THE Y2K (Year 2000)PROBLEM

Submitted by asiaadmin2 on Thu, 09/20/2012 - 06:37

Paper no. 30

The Y2K problem, if inadequately dealt with and unrectified , could have an impact on our national security due to economic disruption and damage to the operational effectiveness of our military and scientific establishments and equipment and , hence, the monitoring of the action being taken to deal with this problem should be a subject of immediate attention for our newly-constituted National Security Council Advisory Board.

There are three aspects to tackling the problem:

- Stepping up the awareness of the problem and its likely implications not only in the minds of ought-to-be-concerned professionals, but also in the minds of the public.
- Identification of the likely sources of the problem in our computer networks and other equipment with embedded systems and rectifying them in time in order to make them year 2000-friendly.
- Keeping ready contingency plans to deal with disruptions and break-downs if, in spite of the rectifications, difficulties occur due to incomplete identification of the sources of the problem.

The problem has arisen due to the practice in the 1970s and 1980s of the date command being written only with the last two digits of the year. Consequently, as one enters the next millennium, the computers and embedded systems could mistake “00” which would follow “99” for the year 1900 and not for the year 2000 and thereby set in motion a chain reaction of data and operational distortions with not easily predictable consequences.

The understanding of the problem has passed through three stages. Initially, it was believed that the problem

would occur only in mainframe computers of old vintage and hence damage control and consequence management should not be difficult. Subsequently, it was realised that the problem could arise even in personal computers and all equipment having embedded processors (microchips) with date commands. Such equipment would range from consumer electronic items such as VCRs, refrigerators etc to thousands of other equipment controlling economic and industrial activity and even the functioning of hospitals. There is hardly any modern electronic equipment which does not have a date command.

In such equipment, the date command serves various purposes such as keeping track of the time elapsed since the last servicing of the equipment and alerting when the next servicing is due, regulating life-saving functions of modern hospital equipment such as those used for drip-feed and performing any other function where time regulation and date compliance are important factors.

The date commands in the embedded processors have made the problem much more complex and much more difficult to handle. It is estimated that the various electronic equipment in use in the world today has about 25 billion microchips, of which only about 3 per cent have date commands. Since, in the past, there was no proper documentation of the number and location of such microchips with date commands, identifying all of them for rectification is going to be as difficult as locating a needle in a haystack.

That is why computer experts are not confident that they would be able to locate and rectify in time all embedded processors with date commands. In spite of their best efforts, some could remain undetected and unattended, thereby posing problems.

Another complicating factor could arise from the fact that even as software experts are dealing with the problem in the equipment acquired in the past, equipment of new design, but with old microchips with two-digit date commands might be entering the market thereby increasing the possibility of many equipment with potential date problems remaining unidentified and unattended.

Recent months have seen a virtual crashing of the prices of computers and other electronic equipment in Asia and other Third World countries, with companies vying with each other in reducing prices and offering other incentives for the purchase of their equipment.

This is partly due to overproduction during the boom years resulting in large unsold stockpiles. Another plausible —and a more disquieting ----explanation could be that these companies are dumping on unwary customers unaware of the implications of the Y2K problem equipment with potential date command problems, as such equipment, without rectification, would become junk by next year and the companies would not be able to sell them..

The Governments of India and other countries in this region have not woken up to this danger and educated the consumers about it.

The third stage in the understanding of the problem relates to the nature of computer networks, which recognise no jurisdiction and have no beginnings and no ends. Once your system becomes part of a network, it gets interwoven

with other systems in the same network for the good as well as for the bad, sinking or surviving with each other.

Functioning as a part of such networks is like driving a car on the road. You may be a very good driver, law-abiding, observing the traffic regulations and taking all precautions, but you may still get killed in a traffic accident if other users are not equally law-abiding and cautious.

Similarly, in a network, you might have got your system checked thoroughly and ensured that it would be 2000-friendly, but if any of the others forming part of the same network has not done it, distortions in the operations of their systems could spread to yours too through the network and create disruptions for no fault of yours.

This underlines the need for the problem being tackled individually as well as collectively by all nations of the world and by all inter-connected enterprises and establishments. Compartmentalisation of efforts could prove counter-productive and even suicidal.

One sees evidence of such co-ordinated action in the Western countries, but not in Asia and other regions of the Third World. Since dealing with potential Y2K disruptions
would possibly be the most important management problem of 1999 and 2000 in Government as well as private establishments, one would have expected this issue to be on the top of the agenda in the summits of the SAARC (Colombo), the APEC (Kuala Lumpur) and the ASEAN (Hanoi) held in recent months and in the meetings of businessmen which preceded or accompanied them, but it did not. There was hardly any reference to the problem.

Each Asian nation is tackling the problem individually as best as it can without any effort for co-ordination with other nations. There seems to be an air of self-complacency due to a mistaken impression that since the Asian countries are not yet as computerised as the West, the fall-out in this region would be minimal. This is an unwise approach and could cost the region heavily in the first two or three years of the next millennium.

There are conflicting and often confusing assessments of the progress made by different countries and regions in tackling the problem. While some of these assessments have been made by organisations such as the Paris-based Organisation For Economic Co-operation And Development (OECD), others have been by non-governmental consultancy and business groups.

Without getting involved in the various percentages of compliance by different countries which have been floating around, it would be safe to say that while the progress has been above average in the US, Canada and West Europe (including Finland), it is below average in the rest of the world, with the former communist States of East Europe being at the bottom of the evaluation scale.

In Asia itself, India, Japan, South Korea, Taiwan, the Hong Kong Special Administrative Region of China and Singapore have made better progress than the rest of the region. Mainland China is a big question mark. While the joint ventures with foreign firms and manufacturing facilities and service establishments set up by foreign enterprises—particularly Western enterprises—are better prepared, one cannot say the same thing of the thousands of State-owned enterprises (SOEs).

Many of these enterprises have been running at losses for many years now, are already heavily indebted to

financial institutions and have not been paying regularly the salaries of their staff. Unless the State helps them in a big way, whether they would have the required funds to deal with the Y2K problem is doubtful. No data is forthcoming as to how the Chinese Government is tackling this problem in the SOEs.

However, that China is sensitive to the potential seriousness of the problem could be gauged from its reported request to the International Atomic Energy Agency (IAEA) in Vienna for assistance in identifying and removing potential Y2K problems in its sole indigenously-designed nuclear power station.

Y2K problems have already started surfacing in different countries long before the birth of the new millennium in the form of rejection by computers of credit and guarantee cards with the validity date extending into the year 2000 and of medicines with the expiry date similarly extending to the year 2000. Computers used for long-term projections of raw material, spare parts and man power requirements have also been facing difficulties due to their inability to span two millenniums.

The consequences of unattended Y2K problems may not come like a thunderbolt at the midnight of December 31,1999/January 1,2000, as often projected in over-dramatised media accounts. They are more likely to occur as a creeping paralysis of government and private establishments which have failed to take timely rectification action, with the paralysis spreading ultimately even to enterprises which had tackled the problem energetically.

Such paralysis could lead to a long spell of recession the world over, with the prospects for an early recovery of the Asian economies being adversely affected for some months, if not years, to come. Since information is the most important raw material which keeps industrial, economic and social welfare activities going in the globally-networked world and protects national security, the consequences of the drying-up or degradation of this raw material could be of unpredictable dimensions.

In India, the initial focus was on how our software experts should be mobilised to earn more foreign exchange by offering their services to other countries in rewriting their date command codes. Only recently, is more attention being paid to the type of problems likely to occur in the country itself and to dealing with them in order to ensure Y2K-compliance. There is not yet sufficient awareness of the problems that could be faced by embedded systems and of the difficulties that could start arising from April,1999, itself due to the fact that the 1999-2000 financial year would be spanning two millenniums.

The first task has to be the identification of priority sectors needing attention such as public utilities supplying water and electricity and specially nuclear power stations, transport and telecommunications, the financial sector, oil production and refining, the defence and scientific establishments and other industrial facilities.

India’s vulnerability, as in the case of China too, is likely to be greater because of the large number of Soviet/Russian equipment in use in the civilian as well as military sectors. The Y2K problem has not received the same attention in Russia and other East European countries as it has in the West and there is consequently a data gap.

The Russians have shown themselves to be excellent in dealing with computer problems after they have arisen,

but not so much in preventing them as one noticed during the repeated break-downs of the computers on board the Mir, their space vehicle, in the last few months.

One still does not know why these break-downs occurred. Were they due to an early manifestation of Y2K problems?

B.RAMAN 28-1-99

(The writer is Additional Secretary (Retd), Cabinet Secretariat, Govt. of India, and presently, Director, Institute For Topical Studies, Chennai. E-Mail address: corde@md3.vsnl.net.in [1])

Category:
Papers [2]
Topics:
Technology [3]

Copyright ©2012. All Rights are Reserved.

Source URL: http://www.southasiaanalysis.org/paper30

Links
[1] mailto:corde@md3.vsnl.net.in
[2] http://www.southasiaanalysis.org/papers
[3] http://www.southasiaanalysis.org/technology