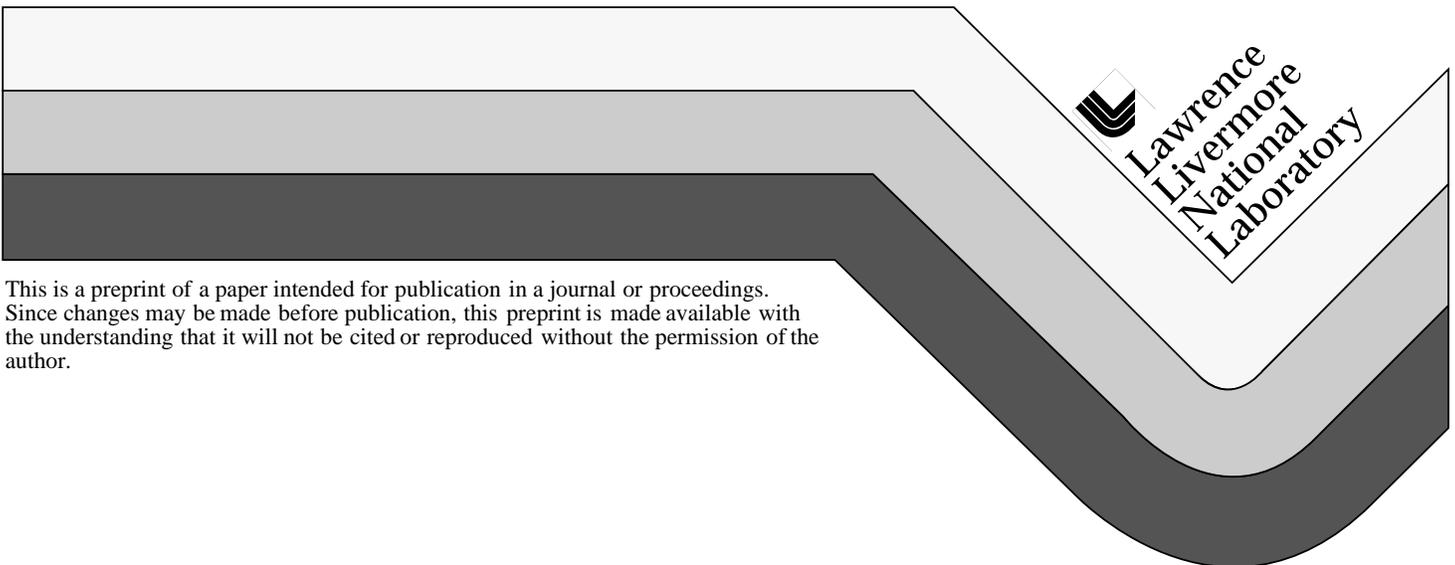


The Year 2000 Issue: International Action and National Responsibilities

Olivia Bosch

This paper was prepared for submittal to the
The Millennium Date Change Problem and Crisis Management
Stockholm, Sweden
March 8-10, 1999

July 21, 1999



This is a preprint of a paper intended for publication in a journal or proceedings.
Since changes may be made before publication, this preprint is made available with
the understanding that it will not be cited or reproduced without the permission of the
author.

DISCLAIMER

This document was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor the University of California nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or the University of California. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or the University of California, and shall not be used for advertising or product endorsement purposes.

The Year 2000 Issue: International Action and National Responsibilities

by
Olivia Bosch

Research Associate, International Institute for Strategic Studies (London) and
Center for Global Security Research (Lawrence Livermore National Laboratory,
California)

for proceedings of NATO Partnership for Peace (PfP) Seminar:
"The Millennium Date Change Problem and Crisis Management",
organised by the Swedish Agency for Civil Emergency Planning,
Stockholm, 8-10 March 1999

Introduction

This presentation will examine international aspects of the Year 2000 (Y2K) issue, in terms of how various countries are managing the problem and how international organisations are involved in that process. The paper notes that while international cooperation is essential in dealing with part of the problem, it is at the national level that preventive measures are undertaken and emergency services provided.

Most NATO and OECD states have recognised that by now it will not be possible to find and fix all problems in software and embedded chips. Their focus, therefore, is shifting to the planning of contingency measures, that is, what to do when disruptions occur so that the physical safety of persons is protected, damage to physical assets is minimised (e.g., extensive networks of energy supplies and telecommunications), and resources for the common good are protected (e.g., water supplies).

Not only is this conference timely, but the experience of various sectors can be shared to enable cross-sector comparisons to be made, for example, there might be lessons from within air transportation that might be applicable to the energy industry. In addition, while most countries have tended to focus on their national situation, this conference brings together persons from more than 25 countries, thus enabling further comparisons to be made on how other countries are pursuing contingency plans.

It is within this cross-sector and multinational context that international action and national responsibilities of aspects of the Y2K issue will be discussed. This presentation is in four sections. The first examines what is at risk and categorises the kinds of disruptions likely to occur.

The second presents an approach from which to understand how different countries are trying to manage the Year 2000 issue. This approach is based on

a three-step process adopted by the US and other OECD countries, the most dependent on computer and electronic processing systems and large information networks. The steps are:

1. awareness and perception of the problem;
2. technical preventive measures;
3. contingency action and consequence management.

The same steps are used to examine the Y2K efforts of non-OECD countries. This presentation does not advocate a right or wrong way to deal with the issue, but uses the approach as a framework in which to understand what factors might be significant with regard to managing Year 2000 disruptions, especially at the international level.

The third part of the presentation will examine the efforts of some of the relevant international governmental organisations and their activities regarding the Year 2000 issue. These organisations include the International Atomic Energy Agency (IAEA), the International Civil Aviation Organisation (ICAO), and the International Telecommunications Union (ITU). Understanding how these international organisations function illustrates not only their role but also their limits in dealing with Y2K issues. Member states of these organisations are ultimately responsible for dealing with the Y2K issues at the national level. This includes cooperation among national and regional or local governmental authorities and emergency services, which at the end of the day – and on the day and the day after – will be responsible for dealing with Y2K disruptions.

The fourth section will explore other measures, both non-governmental and governmental, urging states to pay more attention and which might include new processes to manage disruptions. For example, some industries lobby their foreign ministries to urge other states to undertake Y2K remediation. New international collaboration regarding the safety of nuclear weapons and associated early warning systems is being established which in future may yield to positive developments in political relations. This type of example is applicable to other sectors and illustrates some of the positive outcomes or lessons learned from the Y2K issue. On an assumption that there are these positive aspects, the term “Y2K issue” rather than “Y2K problem” is often used in this presentation.

I. Setting priorities

Part of the awareness of the problem requires examining which systems need attention. While most aspects of a nation's infrastructure are considered the main priority, in particular the energy and power industries and the telecommunications sector, another way to measure importance is in terms of the effects of their disruptions. This means placing into a hierarchy of

importance those systems which will need the most attention. It can be argued that those Y2K disruptions that risk causing long-term effects on persons need the most attention. For example, a worst case scenario may be a radioactive emission from a failing civil nuclear power plant which could result in effects on the human population and environment for generations. Thus making sure that the reactors within the civil nuclear power industry are Y2K compliant seems most important. The risk, however, of an occurrence similar to the April 1986 Chernobyl incident arising directly from a Y2K fault compared to other factors is improbable. First, the combination of operator errors and unique plant design flaws which led to the “melt down” rather than shutdown of the Chernobyl RBMK reactor, is unlikely to occur elsewhere. Secondly, RBMK reactors had design and control rod flaws that have since been altered to enable them to be able to be shut down safely. Thirdly, during the Chernobyl incident improper procedures were followed. Plant operators now have the opportunity to re-examine and practice their contingency measures many of which will have been in place for decades. Thus an unplanned shut down is likely to be the worst that could occur as a result of a Y2K error. Focusing too much on Y2K however, should not make operators oblivious or less cautious of other mishaps that might occur – as with any large system.

Even if an unplanned shutdown were to occur, the secondary effects might also vary depending in part on how dependent a country is on nuclear energy. For example, while both Lithuania and France rely on their nuclear power reactors for about 75% of their energy needs, Lithuania has only two nuclear power reactors which means that a shutdown could have nationwide effects while in France, the shutdown of several its 58 reactors may result in local difficulties only. Perhaps more importantly, however, are the assessments made of interconnections between power plants and other parts of a national infrastructure, for example, the national power grid, water supplies, and communications. While one’s own plant might be Y2K compliant, if some of the external facilities and services on which it relies are not, then Y2K remediation efforts at the plant will have been in vain.

While this is a physical risk which could have long-term implications, the next priority could be physical risks of medium-term or local implications – to persons and to assets. Here, for example, the effects of Y2K disruptions on a chemical plant could result in toxic emissions leading to health effects such as that from the 1984 Bhopal incident in India in which thousands of persons were killed and tens of thousands injured. Other health effects could result from disruptions to water and sewage treatment plants. Regarding loss of valuable assets, aluminium plants are complex systems built over years and which rarely, if ever, have been shut down. A Y2K disruption therefore may have devastating effects on this type of plant which would “freeze” or seize up after a forced shutdown. The types of incidents in this category of effect are

likely to have more local effects than for civil nuclear power plants, and thus emergency services can direct attention to where such plants are located.

A next category of effect is those disruptions which occur singly in one area and thus seem minor but propagate more widely – perhaps even internationally. Effects on communications and messaging services as well as within the stock market and other financial systems may fall into this category. Yet, the stock market, for example, has already put into place many “brake” systems as a result of past disruptions.

Failures in electricity represent another type of occurrence, whereby disruptions of a minor nature could occur locally, but they will also occur separately and simultaneously across a state. While large states with several time zones may see possible effects a few hours beforehand, it is not certain what advantages that might provide. Such occurrences mean that local civil emergency agencies will have to be prepared to take a burden from national or federal emergency agencies. Federal or national emergency agencies tend to be more prepared to deal with a few major incidents – rather than many which might occur simultaneously throughout a state. Coordination between local and national civil emergency agencies, therefore, is necessary with national capabilities being on call for more high impact disruptions, for example, where important nodes of infrastructure networks exist or at facilities mentioned in the first two categories above regarding civil nuclear power reactors and chemical plants.

While air traffic is likely to have many disruptions, services are likely to be reduced if it appears that safety could be compromised. Some airlines may not fly if they are not confident in the capabilities of air traffic control, or their public liability insurance is called into question.

II. Varying International Perspectives on Y2K

This second section of the presentation deals with the varying international perspectives on the Year 2000 issue. The from which to better understand how different countries around the world are trying to manage the Year 2000 issue is based on a simplified three-step process initially adopted primarily by OECD countries, most dependent on computer and electronic processing systems and large information networks. The steps of awareness and perception of the problem, technical preventive measures, and contingency action and consequence management provide a basis from which to examine the Y2K efforts in non-OECD countries.

The country most representative of this approach is the United States considered to be the most dependent on computer networks and microprocessor systems. Aware of this dependency, President Clinton established in July 1996 the Commission on Critical Infrastructure Protection,

which in 1997 reported that damage could be inflicted on complex and interdependent computer systems. This damage would be as a result of both threats and vulnerabilities. Vulnerabilities, or existing weaknesses, are many and include the Y2K issue. Threats include what are often called crackers (malicious hackers), potential terrorists, and international criminal groups which take advantage of these vulnerabilities. Following from the 1997 Report, President Clinton issued in May 1998 Presidential Decision Directive 63 (PDD-63) on critical infrastructure protection. This put into motion activities to implement protection of the national infrastructure and these efforts continue today.

Companies and governmental organisations have tended to compartmentalise how they deal with threats to a system and its vulnerabilities. One of the lessons to be learned from the Y2K issue may be a requirement to narrow this gap or focus on a more holistic approach to information security similar to that undertaken by the US initiatives on critical infrastructure protection.

Examining the three-step process will bring out some of the thinking behind why or how developing countries might react differently to the Y2K issue.

1. *Awareness of the problem and perception of its importance*

The United Nations ECOSOC's Working Group on Informatics organised a National Y2K Coordinators Meeting on 11 December 1998 to focus on the Y2K issue. As a result most countries are now aware of the problem at least at the governmental level, and have at least one person designated to work on the issue. However, while most OECD countries see the Y2K issue as an important problem, many developing countries perceive it as a lower priority issue among their many economic, social, and health problems and natural disasters.

A more significant aspect of perception, however, is the degree to which disruptions around the end of 1999 will be self-induced. These are attributable to factors which are not explicitly the result of a technical Y2K problem but relate to the end of the millennium or some other self-fulfilling prophecy. There fall into two categories:

- the objectives of particular apocalyptic or religious cults which are looking for disruptions as a sign of the end of the world, and in so doing fulfill their organisational goals. The effects of Y2K disruptions are likely to have localised impacts in this scenario, and law enforcement agencies may already know where such cults operate to mitigate effects.
- self-induced shortages as a result of a perceived fear or lack of public confidence of what might or might not happen. For example, the end of

the millennium may mean that many more persons will telephone each other on the night and weekend and therefore induce an overload on communications systems. Possible failures are caused by the overload rather than by a Y2K problem, nevertheless, many people will blame it on Y2K. On a larger scale, world recession is sometimes forecast to result from investor speculation or lack confidence if major investments were to be withdrawn from the financial system.

2. *Preventive measures*

Following awareness of the problem and perception of importance is the second step on preventive measures. Many developing countries argue that unlike advanced industrial countries, they have fewer computer systems to check. This also means fewer labour hours are needed to search for the relevant chips. By implication costs therefore are lower, and these may even be defrayed by World Bank funds which in the middle of 1998 amounted to \$30 million available for remediation efforts. These funds are for non-OECD countries and primarily come from the United Kingdom and the United States.

While many of these countries have fewer computerised systems, some wrongly perceive that they therefore do not have a problem because they do not see or perhaps do not understand the degree to which Y2K also affects microprocessors often embedded in systems and in areas not easily located. In addition, there may not be awareness of the degree of interconnectivity between the few systems that they do have. And even if the difficulty in locating "embedded chips" were overcome, the chip or computer software code may not be easily repairable. Most manufacturers are able to provide licensed upgrades or replacement parts but they will not be obligated to do so for pirated or unlicensed equipment. Piracy has been reported to be a major issue, for example, in China and other parts of Asia. In addition, older systems may no longer be produced and therefore have no upgrade, while bespoke or custom-designed equipment may require *ad hoc* fixes as programmers who originally wrote the software are no longer accessible.

While the government-owned critical infrastructure in most developing countries (unlike, for example, in the US and Europe, where there is a combination of private and public ownership) may have the advantage of more easily concentrating remediation efforts, many of these countries have very bureaucratic and inefficient government processes to implement measures.

3. *Contingency measures and consequence management*

This third step, sometimes divided into two, has become the focus of attention now as planners and managers realise that there is not enough

time, and in some cases money, to conduct all desirable preventive repairs. Contingency measures are being prepared to ensure business or government continuity. This may mean stockpiling component parts, obtaining back-up power and water supplies, making sure older communications systems are operational, and limiting work to only essential or mission-critical activities.

Some developing countries which do not have appropriate resources, and perhaps even some small- and medium-sized companies in advanced countries, might rely solely on consequences management. They will wait and see what happens and then pay for any damage or loss after it occurs. Additionally, whatever the source of the consequences, many developing countries lack adequate emergency services to deal with disasters as is evident in the problems and catastrophes already confronting many of them. Therefore what initially might be a minor Y2K disruption may become larger as emergency services are not sufficient to contain the initial smaller ones. A possible counter to this argument, however, is that given the number of existing disruptions and inefficiencies, including regular electricity failures, which already occur in many developing countries, disruptions from Y2K may not be noticeable or perceived as significant.

At the international level, some consequence management may take the form of unscheduled humanitarian relief missions conducted by countries and organisations capable of doing so. These missions might assist with the implications of electricity shortages in cold climates, and are discussed in section four.

III. International Organisations

The next section examines the efforts of some of the relevant international governmental organisations and their activities regarding the Year 2000 issue. Most of the activities contribute to the first step mentioned above, that is, of increasing awareness and stressing the importance of the Y2K issue. These organisations include the International Atomic Energy Agency (IAEA) regarding the safety of civil nuclear reactors and facilities; the International Civil Aviation Organisation (ICAO) with respect to air traffic control, and the aircraft and airlines industries, and the International Telecommunications Union (ITU). These organisations have a regulatory influence and have issued statements and resolutions urging member states to take their responsibilities seriously, and also try to set standards in the way in which Y2K assessment, testing and validation are carried out.

The IAEA passed a resolution in September 1998 urging its then 128 member states to share information with the IAEA Secretariat regarding diagnostic and corrective action and to draw up contingency plans. In January 1999, it

issued a 55-page report, available on the Internet, on “Guidance for Achieving Year 2000 Readiness” and this report would seem to contribute to the standards-setting objective. The IAEA does not fund national remedial efforts, this being the responsibility of member states, and thus indicates that national responsibilities despite international action are essential.

While the IAEA has become a clearing house for civil nuclear power issues and Y2K, the World Association of Nuclear Operators (WANO) had been quite active in 1998 in raising Y2K awareness and conducting seminars for its 130 utility company members that run the world’s 434 reactors in 32 countries. The US, France, Japan and the UK together have 250 of these reactors; 70 reactors are located in Eastern Europe and the former Soviet Union. As mentioned, Chernobyl-like disasters are not expected, those remaining 13 RBMK reactors having been adjusted to shutdown properly rather than melt down.

While the civil nuclear power sector has 434 reactors to deal with in terms of volume, the members of the International Civil Aviation Organisation (ICAO), with headquarters in Montreal, have tens of thousands of items. The ICAO’s 185 member states are bound by its Convention (Article 28) to provide air navigation facilities and standard systems. This means that information on hazardous issues, including Y2K, should be made available to all members – a regulatory requirement which the ICAO can do little more than issue. In December 1997 and May 1998, the ICAO issued letters to all its members to raise the Y2K problem. In June 1998, under the ICAO auspices, the Informal Global Y2K Coordination Action Group was formed. On the ICAO web-site, its newsletters were perhaps some of the most informative on the internet at the time and helpful in raising appropriate and difficult issues. This Coordination Group seems well-organised at least in its presentation, which seems extraordinary given that the Action Group comprises the world’s air industry, air traffic controllers and airlines. Together they are to ensure air traffic safety, efficiency and regularity and to review around 2,000 airports around the world, with visits to 70 designated as the most important. The Group meets once a month to coordinate steps to establish a Y2K programme, develop regional solutions and contingency plans, and to establish a mechanism to issue warning of Y2K disruptions.

Understanding how these international organisations function illustrates their role but also their limits in dealing with Y2K issues. Member states of these organisations, as well as businesses, are ultimately responsible for dealing with the Y2K issues at the national or corporate levels. This includes cooperation not only among national, regional, and local governmental emergency services and authorities but also between government and private or corporate-owned services. How this cooperation, which is both top-down and bottom-up, is central to any discussion of this matter.

So while international organisations have important roles before 31 December 1999, national to local government and emergency services will be the focus of action on the day and days around the 31st. And then in the aftermath of the Y2K disruptions, there may then be a shift back to international cooperation, for example, in the provision of electricity supplies to neighbouring countries, or international humanitarian relief operations.

IV. Other International Measures

These are other measures or processes, both non-governmental and governmental, to urge states to pay more attention. These also include mechanisms being created to manage possible disruptions. These processes include industrial lobbying, for example, of Foreign Ministries to exert influence for Y2K compliance abroad. This form of pressure has so far been quiet: enough to let governments know of the consequences of not doing so, yet not publicly “blacklisting” them which may prematurely adversely affect trade or tourism.

Regarding government-to-government processes, there has been new collaboration between states regarding the safety of nuclear weapons. Given the destructive capability of nuclear weapons, these systems are addressed with high priority. Averting these possibilities, however, may also provide opportunities for new forms of political cooperation or positive developments in political relations. These new arrangements might not have occurred so easily were it not for the Y2K issue.

With respect to nuclear weapon systems there is less concern about their operational aspects than of their early-warning and communications systems. Operationally, nuclear armed missiles do not launch autonomously; a multi-layered launch procedure involves personnel and thus should fail-safe. The focus of negotiations, for example between the US and Russia, has been on early warning systems. On 2 September 1998, the US-Russia Joint Statement on the Exchange of Information on Missile Launches and Early Warning states that both countries, possibly with personnel working “side-by-side”, would exchange early-warning information regarding inadvertent ballistic-missile launches on the basis of a false warning of attack. Follow-on negotiations into early 1999 were concerned about trying to establish a Joint Warning Center, perhaps outside Moscow and at Colorado Springs, for Americans and Russians to deal with this issue and to do so next to each other. There is also a joint diplomatic initiative to broaden these discussions to become multilateral.

Regarding North Korea and the South Korea, it was reported in February that the respective military commanders met in early 1999 for the first time in about a year to discuss early warning systems and inadvertent missile launches as a result of the Y2K issue. While these talks were within the

framework of the Armistice Commission, there might be scope for expanding discussions to include the US and China within the existing 4-party Working Group dealing with confidence- and security-building measures in the Korean peninsula region.

On 21 February, India and Pakistan's Lahore Declaration included a Joint Statement in which both sides would cooperate on tackling the problems of Y2K. The Declaration also included a Memorandum of Understanding which more specifically focused on improving measures to reduce risk of accident and misinterpretation concerning nuclear weapons under their control. While India and Pakistan do not have the high degree of computerised early warning systems and communications of the United States and Russia, they have shown intent to take seriously the risk of Y2K and other disruptions to their military systems.

While Y2K and nuclear weapon capabilities and relevant systems are limited to specific cases, there is likely to be more activity as humanitarian relief missions and emergency services prepare to react to possible major Y2K disruptions. These would be part of the international activity that might occur in the first two weeks of January 2000, and could take the form of action by NATO using its Civil Emergency Planning Directorate, by the United Nations and the International Committee of the Red Cross, as well as unilateral activities by the US, UK, and other countries as appropriate. Civil emergency agencies such as the Swedish Agency for Civil Emergency Planning can coordinate supplies for international peace-promoting and humanitarian operations. This area is likely to bear fruitful discussion in the months ahead.

These examples of cooperation may be applicable to other sectors or organisations and illustrate some positive outcomes from the approaches and efforts undertaken by governments, industry, and the public in addressing Y2K issues. There will be many valuable lessons learned which will be of great help to deal with threats and other vulnerabilities to all types of information systems and infrastructure.

This work was performed under the auspices of the U.S. Dept. of Energy at LLNL under contract no. W-7405-Eng-48.