment and systems than to non-IT infrastructure. Changes to IT infrastructure may have impacted up to half of the IT inventory items; changes to more traditional infrastructure items probably ranged between 2 and 5 percent (AFCA). As discussed throughout this report, changes to operational and management practice could be far more significant, though less easy to quantify.

Did some of the resources to address Y2K go toward changes that were needed outside of the Y2K effort and would have occurred anyway? Given the interconnectedness of ICT systems, changes to one part of the system invariably impact other parts. Therefore, it is extremely hard to separate changes that addressed Y2K from other associated problems in the system. This was especially true where upgrades were seen as part of the Y2K solution. For instance, hardware could become obsolete from software upgrades—like taking an e-mail system from Microsoft Mail to Outlook—or firmware upgrades could require the replacement of routers (374th AW/CS). Some of these upgrades and replacements, made with Y2K resources, addressed maintenance issues that existed independently of the Y2K situation. For instance, the 374th AW/CES replaced generators dating back to 1948.

This leads to perhaps the most difficult question: Was the magnitude of the Y2K response proportional to the Y2K risk faced? It is extremely difficult to tie specific remediation efforts to the eventual outcome or to precisely quantify the costs of those efforts. To some, "the real loss was the functionality that we didn't have because we were working on Y2K. …All the manpower [not accounted for in the costs] that we spent on Y2K [could have been allocated to more meaningful tasks]," such as implementing new functionality (AMC/HQ).

Given all the factors discussed thus far, it certainly was difficult for Y2K managers to determine when their efforts were cost-effective. The combination of reduced risk tolerance and a situation where risk could never be eliminated meant that there was little rationale for declaring a Y2K activity to be completed. Instead, Y2K workers ran a race against the clock to continually reduce risk, with little basis for determining when a given effort was sufficient.

> Toward the end, the questions were coming down from on high—"Have we done enough? How sure do you feel?"… A contractor came forward at one of the OSD meetings and said, "We've tested a couple of your systems and we've found a couple of errors." That just drove

> people crazy. "You mean we haven't solved every error?" Then we expanded this risk aversion out to the overseas bases. There's nothing wrong here [but] let's check the countries that are giving any kind of infrastructure support to the host base. ... Even to the last moment… if you had any resources left, [you had to find] something else to do. …How much risk [should we have been] willing to accept [given our] mission operation? I can't answer that, but if you take that train of thought you're going to lead to that same paranoia we had. … I don't know what enough is. [At some point] you have to say, "This is enough" and then live with that. (AFCA)

Thus, from the perspective of many ICT workers who were used to dealing with constant risk to software and systems, the unusually reduced tolerance for risk in the face of Y2K uncertainty led to an excessive response. "It was a due diligence action that…wasted…[a] lot of time and money doing things that were completely unimportant" (AMC HQ). With IT, risk is assumed just by using it, something upper management did not understand. "Every one of our programs has a number of problems that are always being uncovered and always being fixed. ...Was the cost of the response equal to the potential cost of harm? …Absolutely not. I think we spent a lot more than was necessary…" (AMC/SCA). "There was a genuine risk," but because of the publicity surrounding it and the abundance of funding available, "it was overstated" (374th AW/CS).

For numerous reasons, however, many of which had little to do with technology, senior leadership took the position that disruption was not acceptable and that if it did occur, it would not be for lack of attention or effort. Viewing Y2K primarily as a predictable and potentially highly disruptive threat, this was a reasonable stance to take. An effort that went beyond the usual cost justification was acceptable as long as disruption was minimized, which it was. If a similar degree of success could have been achieved with less effort, that does not negate Y2K as a real problem, nor does it mean that future efforts to manage risk should receive not comparable attention and support.

Far more important than trying to determine whether the Y2K response went beyond cost-effectiveness is the recognition that Y2K was an important new experience and that we need to learn from it. For most senior leaders, it was their first experience in being responsible for an enterprise-wide, mission-driven, highly uncertain ICT problem. The goal at this point should not be to determine the cost-effectiveness of the Y2K effort but, rather, to continually improve handling what is an extremely complex and dynamic job—managing ICT in general and ICT risk in particular.

> We need to treat CIP and information warfare and where we go post-Y2K in some of the same ways we treated Y2K. We have to… bring it to the attention of the leadership in such a fashion that they understand it, so that these don't fall off the table like Y2K almost did. (AFY2KO)

4.2 Application to Security, CIP, and Infrastructure Assurance

Even though Y2K included a massive, multiyear ICT risk management effort, that effort did not significantly impact the ongoing programs for addressing threats to ICT. One of the main reasons for this was that Y2K represented a different kind of ICT risk that did not fit neatly under the existing categories of ongoing effort: security, critical

infrastructure protection, and infrastructure assurance. Security and CIP focus on deterring hostile threats, while infrastructure assurance focuses on mitigating the impacts of those threats.

> *Infrastructure Assurance*: Preparatory and reactive risk management actions intended to increase confidence that a critical infrastructure's performance level will continue to meet customer expectations despite incurring threat inflicted damage. For instance, incident mitigation, incident response, and service restoration. (PCCIP 1997)

Probably the central lesson of the Y2K experience for ongoing management of ICT risk was the recognition that serious and costly threats could stem not only from the intentional action of a conscious enemy but also from the unintentional consequences of our own actions, confounded by complexities of the ICT system itself and our inability to adequately manage those complexities. Y2K argues that we should expand our notion of infrastructure assurance to include these unintentional, systemic threats.

4.2.1. Intentional versus Systemic ICT Risk

The 1997 report of the President's Commission on Critical Infrastructure Protection focused on issues stemming from intentional actions of hostile enemies. "A *threat* is traditionally defined as a *capability* linked to hostile *intent*" (PCCIP 1997). In the commission's report, the categorization of risk was based primarily on the nature of the target. Physical threats were threats to such physical assets as power stations, pipelines, telecommunications facilities, bridges, and water supplies. Cyber threats were threats to computer systems, especially the information-carrying components of those systems—data and code. "The Commission focused more on cyber issues than on physical issues, because cyber issues are new and not well understood. We concentrated on understanding the tools required to attack computer systems in order to shut them down or to gain access to steal, destroy, corrupt or manipulate computer data and code" (PCCIP 1997).

In its consideration of physical vulnerabilities, the commission acknowledged both natural and man-made threats: "Infrastructures have always been subject to local or regional outages resulting from earthquakes, storms, and floods. … Physical vulnerabilities to man-made threats, such as arson and bombs, are likewise not new" (PCCIP 1997).

Similarly, in its consideration of new cyber vulnerabilities, the commission acknowledged natural threats in the form of accidents and negligence while focusing its energies almost entirely on man-made threats, which range "from prankish hacking at the low end to organized, synchronized attacks at the high end" (PCCIP 1997). Following this report, the next year's Presidential Decision Directive (PDD) 63 focused on intentional man-made "attacks" on cyber systems (even as Y2K was increasingly expanding our awareness of and attention to the more "natural" systemic components of ICT risk).

> II. President's Intent: It has long been the policy of the United States to assure the continuity and viability of critical infrastructures. President Clinton intends that the United States will take all necessary measures to swiftly eliminate any significant

> vulnerability to both physical and cyber attacks on our critical infrastructures, including especially our cyber systems. (EOP 1998b)

No one can deny the importance of ICT security, CIP, and the high degree of attention required to address intentional threats to critical systems. Nevertheless, Y2K illuminated the magnitude of another category of cyber threat—unintentional threats from the complexity of the system itself and our inability to fully manage it. As discussed throughout this report, the Y2K systemic threat went far beyond accidents and negligence to the heart of how ICT systems evolve over time and are used to achieve organizational goals and accomplish mission objectives.

The Y2K experience also revealed fundamental differences between intentional cyber threats and systemic ones. Hostile intentional threats originated primarily from outside the ICT system (although this includes outsiders who gain access to the inner workings of the system); systemic threats originated from the nature of the system itself, including the complexities of its interrelated subsystems, the environments within which it exists, and the ways it is managed and maintained (as discussed in Chapters 2 and 3). Intentional threats presume an adversarial relationship, with a general goal of deterrence; systemic threats presume an interdependent relationship, with a general goal of improved communication and coordination of multiple perspectives, objectives, and tactics.

These two types of threat generate two categories of ICT risk: (1) intentional risk from outside disruption of functionality, and (2) systemic risk that is often the price of increased functionality itself. Y2K was a symptom of the second type of risk. Furthermore, Y2K revealed that the uncertainties surrounding systemic risk could be as great, if not greater, than the uncertainties surrounding hostile enemy attack. For one thing, responsibilities for addressing intentional risk are easier to identify—it is primarily an us-versus-them scenario. Responsibilities for addressing systemic risk are much harder to identify. In fact, identifying responsibility for systemic risk can be the toughest issue to address, particularly when there is a mismatch between functional nodes of responsibility and a potential problem located between those nodes.

Despite the differences between intentional and systemic risk, ICT managers need to address both types of risk within a coherent strategy. In some instances, these two elements of risk overlap, allowing a single tactic such as continuity planning to minimize the potential impact of both. In other instances, efforts to address these types of risk become competing desirable ends that need to be balanced along with the many other competing desirable ends of ICT, such as functionality, usability, and maintainability.

4.2.2. Enterprise-wide ICT Risk Management

As with ICT management in general (discussed in Chapter 3), management of the various types of ICT risk requires an enterprise-wide perspective that carefully considers and appropriately balances the many competing dynamic demands on ICT systems. This means that efforts to manage intentional and systemic risk need to be integrated not only with each other but also with other desirable ICT goals. For example, user behavior that increases ICT risk can stem from tensions between security and desired functionality, as when users punch a hole in or even take out altogether a firewall in order to accommodate a legacy system that cannot deal with it (AFCIC/SY).

Conversely, actions taken to increase security can adversely affect user functionality. Much of IT security tends to degrade capability, and often with unknown consequences. For example, when an e-mail attachment or signature profile is infected with a virus, it is blocked. For a war-fighting CINC, this loss of in-transit visibility means that the information on an airplane's contents (namely, cargo or personnel) is lost. When users detect a virus, their Simple Mail Transfer Protocol and Internet Protocol are blocked. For a 24-hours-a-day, 7-days-a-week operation, this denial of service can mean the loss of an enormous amount of data. Further compounding these issues is the breadth of activity that is affected: Many units operate outside of Air Force bases and even outside the DOD (AMC/SCA). "We're still not organized in how we will deal with balancing security and information flow needs" (AF/XOIWD).

In addition to interdependencies between security and functionality, there are also interdependencies between efforts to manage ICT risk and efforts to acquire, develop, and field systems. Sometimes these interdependencies can lead to tensions in the relationship between the risk management and development communities. For example, units responsible for fielding new systems can be frustrated by the lack of uniformity across the organization, especially in the diverse operating environments. Different servers in the same environment may have different disk drives, use different versions of the database management system, and run different versions of the operating system. "As a result of that we can't distribute software in a rational manner" (SSG).

On the other hand, units responsible for risk management can take a different view of this situation. From the perspective of information warfare, diversity makes it more difficult for an adversary to figure out how to breach a system. "If every piece of software is absolutely standardized, one hole gets you in everywhere. …That's a fundamental point that's almost always missed" (AF/XOIWD). "Using the same system on every base is a double-edged sword. … They figure out what to do with it, and they're going to attack everybody. … That's one of the reasons why we want some variety out there" (AFCERT).

Still other potential tensions can be seen between the goals of risk management and the informational needs for management of integrated systems (see Chapter 3, Section 3.11). ICT managers cannot handle such issues as version control and configuration management without regular gathering and dissemination of system information, yet the restriction of this same information may be necessary for security. Y2K informational efforts brought out this tension. "The cause and tension that really needs to be acknowledged with the issue of classifying the AFASI is that while this database is useful [for ICT managers], it also is your adversaries' targeting database; therefore, there is a rationale for classification. The tension is between usability for continuing IT management and not giving your adversary… the keys to your kingdom" (AF/XOIWD).

These various interrelationships and tensions indicate that strategic risk management, like strategic ICT management in general, is a cross-organizational activity best approached from an enterprise-wide perspective. This lesson was learned during Y2K, but even though many ICT managers saw its relevance to ongoing security and risk management efforts, there was little actual transfer. "Alhough we learned that Y2K was an operational problem—not just the purview of the SC—we fundamentally have handed

CIP to the SC to do. This means that with CIP, people are fighting the same battles we had to fight [with] Y2K" (AF/XOIWD).

Clearly, the Y2K experience was relevant to ongoing ICT risk management, though that relevance still needs to be captured and assimilated. To help in this effort, the following section includes lessons of the Y2K experience that can be incorporated into strategic ICT risk management efforts.

4.2.3. Lessons of Y2K for Strategic ICT Risk Management

Based on the discussion thus far, two central lessons for the ongoing, strategic management of ICT risk can be drawn from the Y2K experience.

1. Expand the notion of infrastructure assurance to include unintentional, systemic risk, and integrate efforts to address systemic risk with more established efforts to address hostile, intentional risk.

2. Manage ICT risk from an enterprise-wide perspective, balancing and incorporating efforts to achieve the goals of security, CIP, and infrastructure assurance with the many other interrelated efforts to achieve ICT goals.

In addition to these two general lessons, additional lessons of Y2K can be applied to the ongoing management of ICT risk. Many are versions of the general management lessons discussed in Chapter 3, applied to the issues of security and risk.

3. In risk management efforts, increase the focus on the use of data and information to achieve organizational goals.

As discussed in Chapter 2, Section 2.3, strategic ICT management needs to shift its central focus from hardware and software to data, knowledge, and organizational goals. Similarly, risk management needs a greater focus on data and information corruption issues, which span both intentional and systemic ICT risk.

As we move increasingly into a world where critical actions are taken based on electronic output, corruption of data and information (whether from hacker maliciousness or systemic complexity) becomes the element of ICT risk that has highest impact and is most difficult to recognize.

4. Integrate risk management with life-cycle management of ICT systems.

Section 3.10 discussed the importance of addressing cross-boundary organizational issues in the life-cycle management of systems. For risk management, this means that life-cycle issues such as version control and configuration management need to be integrated with security and infrastructure assurance efforts. "The real basis of information assurance… is maintaining accurate inventory systems, making sure that configurations are controlled and managed and making sure that all the settings on the firewall are the same on every Air Force base" (SSG). "You need to know what you're defending in order to do critical

infrastructure protection. …This [knowledge] has the possibility of atrophying very quickly…[without a] resource stream to support its continued viability" (AF/XOIWD). Y2K showed the importance of knowing not only what is being protected but also the current state of that protection.

The information needed to support life-cycle management of ICT also represents a security risk, however, as discussed in Section 3.11. "We have to have an up-to-date inventory. But there again, it's a double-edged sword. We have to protect that information; otherwise, somebody else is going to use it" (AFCERT). This further increases the need to integrate ICT risk management with life-cycle management.

5. Clarify how risk information is disseminated.

Another information issue associated with risk management is the dissemination of risk-related information. Y2K demonstrated that there could be considerable confusion about how this occurs, especially in a large, security-conscious organization. Therefore, the dissemination of risk-related information needs to be a coherent component of the enterprise-wide, strategic management of ICT.

6. Extend collaboration on risk management beyond the organization.

Y2K emphasized the importance to risk management of collaboration and information sharing outside the organization. As discussed in Section 3.13, the Chief Information Officer's (CIO's) office should serve as the single point of contact for ICT coordination outside the organization. Actual cooperation and communication among organizations, as coordinated by the CIO's office, might well be undertaken at various levels.

7. Address funding barriers to enterprise-wide risk management.

Just as funding issues can become a barrier to overall ICT management (as discussed in Section 3.8), so too can they represent a barrier to enterprise-wide ICT risk management. Security is an area where funding is often available and where "stovepipe" efforts to gain that funding can work against cross-organizational coordination. In most cases, an enterprise approach to risk management is both functionally superior and more cost-effective. "Until SPOs (system program offices) and requirements writers and commanders understand information assurance, we're not going to have it built into the system. … [Some say] security is too expensive to build in up front, but it's a lot more expensive to put in later" (AFCIC/SY).

8. Distinguish day-to-day functional issues from enterprise-wide issues.

Y2K demonstrated the importance of distinguishing day-to-day operational issues from cross-organizational strategic issues. The strategic approach of senior leaders was not always applicable to individual issues of ICT risk, nor was the functional approach of ICT managers always applicable to enterprise-wide strategic risk issues. In adopting an enterprise-wide approach to risk management, it is important to distinguish day-to-day

functional issues that can be handled better and more efficiently at the local level from higher-level, cross-organizational issues that require more central, strategic management.

9. Adopt and apply existing safety-oriented approaches to ICT risk management.

As discussed in Section 4.1.7, safety-oriented approaches to risk management, such as COOPs, ORM, and Operationalizing and Professionalizing the Network (OPTN) were only marginally applied to the Y2K situation. With modification, these approaches can help formalize cross-organizational risk management, but the transition from safety to ICT is not trivial.

For many, the Y2K effort that was most clearly relevant to ongoing ICT risk management was the COOP initiative. While this effort revealed a number of inadequacies in the creation and maintenance of existing COOPs, the Air Force can build on this learning experience. COOPs are a highly applicable way to minimize ICT risk, whether from hostile enemy action or systemic complexity, but problems were revealed during Y2K. Specifically, COOPs need to be far more rigorous in both creation and maintenance. In addition, given their background in traditional disaster planning, COOPs need to be more sophisticated in accounting for the complexities of ICT systems.

10. Do not return to business as usual.

As discussed in Section 2.7, after Y2K there were many reasons why managers sought a return to more comfortable, less enterprise-wide methods of managing ICT. Nevertheless, the crisis mentality of Y2K stimulated enterprise-wide approaches to ICT that produced benefits for related security and infrastructure protection issues. ICT risk is always with us, and even in the absence of immediate crisis, it is critical to resist the seemingly easy path of a return to business as usual. Certainly the events of 9/11 have cemented this lesson.

11. Recognize the possible need for special regulations in support of ICT risk management.

Y2K helped the Air Force recognize that, in many ways, ICT risk management was different from managing risk in a more traditional infrastructure. These differences could require special regulations and more centralized, cross-functional management. For example, stricter regulations are needed on the use of International Merchant Purchase Authorization Cards to make ICT purchases outside the funding cycle.

12. Recognize the need for special training on ICT risk management.

Y2K demonstrated that ICT risk management could require both the need for special regulations and the need for special training, particularly in support of users. For example, some units recognized the need to give users more exposure to network issues, since they represented "an internal vulnerability" (374th AW/XP).

13. Consider not only the question of why complex systems fail but also why they do not.

One of the hidden lessons of Y2K was that complexity increases system vulnerabilityas well as reduces vulnerability through redundancies and other inherent backups and alternative functions. As an organization with experience in attacking infrastructure, the Air Force knows that disrupting critical infrastructure is not a trivial undertaking. Y2K revealed that the Air Force is not yet completely dependent on ICT systems, and perhaps that it does not want to be. Most units are trained in operating without computers, and they perform quarterly exercises that involve using manual forms. This, of course, slows down the procedure and causes a slight degradation of service; moreover, during wartime it would be "an enormous manpower drain." However, it can be done (374th AW/LG). In part, this is an issue of trust in technology as well as a realization that, ultimately, people enable our systems to function.

Understanding why systems are resistant to failure is an important component of learning to better protect them. The rhetoric of cyber warfare is that infrastructures fail rapidly, yet Y2K indicated that "information infrastructure may be more robust than people assume" (AF/XOIWD). Did the small scale of Y2K disruption result from organizations solving all their problems, or did the infrastructures have an inherent robustness that we need to better understand? More study is needed to explore this question.

14. Establish a permanent, enterprise-wide point of contact for ICT risk management.

Finally, the difficulty in capturing and applying the lessons of Y2K, even after a multiyear, multibillion-dollar, cross-organizational effort, indicates the need for better methods of absorbing new ICT policies and practices into organizational structure and culture. As ICT systems open new operational possibilities, they also call for increased coordination and organizational flexibility.

Like the many other aspects of ICT management discussed throughout this report, ICT risk management requires a permanent, cross-organization point of contact under the guidance and auspices of the CIO (as discussed in Section 3.13). Only such an entity, bringing together not only knowledge of security issues but also multiple perspectives on the organizational roles and goals of ICT, can take on the complexity of enterprise-wide, strategic ICT risk management.

Chapter 5 Technology Risk as a Socially Embedded Issue

Y2K was a massive meta-experiment that touched on the core processes of the new digital millennium that was dawning. It offers us valuable perspectives on the nature of software, our vulnerabilities in a computer-dependent world, the future evolution of information technology, and the relationship of these with people and organizations. If Y2K was a threat to the trustworthiness of critical infrastructure, what lessons from Y2K are relevant to other threats, such as blackouts, terrorism, or software reliability? Can the Air Force's Y2K experience help us understand those vulnerabilities and better appreciate their differences and the effectiveness of potential responses? Going even further, does the Y2K experience provide lessons that will better enable us to take advantage of the increased capabilities of networked information and communication systems while minimizing the inherent risks in this increasingly connected world?

The "decision" (however complex its evolution) to represent calendar years with two digits was human and organizational, not technical—just as the mismatch between metric and English measurements that destroyed the *Mars Climate Orbiter* in 1999 was a human and organizational error, not a technical or a mathematical one (or a terrorist attack). Thus, a key perspective reinforced by this study is that *technology is socially embedded*. It exists in the context of people and organizations. Ineffective organizations with great technology will usually produce ineffective results, while effective organizations with less than state-of-the-art technology can get by just fine.

As in many other organizations, Y2K instigated the Air Force's first enterprise-wide, formal effort to integrate IT management with organizational missions and functions. This large-scale alignment of operational and strategic management (see Section 2.4) reinforced the importance of recognizing the social nature of technology. For example, continuity planning was an element of the buildup to Y2K and is an essential part of preparations for natural disasters, terrorist attacks, and other threats and disruptive events. This planning requires deciding what functions are vital and identifying who depends most crucially on what systems, decisions that necessarily involve social, organizational, and political issues.

History repeatedly shows us the necessity of incorporating a human, social, and organizational perspective on technology security and reliability. For example, even a mathematically *perfect* encryption system (the "one-time pad") is vulnerable to the human element when people decide to reuse pages. (Benson). Similarly, the widespread electricity grid failure in August 2003 has been attributed in part to an analyst who fixed a data error for an automated tool assessing the health of the grid, then forgot to reset it to run automatically and left for lunch (U.S.-Canada Power System Outage Task Force). This set of conclusions is actually a point of view: large-scale complex IT systems must be viewed through the lens of a social system, giving priority to management and other "people" issues.

The Air Force's Y2K experience teaches us about software as a social system. It highlights the limitations and pathologies that typically grow out of social organization, training, and group complexity. It also illustrates that some technical approaches are better adapted than others to the social systems currently in use. Y2K thus enables us to ask what alternative approaches to software development, deployment, maintenance,

testing, and security may be more successful, recognizing the enduring impact of people on technical systems.

This report rejects the idea that the Y2K problem was simply one of fixing the technology, recognizing that it was driven instead by a concatenation of institutional, leadership, economic, and political factors, as well as technical ones. As the introduction to Chapter 2 observes, "the problem… taught those who worked on it more about their overall organizational operation than about their technology."

A key organizational issue identified by this report is that no single unit "owned" the problem, that "no single group could fully control the issues. Enterprise-wide perspectives…had to be considered." This meant, for example, that "efforts to decompose the Y2K problem and organizational responses into discrete components were largely unsuccessful."[1] Cross-unit interdependencies were the single biggest challenge to remediation.

As the report observes, these problems were not unique to Y2K. They just became more obvious under its intense spotlight. We should therefore understand the Air Force's Y2K experience not as a freestanding phenomenon but as typical of large-scale software systems embedded in a complex institutional setting. As the Air Force gradually discovered (see Section 2.3), this meant shifting the focus from hardware and software to organizational issues.

The extent to which remediation efforts were successful can be attributed in part to a shift in perspective—an evolution from techno-determinism to a broader social understanding. A "technical" problem like Y2K may initially be seen as *sui generis*, to be described only in its own terms. Its effects are seen as direct, widespread, and determinative of other social outcomes. Eventually, these initial erroneous enthusiasms are subdued and put into perspective when traditional paradigms of analysis in the social sciences, engineering, or even the humanities reveal this "unique" thing to be a member of broader social categories with their own determinants and well-known laws of motion.

This general trajectory has been true for the Information Revolution as a whole.[2] The arc of understanding starts with an unhealthy dose of techno-determinism. As the report notes, "Over the course of Y2K it became clear that changes made to hardware and software generally did not address the central Y2K … issues."[3] The shift to a broader contextual focus on knowledge, management, and institutions, away from a more narrow hardware and software focus, is imperative for successful action, whether in Y2K or beyond. This experience underscores that more research is needed to understand and support individuals and organizations shifting from a techno-perspective to a strategic and managerial one.

Related examples from the safety field reinforce the hazards of treating large technological systems as consisting purely of technology. Consider the most notorious technology-heavy accidents of the past quarter-century: Three Mile Island and Chernobyl, the *Challenger* and *Columbia* shuttles, the USS *Vincennes,* and Bhopal. In

[1] Section 2.2 in the current draft.

[2] This perspective was provided by Professor Ernest Wilson of the University of Maryland.

[3] Section 2.3 in the current draft.

each case the accidents occurred despite the presence of sophisticated safety systems and devices, whose effectiveness in each case was cancelled out by social, managerial, and organizational issues. Similarly, computer-based automation of key safety tasks can paradoxically *increase* the risk of failure. An expert system introduced for aircraft maintenance at a leading airline saw a rise in mechanical problems, apparently because maintenance staff came to depend more on the system and less on their own experience, powers of observation, and personal initiative. When the software was changed to provide just information, not decisions—and even that only on request—quality again rose (Leveson).

The inextricably intertwined nature of software and organizational issues is not new, yet it is still not well understood, even after many decades. Thomas Hughes describes the development of the first large-scale real-time general purpose digital computer (SAGE, the first machine that we would recognize today as being a computer at all), observing that "system builders in the 1950s were learning that the managerial problems of large-scale projects loomed as large as engineering ones." Even in this early system, software development and project management became a prominent issue, as the number of programmers grew from a handful to more than 800, and as the programming group at the RAND almost outnumbered all other RAND employees. One striking recollection that Hughes relates is that "When we all began to work on SAGE, we believed our own myths about software—that one can do anything with software on a general-purpose computer, that software is easy to write, test, and maintain. …We had a lot to learn" (Bennington, as quoted in Hughes).

Cross-organizational issues during real-time operations played a key role in the buildup to the August 2003 blackout (see Section 3.7). Several IT problems triggered automated pages to the IT staff at the key Ohio utility (FirstEnergy). While the staff responded and thought they had restored full functionality, there was no communication between the IT staff and the control room operators. The IT personnel therefore did not know that some functionality had been restored to the immediately previous *defective* state, and control room personnel did not know that they were relying on out-of-date data or frozen systems (U.S.-Canada Power System Outage Task Force).

Y2K reminded organizations that the ultimate goal of IT is not the continued functioning of local clusters of technology but, rather, the effective use of information in support of strategic goals. Why does this horrific gap continue to persist, even as Y2K is viewed as a temporary blip? Will the lessons learned from Y2K have lasting effects (see Sec 2.7)? A critical issue was that temporary organizations and money were used to guide the Y2K effort, and as a result, no permanent homes were established for the arduously developed policy and practice. Nevertheless, there has been a historical trend in the direction of better alignment between mission objectives and IT, and Y2K helped this transition. The CIO offices that grew out of Y2K have expanded in their scope and mission, while new data standards make it far easier to share information (that is, data integration instead of application integration, as discussed in Section 2.3). SOAP, XML, message-oriented middleware, Enterprise JavaBeans, and similar standards focus on mission-critical data, both technically and managerially, helping to address integration and organizational issues. Still, considerable follow-up research is needed.

Y2K tells us that the Air Force, or any other IT-dependent organization, can mitigate risk by becoming more process based and less technology based. Process-based

tools focus on training people to do their jobs by providing procedures that mitigates risks. While the procedures are adopted at the enterprise-wide level, they can guide the creation of more specific, site-variant processes and desktop procedures that would mitigate the risk that uniformity might introduce. (As described earlier by an information warfare defense officer,[4] relying on one system could be a risk in itself.) If the right metrics are selected, this approach can also enable better tracking of the health of the organization as well as the IT infrastructure.. However, this approach must consider organizational and technology changes and the ongoing need to modify procedures and to continue learning.

The perspective that "built" or self-consciously designed systems need to fit harmoniously with their full context is not new (Alexander). Its transition from traditional fields such as architecture into supposedly modern fields like software engineering has been inconsistent: ironically, the more technologically sophisticated endeavor is undertaken with a more sociologically naive approach. The Air Force Y2K experience can be compared with current business writing on the important "people questions" to consider when executing a big software project. Representative of this category is Tom Demarco and Timothy Lister's *Peopleware: Productive Projects and Teams* (1999). The primary thesis in *Peopleware* is expressed as: "The major problems of [implementing large-scale IT systems] are not so much technological as sociological in nature." Demarco and his team have been studying failed software development since 1979, and "for the overwhelming majority of the bankrupt projects we studied, *there was not a single technological issue to explain the failure*." Rather, managerial, organizational, and other "people" issues are usually the underlying cause (Demarco and Lister).[5]

Clearly, the issues described in this report apply well beyond Y2K. Anyone who thinks they can carry out an IT project without thinking about organizational and social systems is heading for failure. As this report shows, it is essential to ask these questions, among others:

- What are the relationships with management and other organizations?
- What incentives are people responding to as the software is developed, deployed, and maintained?
- What are the different skill levels, needs, and assumptions of users, implementers, and supervisors?
- Who decides what's important?
- Who decides what gets done—when, and how?
- Who gets to contest those decisions?
- Who controls the resources needed to get it done?
- Who else is competing for those same resources?

These are the same questions facing a company planning to launch a new product, a local government planning an airport expansion, or a federal government planning a national incident management system.

[4] Section 4.2.2 in the current draft.

[5] Other well-known works that incorporate similar conclusions have been written by Hughes, Brooks, and Collins.

Certainly there is a need to understand specialized design and implementation issues and a need for skilled workers and expensive tools. But any IT-dependent organization also needs to understand its users (whether war fighters, customers, or random people impacted by a disaster) and to choose the right executives and management structure. They need to get all the relevant stakeholders on board before starting a major project. Just as a real estate developer needs to know what kinds of newly built communities will attract home buyers and sustain property values before they can succeed in the technical task of building houses, so the Air Force, faced with the Y2K threat, needed to look at its information and communication systems from the perspective of their use and evolution in an organizational context.

The Y2K experience helped introduce the Air Force and other technology-based organizations to a human, organizational, and social perspective on technology risk. The degree to which these organizations understand its repercussions and choose to act on that understanding is a key question for the future.

REFERENCES

Alexander, Christopher. 1964. Notes on the synthesis of form. Cambridge: Harvard University Press.

Ambrose, Brig. Gen. Gary A. 1999. Top 10 tips for handling Y2K. Air Force News. August 4.

Anderson, Mark C., Rajiv D. Banker, and Sury Ravindran. 2006. Value Implications of Investments in Information Technology. Management Science. 52(9): 1359–1376. September.

Ashton, Thomas V. 1998. Year 2000 certification: Air Force tenets to success. Crossfire: The Journal of Defense Software Engineering. August.

Barr, Stephen. 1997. "Year 2000" Report Flunks 3 Agencies, Lawmakers Urge Special Aide to Handle Looming Computer Problem. The Washington Post. September 16.

Bennington, Herbert D. 1983. Production of large computer programs. IEEE Annals of the History of Computing. 5(4): 350–361. October–December.

Benson, Robert L. 2001. The Venona Story. National Security Agency.

Bertalanffy, Ludwig Von. 1976. General System Theory: Foundations, Development, Applications. New York: George Braziller.

Brooks, Frederick. 1995. The mythical man-month: Essays on software engineering. Reading, Mass.: Addison-Wesley Publishing Company. 20th anniversary edition.

CCRP (Common Controls Replacement Project). 1999. CCRP Statement on Year 2000 Compliance. March.

Collins, James. 2001. Good to great: Why some companies make the leap–and others don't. New York: HarperBusiness.

Corcoran, Elizabeth. 1998. Inside Microsoft: An edgy, driven world. The Washington Post. October 18.

Davenport, Thomas H. 1997. Information Ecology: Mastering the Information and Knowledge Environment. New York: Oxford University Press USA.

Demarco, Tom, and Timothy Lister. 1999. Peopleware: Productive projects and teams. 2nd edition. New York: Dorset House Publishing Company.

EOP (Executive Office of the President). 1998a. Protecting America's Critical Infrastructure: Presidential Decision Directive 63. May 22.

EOP (Executive Office of the President). 1998b. White Paper: The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63. May 22.

FAC (Federal Acquisition Circular). 1997. FAC No. 97-01. August 22.

Farrell, Chris, Ochen Kaylan, and Catherine Winter. 2004. The Surprising Legacy of Y2K. Radio broadcast and website. American RadioWorks. Accessed online March 6, 2006 (http://americanradioworks.publicradio.org/features/y2k/index.html).

GAO (General Accounting Office). 2000. Year 2000 Computing Challenge: Lessons Learned Can Be Applied to Other Management Challenges. GAO/AIMD-00-290. September.

GAO (General Accounting Office). 1999. Defense Computers: DOD Y2K Functional End-to-End Testing Progress and Test Event Management (Letter Report). GAO/AIMD-00-12. October.

GAO (General Accounting Office). 1998a. Military Readiness: Reports to Congress Provide Few Details on Deficiencies and Solutions. GAO/NSIAD-98-68. March.

GAO (General Accounting Office). 1998b. Year 2000 Computing Crisis: Business Continuity and Contingency Planning. GAO/AIMD-10.1.19. August.

GAO (General Accounting Office). 1998c. Year 2000 Computing Crisis: A Testing Guide. GAO/AIMD-10.1.21. November.

GAO (General Accounting Office). 1997. Year 2000 Computing Crisis: An Assessment Guide. GAO/AIMD-10.1.14. September.

Gharajedaghi, Jamshid. 1999. Systems Thinking: Managing Chaos and Complexity. Oxford, United Kingdom: Butterworth-Heinemann.

Hughes, Thomas P. 1998. Rescuing Prometheus: Four monumental projects that changed the modern world. New York: Pantheon Books.

IEEE (Institute of Electrical and Electronics Engineers). 1999. Year 2000 Technical Information Statement. July 30.

IEEE (Institute of Electrical and Electronics Engineers). 1998. The Y2K date problem: A bad moon rising. The Institute. February.

Isaacs, Charles. 1999. The Value of Leveraging Y2K Inventory Information for Corporate Risk Management and Model-Based Contingency Planning. Information Systems Frontiers. 1:2 (163-172). August.

ITMRA (Information Technology Management Reform Act) of 1996. Pub. L. No. 104-106. Section 5125.

Kling, Rob. 1999. What Is Social Informatics and Why Does It Matter? D-Lib Magazine. 5:1. January. Accessed online March 6, 2007 (http://www.dlib.org/dlib/january99/kling/01kling.html).

Kling, Rob, and Walter Scacchi. 1982. The Web of Computing: Computer Technology as Social Organization. In Yovits, Marshall, editor, Advances in Computers, 21, 1–90. New York: Academic Press.

Leveson, Nancy G. 1994. High pressure steam engines and computers. IEEE Computer. 27(10): 65–73. October.

LMIS (Lockheed Martin Information Systems). 1999. Year 2000 Issues. Statement accessed on company website during 1999.

Malhotra, Yogesh. 1993. Role of Information Technology in Managing Organizational Change and Organizational Interdependence. Brint Institute. Accessed online May 18, 2006 (http://www.brint.com/papers/change/).

Marcoccia, Louis J. 1998. Building Infrastructure for Fixing the Year 2000 Bug: A Case Study. Journal of Software Maintenance: Research and Practice. 10(5): 333–325. September–October.

McCartney, Laton. 2001. Trends: Change agents. CIO Insight. May 1. Accessed online May 18, 2006 (http://www.cioinsight.com/article2/0,1397,1438214,00.asp).

Mercado, Rachel C. 1999. Yale–New Haven Hospital Remediation Plan: Medical Devices and the Year 2000. Journal of Clinical Engineering. 24(4): 16–22. July–August.

Mussington, David. 2002. Concepts for Enhancing Critical Infrastructure Protection: Relating Y2K to CIP Research and Development. Santa Monica, Calif.: RAND.

Newsweek. 1997. The day the world shuts down (cover story). June 2.

OMB (Office of Management and Budget). 1997. Year 2000 Interagency Committee Best Practices Guide. Draft document.

Ornstein, Robert E. 1975. The Psychology of Consciousness. Gretna, La.: Pelican Books.

Paterno, Fabiano, and Cristiano Mancini. 1998. Developing adaptable hypermedia. In Proceedings of the 4th international conference on intelligent user interfaces. New York: ACM Press.

PCCIP (President's Commission on Critical Infrastructure Protection). 1997. Critical Foundations: Protecting America's Infrastructures. Washington, DC: U.S. Government Printing Office. October.

Peters, F. Whitten. 2000. Remarks by the Secretary of the Air Force at the American Institute of Aeronautics and Astronautics International Global Air and Space 2000 Forum on Future Space in the Military. May 12.

QLogic Corporation. 1999. Y2K compliance statement, Version 1.1. Accessed on company website during 1999.

Rosenberg, Eric. 2001. Studies of Gulf War reveal U.S. military deficiencies. Seattle Post-Intelligencer. January 18.

SAGE. 2006. SAGE website. Accessed online May 14, 2006 (http://www.sage.org/field/).

SAGE. 2000. SAGE System Administrator Salary Profile 1999. Berkeley, Calif.

Standish Group. 1994. The chaos report. West Yarmouth, Mass. Accessed online May 18, 2006 (http://www.standishgroup.com/sample_research/chaos_1994_1.php).

USAF (United States Air Force). 2000a. Air Force Year 2000 Final Report.

USAF (United States Air Force). 2000b. Global vigilance reach & power: America's Air Force Vision 2020. Washington, DC.

USAF (United States Air Force). 2000c. Air Force Policy Letter Digest. April.

USAF (United States Air Force). 1999a. Air Force Critical Infrastructure Program, Air Force Policy Directive 10-24. December 1.

USAF (United States Air Force). 1999b. Air Force Assessment Master Plan for Operations in the Year 2000. May 15.

USAF (United States Air Force). 1997. Air Force Communications Agency Year 2000 Guidance Package. April 1.

U.S.-Canada Power System Outage Task Force. 2004. Final Report on the August 14, 2003, Blackout in the United States and Canada: Causes and Recommendations. April.

USA Today Tech Report. 1997. For some computers 2000 will never come. August 22.

Weill, Peter, and Marianne Broadbent. 1998. Leveraging the New Infrastructure. Boston, Mass.: Harvard Business School Press.

Weinraub, Mark. 2001. NASDAQ fixes system but traders struggle. Reuters. July 2.

Wick, Corey. 2000. Knowledge management and leadership opportunities for technical communicators. Technical Communication. 47(4): 515–529. November.

Y2K Act. 1999. Pub. L. No. 106-37.

APPENDIX A: REFERENCES TO WORKSHOP DISCUSSIONS AND INTERVIEWS

The study process involved several interview sessions and a workshop aimed at gathering perspectives and lessons learned from the Air Force's Y2K response effort. These sessions were held as follows:

Interviews at Yokota Air Base (Japan), November 29–December 3, 1999
Interviews at Scott Air Force Base (Illinois), December 13–15, 1999
Interviews at Scott Air Force Base (Illinois), February 24–25, 2000
Interviews at Yokota Air Base (Japan), March 13, 2000
Air Force Y2K Lessons Learned Workshop (Washington, DC), April 14, 2000

This report draws extensively on quotations and other information from the workshop and interview sessions. Rather than use actual names in the citations, abbreviations of the organizational affiliations of speakers are given. This is a key of the cited organizational affiliations.

374th AW	374th Airlift Wing (Yokota Air Base, Japan)
374th AW/CES	374th Airlift Wing, Civil Engineering Squadron
374th AW/CS	374th Airlift Wing Communications Squadron
374th AW/LG	374th Airlift Wing Logistics Group
374th AW/OG	374th Airlift Wing Operations Group
374th AW/SC	374th Airlift Wing Systems and Computers
374th AW/XP	374th Airlift Wing Plans and Programs
375th AW	375th Airlift Wing (Scott Air Force Base, Illinois)
375th AW/CE	375th Airlift Wing, Civil Engineering
375th AW/CG	375th Airlift Wing Communications Group
375th AW/MDG	375th Airlift Wing Medical Group
375th AW/NCC	375th Airlift Wing Network Control Center
375th AW/Y2K	375th Air Wing Y2K Program Office
630th AMSS	630th Air Mobility Support Squadron (component of 374th AW)

ACC	Air Combat Command
AFCA	Air Force Communications Agency
AFCIC/SY	Air Force Communications and Information Center
AF/XOIWD	Air Force Director of Intelligence, Reconnaissance and Surveillance, Defensive Information Warfare Division
AMC/HQ	Air Mobility Command Headquarters
AMC/SCA	Air Mobility Command/Support Center Atlantic
AMC/SCP	Air Mobility Command/Support Center Pacific
Cheyenne Mountain	Cheyenne Mountain Operations Center
HQ/SC	Headquarters United States Air Force Deputy Chief of Staff for Communications and Information
MITRE	MITRE Corporation
MSG	Materiel Systems Group
SAF/AQ	Secretary of the Air Force, Acquisitions
SSG	Standard Systems Group
USFJ	United States Forces Japan

APPENDIX B: ABBREVIATIONS AND ACRONYMS

ACC	Air Combat Command
AEF	Aerospace Expeditionary Force
AFASI	Air Force All Systems Inventory
AFB	Air Force Base
AFCA	Air Force Communications Agency
AFCERT	Air Force Computer Emergency Response Team
AFCERTS	Air Force Certified Software Changes
AFCIC	Air Force Communications and Information Center
AFED	Air Force Evaluation Database
AFMC	Air Force Materiel Command
AFY2KO	Air Force Y2K Office
AMC	Air Materiel Command
AWACS	Airborne Warning and Control System
BIOS	Basic Integrated Operating System
CCRP	Continuously Computed Release Point
C2IPS	Command and Control Information Processing System
CDA	Central Design Activity
CETL	Communications Environment Test Laboratory
CINC	Commander in Chief
CIO	Chief Information Officer
CIP	Critical infrastructure protection
CKO	Chief Knowledge Officer

CMOS	Cargo Movement Operation System
COMS	Communications squadron
CONUS	Continental United States
COOP	Continuity of operations plan
COTS	Commercial off-the-shelf
DISA	Defense Information Systems Agency
DMS	Defense Messaging System (a DOD-led initiative to establish secure e-mail throughout the department)
DTS	Defense Travel System
ESC	Electronic Systems Center
FAR	Federal Acquisition Requirements
FIPS	Federal Information Processing Standards
Fusion Center	Operated by SSG, it monitors information relevant to information warfare attacks and other systems crises
GAO Office)	General Accounting Office (now the Government Accountability
GATES	Global Air Transportation Execution System
ICT	Information and communications technology
IEEE	Institute of Electrical and Electronics Engineers
IMPAC	International Merchant Purchase Authorization Card
IT	Information technology
IWD	Information Warfare Defense
JACAL	An interactive, symbolic mathematics program
MAJCOMs	Major commands

MSG	Material Systems Group
NCC	Network Control Center
NRC	National Research Council
OCONUS	Outside the continental United States
OPTN	Operationalizing and Professionalizing the Network
ORM	Operational risk management
PACAF	Pacific Command
PDD	Presidential Decision Directive
PMO	Program Management Office
POC	Point of contact
SA	System administrator
SBSS	Standard Base Supply System
SC community	Systems and computing units
SPO	System Program Office
SSG	Standard Systems Group
TDY	Temporary Duty
USFJ	U.S. joint services in Japan
USTRANSCOM	U.S. Transportation Command

APPENDIX C: BIOGRAPHICAL INFORMATION ON THE PRINCIPAL INVESTIGATOR

Mark P. Haselkorn is Professor and Founding Chair (1985–97) of the Department of Technical Communication in the College of Engineering at the University of Washington. He has more than two decades of leadership in interdisciplinary technology areas such as assessment of information technology in organizations, design of electronic communities and online services, and management of knowledge and communication in large organizations. Dr. Haselkorn is also the Co-Director of the University of Washington's Interdisciplinary Program in Humanitarian Relief and a Research Scientist for the Veterans Health Administration. He currently leads an NSF-supported initiative on the emerging research frontier of "Humanitarian Service Science & Engineering," conducts research on the integration of DOD and VA electronic medical records, and, before Y2K, conducted foundational research in the area of intelligent transportation systems, including development of the first Web-based real-time traveler information system (*Traffic Reporter*, 1990). He received his Ph.D. in English Language, M.A. in Computational Linguistics, and M.A. in English from the University of Michigan.