[Please copy and distribute]

The Year 2000: Social Chaos or Social Transformation?

by

John L. Petersen, Margaret Wheatley, Myron Kellner-Rogers

The Millenial sun will first rise over human civilization in the independent republic of Kiribati, a group of some thirty low lying coral islands in the Pacific Ocean that straddle the equator and the International Date Line, halfway between Hawaii and Australia. This long awaited sunrise marks the dawn of the year 2000, and quite possibly, the onset of unheralded disruptions in life as we know it in many parts of the globe. Kiribati's 81,000 Micronesians may observe nothing different about this dawn; they only received TV in 1989. However, for those who live in a world that relies on satellites, air, rail and ground transportation, manufacturing plants, electricity, heat, telephones, or TV, when the calendar clicks from '99 to '00, we will experience a true millennial shift. As the sun moves westward on January 1, 2000, as the date shifts silently within millions of computerized systems, we will begin to experience our computer-dependent world in an entirely new way. We will finally see the extent of the networked and interdependent processes we have created. At the stroke of midnight, the new millenium heralds the greatest challenge to modern society we have yet to face as a planetary community. Whether we experience this as chaos or social transformation will be influenced by what we do immediately.

We are describing the year 2000 problem, known as Y2K (K signifying 1000.) Nicknamed at first "The Millennial Bug," increasing sensitivity to the magnitude of the impending crisis has escalated it to "The Millennial Bomb." The problem begins as a simple technical error. Large mainframe computers more than ten years old were not programmed to handle a four digit year. Sitting here now, on the threshold of the year 2000, it seems incomprehensible that computer programmers and microchip designers didn't plan for it. But when these billions of lines of computer code were being written, computer memory was very expensive. Remember when a computer only had 16 kilobytes of RAM? To save storage space, most programmers allocated only two digits to a year. 1993 is '93' in data files, 1917 is '17.' These two-digit dates exist on millions of files used as input to millions of applications. (The era in which this code was written was described by one programming veteran as “the Wild West.” Programmers did whatever was required to get a product up and working; no one even thought about standards.)

The same thing happened in the production of microchips as recently as three years ago. Microprocessors and other integrated circuits are often just sophisticated calculators that count and do math. They count many things: fractions of seconds, days, inches, pounds, degrees, lumens, etc. Many chips that had a time function designed into them were only structured for this century. And when the date goes from '99 to '00 both they and the legacy software that has not been fixed will think it is still the 20th century -- not 2000, but 1900.

Peter de Jager, who has been actively studying the problem and its implications since 1991, explains the computer math calculation: “I was born in 1955. If I ask the computer to calculate how old I am today, it subtracts 55 from 98 and announces that I’m 43. . . But what happens in the year 2000? The computer will subtract 55 from 00 and will state that I am *minus 55 years old*. This error will affect any calculation that produces or uses time spans. . . . If you want to sort by date (e.g., 1965, 1905, 1966), the resulting sequence would be 1905, 1965, 1966. However, if you add in a date record such as 2015, the computer, which reads only the last two digits of the date, sees 05, 15, 65, 66 and sorts them incorrectly. These are just two types of calculations that are going to produce garbage.”[1]

The calculation problem explains why the computer system at Marks & Spencer department store in London recently destroyed tons of food during the process of doing a long term forecast. The computer read 2002 as 1902. Instead of four more years of shelf life, the computer calculated that this food was ninety-six years old. It ordered it thrown out.[2] A similar problem happened recently in the U.S. at the warehouse of a freeze dried food manufacturer.

But Y2K is not about wasting good food. Date calculations affect millions more systems than those that deal with inventories, interest rates, or insurance policies. Every major aspect of our modern infrastructure has systems and equipment that rely on such calculations to perform their functions. We are dependent on computerized systems that contain date functions to effectively manage defense, transportation, power generation, manufacturing, telecommunications, finance, government, education, healthcare. The list is longer, but the

[1] See Peter de Jager, www.year2000.com

[2] United Airlines, Flight Talk Network, February 1998

picture is clear. We have created a world whose efficient functioning in all but the poorest and remotest areas is dependent on computers. It doesn't matter whether you personally use a computer, or that most people around the world don't even have telephones. The world's economic and political infrastructures rely on computers. And not isolated computers. We have created dense networks of reliance around the globe. We are networked together for economic and political purposes. Whatever happens in one part of the network has an impact on other parts of the network. *We have created not only a computer-dependent society, but an interdependent planet.*

We already have frequent experiences with how fragile these systems are, and how failure cascades through a networked system. While each of these systems relies on millions of lines of code that detail the required processing, they handle their routines in serial fashion. Any next step depends on the preceding step. This serial nature makes systems, no matter their size, vulnerable to even the slightest problem anywhere in the system. In 1990, ATT's long distance system experienced repeated failures. At that time, it took two million lines of computer code to keep the system operational. But these millions of lines of code were brought down by just three lines of faulty code.

And these systems are lean; redundancies are eliminated in the name of efficiency. This leanness also makes the system highly vulnerable. In May of this year, 90% of all pagers in the U.S. crashed for a day or longer because of the failure of one satellite. Late in 1997, the Internet could not deliver email to the appropriate addresses because bad information from their one and only central source corrupted their servers.

Compounding the fragility of these systems is the fact that we can't see the extent of our interconnectedness. The networks that make modern life possible are masked by the technology. We only see the interdependencies when the relationships are disrupted -- when a problem develops elsewhere and we notice that we too are having problems. When Asian markets failed last year, most U.S. businesses denied it would have much of an impact on our economy. Only recently have we felt the extent to which Asian economic woes affect us directly. Failure in one part of a system always exposes the levels of interconnectedness that otherwise go unnoticed—we suddenly see how our fates are linked together. We see how much we are participating with one another, sustaining one another.

Modern business is completely reliant on networks. Companies have vendors, suppliers, customers, outsourcers (all, of course, managed by computerized data bases.) For Y2K, these highly networked ways of doing business create a terrifying scenario. *The networks mean that no one system can protect itself from Y2K failures by just attending to its own internal systems*. General Motors, which has been working with extraordinary focus and diligence to bring their manufacturing plants up to Year 2000 compliance, (based on their assessment that they were facing catastrophe,) has 100,000 suppliers worldwide. Bringing their internal systems into compliance seems nearly impossible, but what then do they do with all those vendors who supply parts? GM experiences production stoppages whenever one key supplier goes on strike. What is the potential number of delays and shutdowns possible among 100,000 suppliers?

The nature of systems and our history with them paints a chilling picture of the Year 2000. We do not know the extent of the failures, or how we will be affected by them. But we do know with great certainty that as computers around the globe respond or fail when their calendars record 2000, we will see clearly the extent of our interdependence. We will see the ways in which we have woven the modern world together through our technology.

What, me worry?

Until quite recently, it's been difficult to interest most people in the Year 2000 problem. Those who are publicizing the problem (the Worldwide Web is the source of the most extensive information on Y2K,) exclaim about the general lack of awareness, or even the deliberate blindness that greets them. In our own investigation among many varieties of organizations and citizens, we've noted two general categories of response. In the first category, people acknowledge the problem but view it as restricted to a small number of businesses, or a limited number of consequences. People believe that Y2K affects only a few industries—primarily finance and insurance—seemingly because they deal with dates on policies and accounts. Others note that their organization *is* affected by Y2K, but still view it as a well-circumscribed issue that is being addressed by their information technology department. What's common to these comments is that people hold Y2K as a narrowly-focused, bounded problem. They seem oblivious to the networks in which they participate, or to the systems and interconnections of modern life.

The second category of reactions reveals the great collective faith in technology and science. People describe Y2K as a technical problem, and then enthusiastically state that human ingenuity and genius always finds a way to solve these type of problems. Ecologist David Orr has noted that one of the fundamental beliefs of our time is that technology can be trusted to solve any problem it creates.[3] If a software engineer goes on TV claiming to have created a program that can correct all systems, he is believed. After all, he's just what we've been expecting.

And then there is the uniqueness of the Year 2000 problem. At no other time in history have we been forced to deal with a deadline that is absolutely non-negotiable. In the past, we could always hope for a last minute deal, or rely on round-the-clock bargaining, or pray for an eleventh hour savior. We have never had to stare into the future knowing the precise date when the crisis would materialize. In a bizarre fashion, the inevitability of this confrontation seems to add to people's denial of it. They know the date when the extent of the problem will surface, and choose not to worry about it until then.

However, this denial is quickly dissipating. Information on Y2K is expanding exponentially, matched by an escalation in adjectives used to describe it. More public figures are speaking out. This is critically important. With each calendar tick of this time, alternatives diminish and potential problems grow. We must develop strategies for preparing ourselves at all levels to deal with whatever Y2K presents to us with the millennium dawn.

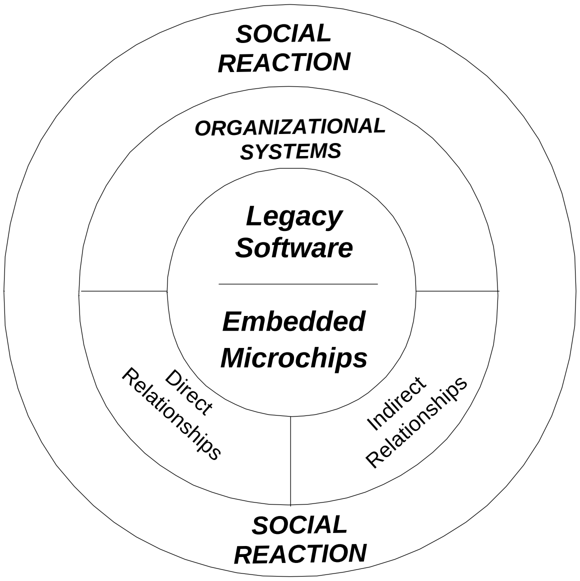
What we know about Y2K

- a technological problem that cannot be solved by technology
- the first-ever, non-negotiable deadline
- a systemic crisis that no one can solve alone
- a crisis that transcends boundaries and hierarchies
- an opportunity to evoke greater capacity from individuals and organizations
- an opportunity to simplify and redesign major systems

[3] "Slow Knowledge," _______1997.

The Y2K problem, really

We'd like to describe in greater detail the extent of Y2K. As a global network of interrelated consequences, it begins at the center with the technical problem, legacy computer codes and embedded microchips. (see Figure One) For the last thirty years thousands of programmers have been writing billions of lines of software code for the computers on which the world's economy and society now depend. Y2K reporter Ed Meagher describes "old, undocumented code written in over 2500 different computer languages and executed on thousands of different hardware platforms being controlled by hundreds of different operating systems . . . [that generate] further complexity in the form of billions of six character date fields stored in millions of databases that are used in calculations."[4] The Gartner Group, a computer-industry research group, estimates that globally, 180 billion lines of software code will have to be screened.[5] Peter de Jager notes that it is not unusual for a company to have more than 100,000,000 lines of code--the IRS, for instance, has at least eighty million lines. The Social Security Administration began working on its thirty million lines of code in 1991. After five years of work, in June, 1996, four hundred programmers had fixed only six million lines. The IRS has 88,000 programs on 80 mainframe computers to debug. By the end of last year they had



[4] See "The Complexity Factor" by Ed Meagher at www.year2000.com/archive/NFcomplexity.html
[5] **"**Industry Wakes Up to the Year 2000 Menace," FORTUNE, April 27, 1998

cleaned up 2,000 programs.[6] Capers Jones, head of Software Productivity Research, a firm that tracks programmer productivity, estimates that finding, fixing and testing all Y2K-affected software would require over 700,000 person-*years.*[7] Programmers have been brought out of retirement and are receiving extraordinary wages and benefits to stick with this problem, but we are out of time. There aren't nearly enough programmers nor hours remaining before January 1, 2000.

Also at the center of this technical time bomb are the embedded microprocessors. There are somewhat over a billion of these hardware chips located in systems worldwide. They sustain the world's manufacturing and engineering base. They exist in traffic lights, elevators, water, gas, and electricity control systems. They're in medical equipment and military and navigation systems. America's air traffic control system is dependent upon them. They're located in the track beds of railroad systems and in the satellites that circle the earth. Global telecommunications are heavily dependent on them. Modern cars contain about two dozen microprocessors. The average American comes in contact with seventy microprocessors before noon every day. Many of these chips aren't date sensitive, but a great number are, and engineers looking at long ago installed systems don't know for sure which is which. To complicate things further, not all chips behave the same. Recent tests have shown that two chips of the same model installed in two different computers but performing the same function are not equally sensitive to the year-end problem. One shuts down and the other doesn't.

It is impossible to locate all of these chips in the remaining months, nor can we replace all those that are identified. Those more than three years old are obsolete and are probably not available in the marketplace. The solution in those cases is to redesign and remanufacture that part of the system -- which often makes starting over with new equipment the best option. That is why some companies are junking their computer systems and spending millions, even hundreds of millions, to replace everything. It at least ensures that their internal systems work.

At issue is time, people, money, and the nature of systems. These technical problems are exacerbated by government and business leaders who haven't yet fully understood the potential significance of this issue for their own companies, to say nothing of the greater economic implications. The U.S. leads all other developed nations in addressing this issue, minimally by

[6] The Washington Post, "If Computer Geeks Desert, IRS Codes Will Be ciphers," December 24, 1997
[7] Business Week, March 2, 1998

six to nine months. Yet in a recent survey of American corporate chief information officers, 70% of them expressed the belief that even their companies would not be completely prepared for Y2K. Additionally, 50% of them acknowledged that they would not fly during January 2000. If America is the global leader in Y2K efforts, these CIO comments are indeed sobering.

The economic impacts for the global economy are enormous and unknown. The Gartner Group projects that the total cost of dealing with Y2K worldwide will be somewhere between $300 billion to $600 billion -- and these are only direct costs associated with trying to remedy the problem. (These estimates keep rising every quarter now.) The Office of Management and Budget (OMB), in a recently released Quarterly Report, estimated total government Y2K expense at $3.9 billion. This figure was based only on federal agency estimates; the OMB warned that this estimate might be as much as *90% too low* considering the increasing labor shortage and expected growing remediation costs as January 1, 2000 looms nearer. And in June of this year, it was announced that federal agencies had already spent five billion dollars. Of twenty-four agencies, fifteen reported being behind schedule.

These numbers don't consider the loss of output caused by diverting resources to forestall this crisis. In more and more businesses, expenditures for R&D and modernization are being diverted to Y2K budgets. *Business Week* in March of 1998 estimated that the Year 2000 economic damage alone would be $119 billion. When potential lawsuits and secondary effects are added to this -- people suing over everything from stalled elevators to malfunctioning nuclear power plants -- the cost easily could be over $1 trillion.

But these problems and estimates don’t begin to account for the potential impact of Y2K. The larger significance of this bomb becomes apparent when we consider the next circle of the global network-- the organizational relationships that technology makes possible.

Who works with whom?

The global economy is dependent upon computers both directly and indirectly. Whether it’s your PC at home, the workstation on a local area network, or the GPS or mobile telephone that you carry, all are integral parts of larger networks where computers are directly connected together. As we’ve learned, failure in a single component can crash the whole system; that system could be an automobile, a train, an aircraft, an electric power plant, a bank, a government agency, a stock exchange, an international telephone system, the air traffic control system. If every possible date-sensitive hardware and software bug hasn't been fixed in a larger system, just one programming glitch or one isolated chip *potentially* can bring down the whole thing.

While there isn't enough time or technical people to solve the Y2K problem before the end of next year, we might hope that critical aspects of our infrastructure are tackling this problem with extreme diligence. But this isn't true. America's electric power industry is in danger of massive failures, as described in *Business Week's* February '98 cover story on Y2K. They report that "electric utilities are only now becoming aware that programmable controllers -- which have replaced mechanical relays in virtually all electricity-generating plants and control rooms -- may behave badly or even freeze up when 2000 arrives. Many utilities are just getting a handle on the problem." It's not only nuclear power plants that are the source of concern, although problems there are scary enough. In one Year 2000 test, notes Jared S.Wermiel, leader of the Y2K effort at the Nuclear Regulatory Commission, the security computer at a nuclear power plant failed by opening vital areas that are normally locked. Given the complexity and the need to test, "it wouldn't surprise me if certain plants find that they are not Year 2000-ready and have to shut down."[8]

Other electric utility analysts paint a bleaker picture. Rick Cowles, who reports on the electric utility industry, said at the end of February: "Not one electric company [that he had talked to] has started a serious remediation effort on its embedded controls. Not one. Yes, there's been some testing going on, and a few pilot projects here and there, but for the most part it is still business-as-usual, as if there were 97 months to go, not 97 weeks.[9] After attending one industry trade show, Cowle stated that, "Based on what I learned at DistribuTECH '98, I am convinced there is a 100% chance that a major portion of the domestic electrical infrastructure will be lost as a result of the Year 2000 computer and embedded systems problem. The industry is fiddling whilst the infrastructure burns." [10]

The Federal Aviation Administration is also very vulnerable but quite optimistic. "We're on one hand working to get those computers Year 2000 compliant, but at the same time we're working on replacing those computers," said Paul Takemoto, a spokesman for the FAA in early '98. At the twenty Air Route Traffic Control Centers, there is a host computer and a backup system. All forty of these machines --mid-'80s vintage IBM 3083 mainframes--are affected.

[8] www.igs.net/~tonyc/y2kbusweek.html
[9] "Industry Gridlock," Rick Cowles, February 27, 1998, www.y2ktimebomb.com/PP/RC/rc9808.htm
[10] Cowles, January 23, 1998, ibid www site

And then there are the satellites with embedded chips, individual systems in each airplane, and air traffic control systems around the globe. Lufthansa already has announced it will not fly its aircraft during the first days of 2000.

Who else is affected?

But the interdependency problem extends far beyond single businesses, or even entire industries. Indirect relationships extend like tentacles into many other networks, creating the potential for massive disruptions of service.

Let's hope that your work organization spends a great deal of money and time to get its entire information system compliant. You *know* yours is going to function. But on the second of January 2000 the phone calls start. It's your banker. "There's been a problem," he says. They've lost access to your account information and until they solve the problem and get the backup loaded on the new system, they are unable to process your payroll. "We don't have any idea how long it will take," the president says.

Then someone tells you that on the news there's a story that that the whole IRS is down and that they can neither accept nor process tax information. Social Security, Federal Housing, Welfare—none of these agencies are capable of issuing checks for the foreseeable future. Major airlines aren't flying, waiting to see if there is still integrity in the air traffic control system. And manufacturing across the country is screeching to a halt because of failures in their supply chain. (After years of developing just in time (JIT) systems, there is no inventory on hand—suppliers have been required to deliver parts as needed. There is no slack in these systems to tolerate even minor delivery problems.) Ground and rail transport have been disrupted, and food shortages appear within three to six days in major metropolises. Hospitals, dealing with the failure of medical equipment, and the loss of shipments of medicine, are forced to deny non-essential treatment, and in some cases are providing essential care in pre-technical ways.

It's a rolling wave of interdependent failures. And it reaches across the country and the world to touch people who, in most cases, didn't know they were linked to others. Depending on what systems fail, very few but strategically placed failures would initiate a major economic cascade. Just problems with power companies and phone systems alone would cause real havoc. (This spring, a problem in ATT rendered all credit card machines useless for a day. How much revenue was lost by businesses?) If only twenty percent of businesses and government agencies crash at the same time, major failures would ensue.

In an interdependent system, solving *most of* the problem is no solution. As Y2K reporter Ed Meagher describes:

> It is not enough to solve simply "most of these problems." The integration of these systems requires that we solve virtually all of them. Our ability as an economy and as a society to deal with disruptions and breakdowns in our critical systems is minuscule. Our worst case scenarios have never envisioned multiple, parallel systemic failures. Just in time inventory has led to just in time provisioning. Costs have been squeezed out of all of our critical infrastructure systems repeatedly over time based on the ubiquity and reliability of these integrated systems. The human factor, found costly, slow, and less reliable has been purged over time from our systems. Single, simple failures can be dealt with; complex, multiple failures have been considered too remote a possibility and therefore too expensive to plan for. [11]

The city of New York began to understand this last September. The governor of New York State banned all nonessential IT projects to minimize the disruption caused by the year 2000 bomb after reading a detailed report that forecasts the millennium will throw New York City into chaos, with power supplies, schools, hospitals, transport, and the finance sector likely to suffer severe disruption. Compounding the city's Y2K risks is the recent departure of the head of its year 2000 project to a job in the private sector.[12]

But of course the anticipated problems extend far beyond U.S. shores. In February, the *Bangkok Post* reported that Phillip Dodd, a Unysis Y2K expert, expects that upward of 70% of the businesses in Asia will fail outright or experience severe hardship because of Y2K. The Central Intelligence Agency supports this with their own analysis: "We're concerned about the potential disruption of power grids, telecommunications and banking services, among other possible fallout, especially in countries already torn by political tensions."[13]

A growing number of assessments of this kind have led Dr. Edward Yardeni, the chief economist of Deutsche Morgan Grenfell, to keep raising the probability of a deep global

[11] The Complexity Factor, Ed Meagher
[12] www.computerweekly.co.uk/news/ll_9_97
[13] REUTER "CIA:Year 2000 to hit basic services: Agency warns that many nations aren't ready for disruption," Jim Wolf, May 7, 1998

recession in 2000-2001 as the result of Y2K. His present estimate of the potential for such a recession now hovers at about 70%, up from 40% at the end of 1997.[14]

How might we respond?

As individuals, nations, and as a global society, do we have a choice as to how we might respond to Y2K, however problems materialize? The question of alternative social responses lies at the outer edges of the interlocking circles of technology and system relationships. At present, potential societal reactions receive almost no attention. But we firmly believe that it is the central most important place to focus public attention and individual ingenuity. *Y2K is a technology-induced problem, but it will not and cannot be solved by technology. It creates societal problems that can only be solved by humans.* We must begin to address potential social responses. We need to be engaged in this discourse within our organizations, our communities, and across the traditional boundaries of competition and national borders. Without such planning, we will slide into the Year 2000 as hapless victims of our technology.

Even where there is some recognition of the potential disruptions or chaos that Y2K might create, there's a powerful dynamic of secrecy preventing us from engaging in these conversations. Leaders don't want to panic their citizens. Employees don't want to panic their bosses. Corporations don't want to panic investors. Lawyers don't want their clients to confess to anything. But as psychotherapist and information systems consultant Dr. Douglass Carmichael has written:

> Those who want to hush the problem ("Don't talk about it, people will panic", and "We don't know for sure.") are having three effects. First, they are preventing a more rigorous investigation of the extent of the problem. Second, they are slowing down the awareness of the intensity of the problem as currently understood and the urgency of the need for solutions, given the current assessment of the risks. Third, they are making almost certain a higher degree of ultimate panic, in anger, under conditions of shock.[15]

Haven't we yet learned the consequences of secrecy? When people are kept in the dark, or fed misleading information, their confidence in leaders quickly erodes. In the absence of real

[14] see www.Yardeni.com

[15] www.tmn.com/~doug

information, people fill the information vacuum with rumors and fear. And whenever we feel excluded, we have no choice but to withdraw and focus on self-protective measures. As the veil of secrecy thickens, the capacity for public discourse and shared participation in solution-finding disappears. People no longer believe anything or anybody—we become unavailable, distrusting and focused only on self-preservation. Our history with the problems created by secrecy has led CEO Norman Augustine to advise leaders in crisis to: "Tell the truth and tell it fast."[16]

Behaviors induced by secrecy are not the only human responses available. Time and again we observe a much more positive human response during times of crisis. When an earthquake strikes, or a bomb goes off, or a flood or fire destroys a community, people respond with astonishing capacity and effectiveness. They use any available materials to save and rescue, they perform acts of pure altruism, they open their homes to one another, they finally learn who their neighbors are. We've interviewed many people who participated in the aftermath of a disaster, and as they report on their experiences, it is clear that their participation changed their lives. They discovered new capacities in themselves and in their communities. They exceeded all expectations. They were surrounded by feats of caring and courage. They contributed to getting systems restored with a speed that defied all estimates.

When chaos strikes, there's simply no time for secrecy; leaders have no choice but to engage every willing soul. And the field for improvisation is wide open—no emergency preparedness drill ever prepares people for what they actually end up doing. Individual initiative and involvement are essential. Yet surprisingly, in the midst of conditions of devastation and fear, people report how good they feel about themselves and their colleagues. *These crisis experiences are memorable because the best of us becomes visible and available*. We've observed this in America, and in Bangladesh, where the poorest of the poor responded to the needs of their most destitute neighbors rather than accepting relief for themselves.

[16] "Managing the Crisis You Tried to Prevent," *Harvard Business Review*, Nov-Dec. 1995, 158.

What we know about people in crisis

- shared purpose and meaning brings people together
- people display unparalleled levels of creativity and resourcefulness
- people want to help others - individual agendas fade immediately
- people learn instantly and respond at lightning speed
- the more information people get, the smarter their responses
- leadership behaviors (not roles) appear everywhere, as needed
- people experiment constantly to find what works

Who might we become?

As we sit staring into the unknown dimensions of a global crisis whose timing is non-negotiable, what responses are available to us as a human community? An effective way to explore this question is to develop potential scenarios of possible social behaviors. Scenario planning is an increasingly accepted technique for identifying the spectrum of possible futures that are most important to an organization or society. In selecting among many possible futures, it is most useful to look at those that account for the greatest uncertainty and the greatest impact. For Y2K, David Isenberg, (a former AT&T telecommunications expert, now at Isen.Com) has

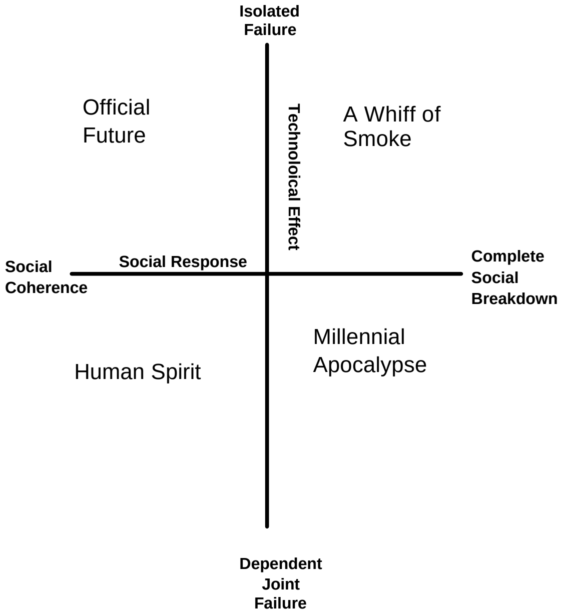


Figure 2

identified the two variables which seem obvious – the range of technical failures from isolated to multiple, and the potential social responses, from chaos to coherence. Both variables are critical and uncertain and are arrayed as a pair of crossing axes, as shown in Figure 2. When displayed in this way, four different general futures emerge. In the upper left quadrant, if technical failures are isolated and society doesn't respond to those, nothing of significance will happen. Isenberg labels this the "*Official Future*" because it reflects present behavior on the part of leaders and organizations.

The upper right quadrant describes a time where technical failures are still isolated, but the public responds to these with panic, perhaps fanned by the media or by stonewalling leaders. Termed "*A Whiff of Smoke,*" the situation is analogous to the panic caused in a theater by someone who smells smoke and spreads an alarm, even though it is discovered that there is no fire. This world could evolve from a press report that fans the flames of panic over what starts as a minor credit card glitch (for example), and, fueled by rumors turns nothing into a major social problem with runs on banks, etc.

The lower quadrants describe far more negative scenarios. "*Millennial Apocalypse*" presumes large-scale technical failure coupled with social breakdown as the organizational, political and economic systems come apart. The lower left quadrant, "*Human Spirit*" posits a society that, in the face of clear adversity, calls on each of us to collaborate in solving the problems of breakdown.

Since essentially we are out of time and resources for preventing widespread Y2K failures, a growing number of observers believe that the only plausible future scenarios worth contemplating are those in the lower half of the matrix. The major question before us is how will society respond to what is almost certain to be widespread and cascading technological failures?

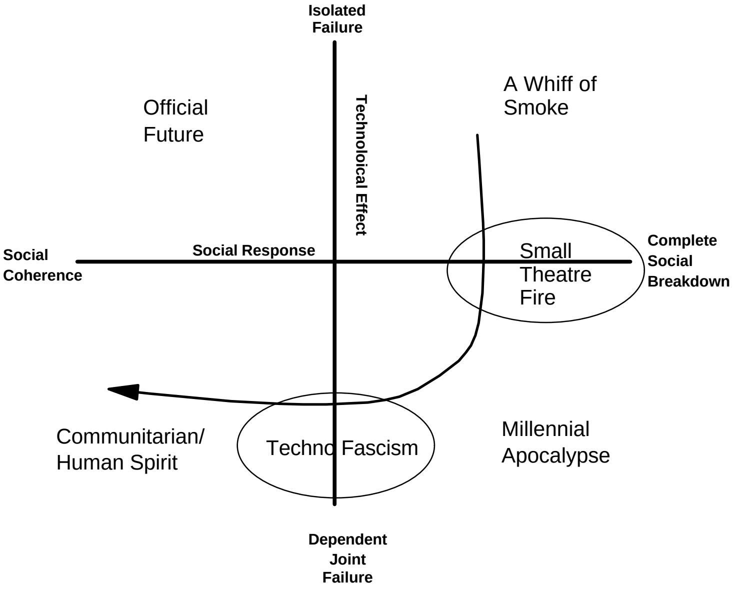


Figure 3

Figure 3 above shows a possible natural evolution of the problem. Early, perhaps even in ’98, the press could start something bad long before it was clear how serious the problem was and how society would react to it. There could be an interim scenario where a serious technical problem turned into a major social problem from lack of adaquate positive social response. This “Small Theatre Fire” future could be the kind of situation where people overreact and trample themselves trying to get to the exits from a small fire that is routinely extinguished.

If the technical situation is bad, a somewhat more ominous situation could evolve where government, exerting no clear positive leadership and seeing no alternative to chaos, cracks down so as not to lose control (A common historical response to social chaos has been for the government to intervene in non-democratic, sometimes brutal fashion. “Techno-fascism” is a plausible scenario -- governments and large corporations would intervene to try to contain the damage -- rather than build for the future. This dictatorial approach would be accompanied by secrecy about the real extent of the problem and ultimately fueled by the cries of distress, prior to 2000, from a society that has realized its major systems are about to fail and that it is too late to do anything about it.

Collaboration is our only choice

Obviously, the scenario worth working towards is “Human Spirit,” a world where the best of human creativity is enabled and the highest common good becomes the objective. In this world we all work together, developing a very broad, powerful, synergistic, self-organizing force focused on determining what humanity should be doing in the next 18 months to plan for the aftermath of the down stroke of Y2K. This requires that we understand Y2K not as a technical problem, but as a systemic, worldwide event that can only be resolved by new social relationships. All of us need to become very wise and very engaged very fast and develop entirely new processes for working together. Systems issues cannot be resolved by hiding behind traditional boundaries or by clinging to competitive strategies. Systems require collaboration and the dissolution of existing boundaries. Our only hope for healthy responses to Y2K-induced failures is to participate together in new collaborative relationships.

At present, individuals and organizations are being encouraged to protect themselves, to focus on solving "their" problem. In a system's world, this is insane. The problems are not isolated, therefore no isolated responses will work. *The longer we pursue strategies for individual survival, the less time we have to create any viable, systemic solutions*. None of the boundaries we've created across industries, organizations, communities, or nation states give us any protection in the face of Y2K. We must stop the messages of fragmentation now and focus resources and leadership on figuring out how to engage everyone, at all levels, in all systems.

As threatening as Y2K is, it also gives us the unparalleled opportunity to figure out new and simplified ways of working together. GM's chief information officer, Ralph Szygenda, has said that Y2K is the cruelest trick ever played on us by technology, but that it also represents a great opportunity for change.[17] It demands that we let go of traditional boundaries and roles in the pursuit of new, streamlined systems, ones that are less complex than the entangled ones that have evolved over the past thirty years.

There's an interesting lesson here about involvement that comes from the Oklahoma City bombing in 1995. Just a few weeks prior the bombing, agencies from all over the city conducted an emergency preparedness drill as part of normal civil defense practice. They did not prepare themselves for a bomb blast, but they did work together on other disaster scenarios. The most significant accomplishment of the drill was to create an invisible infrastructure of trusting relationships. When the bomb went off, that infrastructure displayed itself as an essential resource--people could work together easily, even in the face of horror. Many lives were saved

[17] In *Fortune*, April 27, 1998

and systems were restored at an unprecedented rate because people from all over the community worked together so well.

But there's more to this story. One significant player had been excluded from the preparedness drill, and that was the FBI. No one thought they'd ever be involved in a Federal matter. To this day, people in Oklahoma City speak resentfully of the manner in which the FBI came in, pushed them aside, and offered no explanations for their behavior. In the absence of trusting relationships, some form of techno-fascism is the only recourse. Elizabeth Dole, as president of the American Red Cross commented: "The midst of a disaster is the poorest possible time to establish new relationships and to introduce ourselves to new organizations . . . . When you have taken the time to build rapport, then you can make a call at 2 a.m., when the river's rising and expect to launch a well-planned, smoothly conducted response."[18]

The scenario of communities and organizations working together in new ways demands a very different and immediate response not only from leaders but from each of us. We'd like to describe a number of actions that need to begin immediately.

What leaders must do

We urge leaders to give up trying to carry this burden alone, or trying to reestablish a world that is irretrievably broken. We need leaders to be catalysts for the emergence of a new world. They cannot lead us through this in traditional ways. No leader or senior team can determine what needs to be done. No single group can assess the complexity of these systems and where the consequences of failure might be felt. The unknown but complex implications of Y2K demand that leaders support unparalleled levels of participation—more broad-based and inclusive than ever imagined. *If we are to go through this crisis together rather than bunkered down and focused only on individual security, leaders must begin right now to convene us.* The first work of leaders then, is to create the resources for groups to come together in conversations that will reveal the interconnections. Boundaries need to dissolve. Hierarchies are irrelevant. Courageous leaders will understand that they must surrender the illusion of control and seek solutions from the great networks and communities within their domain. They must move past the dynamics of competition and support us in developing society-wide solutions.

[18] quoted in "Managing the Crisis You Tried to Prevent," Norman Augustine, *Harvard Business Review*, Nov-Dec 1995, 151.

Leaders can encourage us to seek out those we have excluded and insist that they be invited in to all deliberations. Leaders can provide the time and resources for people to assess what is critical for the organization or community to sustain—its mission, its functions, its relationships, its unique qualities. From these conversations and plans, we will learn to know one another and to know what we value. In sudden crises, people instantly share a sense of meaning and purpose. For Y2K, we have at least a little lead time to develop a cohesive sense of what might happen and how we hope to respond.

Secrecy must be replaced by full and frequent disclosure of information. The only way to prevent driving people into isolated and self-preserving behaviors is to entrust us with difficult, even fearsome information, and then to insist that we work together.

No leader anywhere can ignore these needs or delay their implementation.

What communities must do

Communities need to assess where they are most vulnerable and develop contingency plans. Such assessment and planning needs to occur not just within individual locales, but also in geographic regions. These activities can be initiated by existing community networks, for example, civic organizations such as Lions or Rotary, Council of Churches, Chamber of Commerce, the United Way. But new and expansive alliances are required, so planning activities need quickly to extend beyond traditional borders. We envision residents of all ages and experience coming together to do these audits and planning. Within each community and region, assessments and contingency plans need to be in place for disruptions or loss of service for:

-- all utilities – electricity, water, gas, phones

-- food supplies

--public safety

--healthcare

--government payments to individuals and organizations

--residents most at risk, e.g. the elderly, those requiring medications

What organizations must do

Organizations need to move Y2K from the domain of technology experts into the entire organization. Everyone in the organization has something important to contribute to this work. Assessment and contingency plans need to focus on:

--how the organization will perform essential tasks in the absence of present systems

--how the organization will respond to failures or slowdowns in information and supplies

--what simplified systems can be developed now to replace existing ones

--relationships with suppliers, customers, clients, communities—how we will work together

--developing systems to ensure open and full access to information

The trust and loyalty developed through these strategic conversations and joint planning will pay enormous dividends later on, even if projected breakdowns don't materialize. Corporate and community experience with scenario planning has taught a important principle: We don't need to be able to predict the future in order to be well-prepared for it. In developing scenarios, information is sought from all over. People think together about its implications and thus become smarter as individuals and as teams. Whatever future then materializes is dealt with by people who are more intelligent and who know how to work well together.

And such planning needs to occur at the level of entire industries. Strained relationships engendered by competitive pressures need to be put aside so that people can collaboratively search for ways to sustain the very fabric of their industry. How will power grids be maintained nationally? Or national systems of food transport? How will supply chains for manufacturing in any industry be sustained?

What you can do

We urge you to get involved in Y2K, wherever you are, and in whatever organizations you participate. We can't leave this issue to others to solve for us, nor can we wait for anyone else to assert leadership. You can begin to ask questions; you can begin to convene groups of interested friends and colleagues; you can engage local and business leaders; you can educate yourself and others (start with www.Year2000.com and www.Y2K.com for up-to-date information and resources.) This is *our* problem. And as an African proverb reminds us, if you think you're too small to make a difference, try going to bed with a mosquito in the room.

The crisis is now

There is no time left to waste. Every week decreases our options. At the mid-May meeting of leaders from the G8, a communiqué was issued that expressed their shared sensitivity to the "vast implications" of Y2K, particularly in "defense, transport, telecommunications, financial services, energy, and environmental sectors," and the interdependencies among these sectors. (Strangely, their list excludes from concern government systems, manufacturing and distribution systems.) They vowed to "take further urgent action" and to work with one another, and relevant organizations and agencies. But no budget was established, and no specific activities were announced. Such behavior—the issuing of a communiqué, the promises of collaboration and further investigation—are all too common in our late 20th century political landscape.

But the earth continues to circle the sun, and the calendar relentlessly progresses toward the Year 2000. If we cannot immediately change from rhetoric to action, from politics to participation, if we do not immediately turn to one another and work together for the common good, we will stand fearfully in that new dawn and suffer consequences that might well have been avoided if we had learned to stand together now.

John L. Petersen is president of The Arlington Institute, a Washington DC area research institute. He is a futurist who specializes in thinking about the long range security implications of global change. He is author of the award winning book, *The Road to 2015: Profiles of the Future* and his latest book is *Out of the Blue - Wild Cards* *and Other Big Future Surprises*, which deals with potential events such as Y2K. He can be reached at 703-243-7070 or johnp@arlinst.org

Margaret Wheatley and Myron Kellner-Rogers are authors and consultants to business. *A Simpler Way*, their book on organizational design was published in 1997. Dr. Wheatley's previous book, *Leadership & the New Science*, was recently named one of the 10 best management books ever, and it also was voted best management book in 1992 in *Industry Week*, and again in 1995 by a syndicated management columnist. Their consulting work takes them these days to Brazil, Mexico, South Africa, Australasia and Europe. In the States, they've worked with a very wide array of organizations.