IFS Info 2/2001

Olivia Bosch

The Year 2000 Issue and Information Infrastructure Security

Table of Contents

On the author

Olivia Bosch is Senior Fellow at the Center for Global Security Research at Lawrence Livermore National Laboratory, California and at the International Institute for Strategic Studies in London. This paper first appeared as a chapter in G. Ragsdell and J. Wilby (eds.), *Understanding Complexity*, Kluwer Academic and Plenum Press, 2001.

Introduction[1]

This paper explores which measures used to deal with the Year 2000 (Y2K) problem are also applicable to the future security of information networks in critical infrastructure. As information and communications technology (ICT) become ever more widespread, protection of both the information and the infrastructure upon which it relies becomes important as financial transactions and economies become increasingly global and interdependent. The Y2K problem, whereby computers with two digit year formatting are not able to read 00 as the year 2000, meant that errors would occur in many processes and calculations, such as billing, manufacturing and trade, in both the public and the private sector around the world. After January 2000 had passed, other computer incidents occurred such as the distributed-denial-of-service attacks in the US in February 2000 and the ILOVEYOU virus attacks globally in May 2000. Furthermore, high-level attention to international ICT developments was paid in July 2000 at the G-8 Summit of industrialised countries and at the annual meeting of the United Nations Economic and Social Council (ECOSOC); these all sustained the importance of information infrastructure and its protection.

This paper will first assess the steps undertaken by governments, industry and international organizations to deal with the Year 2000 (Y2K) issue. The motivations behind the effort and requirements for fixing this problem varied not only between these three groupings but also within them. For example, advanced western nations and developing countries were influenced by different factors. The second part of the paper will make some preliminary assessments of how representative the Y2K problem was of other threats to and vulnerabilities of information systems. Then, various factors that contributed to managing the Y2K issue will be examined for their applicability to information infrastructure protection. While government and industry cooperation was a predominant element in dealing with Y2K, this and other factors, such as the spread of good management practices and the work of international organizations, are equally important to critical information infrastructure protection.

The Y2K problem is presented as a case study of a threat to or vulnerability in the information networks of critical infrastructure. Given the potential large scale and global scope of the impact of the Y2K problem, it was a valuable example from which to assess the vulnerabilities of critical infrastructure, and thus also the means of protecting it. The Y2K issue was both a simple technical problem readily understood and also a complex issue in that it involved all sectors of society, including those critical infrastructures with complex interdependencies which, if they were to fail, had potential for large-scale adverse consequences.

The critical infrastructure of a nation is defined as those assets upon which the security and economic and social viability of a country rely. In this paper, they comprise the assets of the energy and communications sectors upon which financial, governmental and emergency services depend. Other sector assets such as food, water-treatment plants, manufacturing plants, the oil and gas industries, and transportation are included in broader definitions of critical infrastructure, but these sectors, too, rely ultimately on energy and communications systems. Over the past decade, information technologies have increasingly been used in these infrastructure assets to improve controls and monitoring of processes as well as business transactions, and therefore the security of these information networks in the critical infrastructures requires examination.

The Y2K problem was expected to impact upon the energy and communication sectors in different ways: on the one hand with an immediate noticeable failure, and on the other a cascading or perpetuation of errors in systems that otherwise appear to be working as normal. These two sectors and error types, while general and broadly defined, indicate that critical infrastructure is not a monolithic entity, but composed of different technologies and related

systems which require protection of not only information but also physical assets.

Motivations for dealing with Y2K

Governments, industry, and international organizations are the focus of examination as they own, manage and regulate critical infrastructure, and these three types of entity each differed in their motivation and approach to fixing the Y2K problem. The focus on these categories, however, does not mean the efforts of many other individuals and organizations that also took an active role in dealing with the issue were unimportant. Critical national infrastructure underpins the operations of governments and economies, therefore, its protection is also a matter of national security.

Governments were motivated to deal with the Y2K issue by concern with security and law and order, as well as the smooth running of government services. The confidence of the public therefore was a prerequisite and led governments to encourage disclosure of information about how the problem had been dealt with. Such a view was adopted primarily by the US and UK governments which led the world in efforts to raise awareness of the problem. The US and to a lesser extent the UK and Japan are heavily dependent on computer systems and having the largest financial centers as well as strong industrial and IT sectors, these countries had global interests in making sure the problem had been fixed. Reflecting part of this global concern, the US and the UK were the main contributors to the World Bank's Information for Development Program (known as infoDev) which offered non-OECD countries grants for assistance with their Y2K problems. In developing countries, which are less dependent on computerized or digital automated systems, raising awareness of the problem in a similar way to that adopted by the US was believed to be unnecessarily alarming to their publics, or not considered as important enough in light of other more pressing social, political, and economic problems. These views were held in October 1999[2], even after the June 1999 UN-mandated 2nd Global National Y2K Coordinators conference in New York, where more than 170 countries attended to discuss and compare how countries were preparing for the impact of the Y2K problem.

Not surprisingly, security was the main motivation behind action by ministries of defense and other national security organizations. They too relied on effective communications and energy supplies to be able to maintain existing military operations, and assist with humanitarian relief operations to alleviate Y2K-induced disasters, if required. Additionally, much public attention was devoted to the possible impact of the Y2K problem on nuclear-armed missiles, and thus the nuclear weapons states, particularly the US and Russia, turned attention to showing the public that these particular weapon systems and associated early-warning systems were secure.

While public attention was on high profile areas such as nuclear-armed missiles, commercial aircraft, and civil nuclear power plants, these are complex systems which are potentially vulnerable to hazardous impacts of all kinds, and thus have been heavily regulated for safety and made subject to stringent physical protection measures for decades. Redundancy of safety mechanisms, the shift from manual to automated systems and layered contingency procedures were ways to reduce the risk and impact of errors in such complex systems.[3]

Industry was motivated to fix the Y2K problem by concerns about liability for damage caused by Y2K disruptions and by the impact upon profits, as well as reputation. In the US and UK, and in varying degrees throughout Western Europe, the private sector owns and/or operates upwards of 90% of national critical infrastructure. In developing countries, many electricity utilities and communications facilities are still owned and operated by government, though deregulation of these sectors has already begun. The approaches to fixing the Y2K problem by advanced countries, therefore, were

quite different from those undertaken by developing countries. Not until after January 1, 2000 did factors emerge that more clearly explained the low level of Y2K disruptions in developing countries. These factors included the degree to which a relatively small number of vendors of critical infrastructure could provide a more uniform approach on how best to conduct fixes in their respective sector. Secondly, developing countries "leap-frogged"[4] by benefiting from the research and "homework" done in more computer-dependent countries, in particular from the best practices that were spread by multinational companies abroad. Lower levels of automation and government-owned infrastructures meant that centralised approaches facilitated Y2K repairs as well as contingency planning once the urgency was understood.

The major international governmental organizations associated with dealing with the Y2K problem were primarily the United Nations-mandated International Y2K Cooperation Centre (IYCC), and those organizations that have a regulatory role which includes assuring safety of a sector. These organizations include the International Telecommunication Union (ITU), the International Atomic Energy Agency (IAEA), the International Civil Aviation Organization (ICAO), as well as international trade and industry associations such as the International Energy Association (oil and gas) and the World Association of Nuclear Operators (WANO). The Electric Power Research Institute (EPRI), the Information Technology Association of America (ITAA) and the American Petroleum Institute, while specific to the United States, also had international influence on fixing the problem which was a potential safety hazard if not fixed. The international governmental organizations issued statements and guidelines and requested that their member states take appropriate measures to ensure that Y2K was fixed or its effects mitigated. Though repair or replace efforts were paid for by either member states or private owners of equipment, and any expected disruptions would have local impact, the international organizations were able to use their regulatory role to place pressure on and coordinate governmental efforts in these particular sectors.

International organizations were able to harmonize efforts among governments worldwide, while large multinational companies were able to spread best practices; the private sector had unprecedented cooperation with governments in advanced countries while multinational corporations worked with governments in the developing countries in which they operated. While it was not formal, there was a system of interaction between governments, industry and international organizations to deal with repair efforts. This cooperation also continued when global Internet schemes were being established to monitor and share information about potential Y2K disturbances as they occurred world wide during the roll-over period from December 31, 1999 to at least January 3, 2000.

Expectations in 1999 of potential impact of Y2K

From late 1998 to early 1999, before widespread disclosure of information about how effectively efforts to fix the Y2K had been, the expectations among the public and some organizations as to how the Y2K problem would impact upon them varied from apocalyptic disruption to not much more than a nuisance. The US, by far the most reliable on ICT, appeared to be the only country in which a small sector of the population, for example, some survivalist and particular conservative Christian groups, expected apocalyptic or worst-case scenarios; a "Christian Y2K Relocation" site was on offer in Minnesota for $64,000.[5] More of the US population, though not expecting disaster, nevertheless prepared for a heavy three-day storm, and acquired back-up or emergency generators and foodstuffs.

Various surveys were undertaken to assess public expectation and industry expectations of the disruptions that might occur. One series of surveys was conducted by Bruce Webster[6] for the Washington D.C. Year 2000 Group, in March and May 1998, and in June and November 1999. 2000 email addressees were asked to

predict the impact of Y2K in the US in five different sectors on an escalating scale of 0 (celebratory) to 10 (apocalyptic). The June survey was more optimistic than the ones in 1998. From the usable data of 337 respondents from a range of professions, there were three areas of consensus: "that the social impact will be modest (65% saw it in the 0-4 range); that the government is not as prepared as it claims to be (74% saw it in the 4-10 range) and that infrastructure...will be impacted more broadly than is generally asserted (65% saw it in the 4-10 range". Generally there was also a division between those who expected not much to occur and those who "described organizations far behind in their Y2K efforts (and usually covering it up)". By the December 1999 survey, the results had become more optimistic, reflecting a decreasing concern in the US that the Y2K problem would result in serious disruption.

While the above survey was to assess perceptions of what would occur, surveys were also made to try to assess what countries were actually doing, on the basis that as more information was known then there would be less apprehension among the public and industry. One of the most prominent studies for assessing country readiness around the globe was that conducted by the Gartner Group consultancy organization. Its surveys from autumn 1998 placed countries in rank order of Y2K readiness, based on a number of factors including the state of preparedness for dealing with the Y2K problem and a country's dependence on information technology (IT). Warburg Dillon Read, an organization similar to the Gartner Group, used these two rankings, subtracting the readiness ranking from that of the one on IT dependency, to calculate an aggregate measure of vulnerability. Their results indicated that the countries likely to be most affected were the Philippines, Russia, China and Indonesia, with the countries least likely to be affected being the US, Netherlands and Sweden.[7] The information was based on first quarter 1999 data, and it would not have been appropriate to use it as a basis for making conclusions later in the year when developing countries as well as smaller industries had taken big steps to deal with the problem. Information that was more than three months old was soon outdated. Nevertheless, in October 1999, adequate information about Y2K readiness appears still not to have been known or believed with reports in the US indicating that Russia, and to a lesser extent, China, were still main areas of concern. Gathering information around the world on the status of Y2K efforts required travelling abroad rather than merely relying on the media whose reporters either were not technical experts or were more interested in looking for sensationalist stories.

The focus on readiness, however, was only a partial approach to dealing with the Y2K problem. While knowledge that Y2K repairs or upgrades had taken place might lessen public jitters about disruptions on December 31, 2000, by spring 1999 companies and governments realised that not all computers could be fixed. As importantly, governments and industries realized that it was no longer enough to have one's own systems repaired, but also to know about the efforts undertaken by the company's suppliers and distributors as they, too, either directly or indirectly, affected company operations. In particular, the interdependencies between the telecommunications and energy sectors became evident. Decisions therefore had to be made as to which computers were considered most important, or mission critical, to be fixed first for core government or business operations to be maintained. In addition to such "triage", governments and businesses, including infrastructure operators, focused on contingency planning for the rest of 1999 to ensure provision of service in case disruptions occurred. In the more computer dependent countries, a tension arose for senior officials who had to demonstrate readiness while also having to make contingency planning – the latter being less well understood by the public and, for some persons, calling into question government claims of readiness.

Even in the weeks before December 31, 1999, there remained uncertainty as to how Y2K

would affect information infrastructure. The telecommunications networks expected congestion shortly after each time zone reached midnight, but this was a problem of capacity, not of Y2K. The basic switching of telecommunications networks did not have the Y2K problem to begin with, but the billing, payment, monitoring and other auxiliary functions that used the basic switching systems were expected to incur errors. There would not be a complete outage, but systems would appear to be functioning as normal except that errors occurred in the dates or in calculations using dates.

In the energy sector, however, there were expectations that embedded chips in utilities, gas and oil plants and large complex systems would, if not fixed, cause systems to stop. Embedded chips, of which only about 3-5% of the 25 billion produced had a date function, and even then only those which had data being input required assessing. The chip micro-code was almost impossible to test for every possible logic sequence and combined with the software and hardware in these large plants often being bespoke and updated according to local requirements, these factors also meant there would be a degree of randomness in the occurrence of a Y2K disruption. Precautionary measures were part of contingency planning and thus many complex plants, utilities, mills, chemical plants and other factories, had controlled shutdowns or rescheduled maintenance programs. This process was made easier as the holiday season was a period of slowed activity in any event.[8] Additionally, as safety is a concern for many complex systems, existing in-house emergency services and contingency plans for most mishaps and disasters, for example, using back-up generators for loss of electricity or switching to manual systems, adapted those measures to accommodate the Y2K problem.

What happened?

The Y2K problem has not resulted in long-term strategic or catastrophic security impacts or affected the stability of stock markets or economies. Despite glowing press reports of few Y2K incidents, it is evident that many Y2K disruptions had occurred but technical staff on duty, being the best and brightest, were able to make a quick fix or work around the problems and thus prevent or mitigate a reportable failure. The IYCC and the US Senate Committee on the Year 2000 Technology Problem each produced lists of Y2K disturbances occurring in more than 75 countries around the world.[9] The Y2K disruption to operations of the US reconnaissance and French Syracuse II communications satellites would have been the closest to affecting issues of traditional national security that have been observed. These did not, however, appear to result in serious security problems at that time.

There were few or no confirmed reports of major power outages or communications failures in countries. The main communications issues were problems of congestion just shortly after the rollover occurred in a country. Regarding energy, there were planned reductions of service as part of precautionary measures to prevent unexpected surges; there were reports of minor outages in parts of South America. There were about fourteen reports of Y2K glitches in civil nuclear power plants. These took place primarily in Japan, Spain, the UK, and US, and did not cause safety problems or loss of power production.

Governments and industries and international organizations each had their own requirements for implementing not only plans for repairs and contingency but also the reporting of Y2K incidents. Thus there were varied types of reports; for example, industry used help desks or existing emergency procedures to assess Y2K disruptions at the technical level, while governments were more concerned about the possible effects on public order. Reporting systems which made their results public tended to emphasize impact and failure, rather than cause. Information tended to be filtered to protect commercial proprietary information or for security reasons. Dealing with the temporary fixes as well as non-mission critical systems was delayed until some later date when re-

sources would be available and media attention had diminished. Excepting concern about the leap year date, which also did not result in major incidents, latent effects since the end of February 2000 appear not to have been reported, even if they have occurred.

Protection of critical information infrastructure

The Y2K problem varies in how closely it is representative of the kinds of disruptions expected to affect information infrastructure. While the Y2K problem is studied from many perspectives given its pervasiveness through all sectors of society, it can be seen as a surrogate attack on critical infrastructure.[10] The potentially large impact of the Y2K problem, if repairs had not been made, was compared to that from natural disaster or other worst-case scenarios. It was, however, a known risk with a fixed date and time and occurred in an "artificial" environment as many systems were turned off, on controlled shutdowns, or not subject to regular activity over a holiday period.

The Y2K problem was a vulnerability that is defined as a weakness or feature that exists within a computer or communications network and infrastructure. The Y2K problem emerged from a narrow specification in the formatting of dates in computers, with two rather than four digits used to represent the year. This was a response to what were at the time more serious problems of computer memory space and cost in the early development of computers during the 1950s and 1960s. This formatting, however, became a vulnerability as successive generations of many computers had not corrected it, and, in many cases, the specification could be worked around. Many software developers were not interested in dealing with this issue, as it was not an interesting or challenging problem to solve.

Threats, however, are intentions and capabilities that can use vulnerabilities for unauthorized use, theft or damage to the information or network or infrastructure. They include disgruntled employees, "hactivists", criminals, and professional "infowarriors" working either for governments or corporate entities. These are more widely known in the communications sector, and security measures such as password and access controls, and encryption are among measures often taken to protect information from malicious activity. While the Y2K problem was a vulnerability it was often called a threat to galvanize corrective action. The Y2K problem was often compared to natural disasters, which are categorized by some as threats given the large scale of damage and devastation that often ensues, but natural disasters do not have malicious intent.

Conclusion

The problems for critical information infrastructure are of two kinds: malicious attacks, and vulnerabilities of software, hardware and applications design and implementation. During the 1990s, the plant in the energy sector and in heavier industries have increasingly relied on information and communications technology to monitor plant control and processes, as well as to automate business transactions. One of the main lessons for infrastructure owners, therefore, in particular within the energy sector, is the degree to which incorporating more IT requires a corresponding understanding of both the threats and vulnerabilities which will arise. Utility and plant owners and operators have for decades put into place contingency planning for many kinds of scenarios that affect their physical systems. Thus planning for contingency and for safety was the norm for critical infrastructure owners, and thus provided a sound basis upon which to prepare contingency planning for Y2K disruptions. Issues of information assurance to deal with the new IT issues, which tend to be better understood in the communications sector, therefore, will need to be integrated with more traditional practices related to physical plant and asset protection.

While threats can be managed by adopting some of the various security measures men-

tioned above, the Y2K experience illustrates the importance of adopting good practices for management of technology and information.[11] Unlike the Y2K problem, which was seen as a one-off incident, management and security is a process, and while receiving less media attention than do hackers, it can be more important than preventing malicious attacks. More than 50% of computer disruptions arise from poor IT project implementation (75% of large computer projects are delayed, over budget and do not work as intended), flaws in software, improper configuration of computers and human error. Good IT management can minimize these, thereby allowing more attention to be devoted to dealing with malicious attacks.

To facilitate implementation of technology and information management various international standards exist and new ones are emerging. Prominent examples for consideration include the International Organization for Standardization (ISO) 9000 series for quality assurance management. Secondly, in the UK, in September 1999, the Turnbull Report of the Institute of Chartered Accountants of England and Wales requires companies to raise risk assessment to the level of Board of Directors. This means accountability for disruptions and other irregularities would be in the company's Annual Report and dealt with by other regular review procedures. Thirdly, a management system standard for information security is the British Standards Institute standard BS 7799 which has been submitted to be an international standard in the ISO series.

The Y2K experience also demonstrated the effectiveness of government-industry cooperation to solve complex issues. This cooperation is increasingly important for critical information infrastructure protection. The private owners of infrastructure have direct experience of both vulnerabilities and threats to their assets, but as their systems are critical to a country's economic viability and social and political well-being, then governments require knowledge of incidents of a malicious nature to better fulfil their national security obligations. As attribution of the cause of a computer disruption, however, is difficult to ascertain in the short-term, then more information about both vulnerabilities and threats is required to improve information security. The surveys of the Gartner Group and the Washington D.C. Year 2000 Group were embryonic examples of how some IT information might be obtained. Some of the many international schemes to monitor and share information about Y2K disruptions over the rollover period are now being developed further to deal with other developments in IT and its security. These schemes included that of the IYCC the development of which the July 2000 UN ECOSOC substantive meeting discussed. The successor to the IYCC's global network of national Y2K coordinators might now focus on other IT issues, such as building communications infrastructure in developing countries and promoting e-commerce in others. The scheme set up to monitor Y2K disruptions in civil nuclear power plants might be considered by the International Atomic Energy Agency to deal with other types of accidents or incidents. Such information sharing enables government officials or company Directors and Chief Executive Officers to make decisions to mitigate or reduce potential destabilizing effects as a result of computer incidents, especially as IT systems are increasingly global and interconnected.

While the Y2K experience will not solve all future information security issues, it went a long way to demonstrating how effectively governments and industry worldwide can work together to deal with the large-scale and complex IT issues likely to occur as economies and trade become increasingly interdependent.

Notes

[1]This paper provides some preliminary assessments which are part of a larger project organised jointly by the Center for Global Security Research (CGSR) at Lawrence Livermore National Laboratory and the International Institute for Strategic Studies (IISS), London, on international security implications of threats and vulnerabilities to critical information infrastructure. This work was performed under the

auspices of the U.S. Department of Energy by the University of California, Lawrence Livermore National Laboratory under contract No. W-7405-Eng-48.

[2]During the Asian workshop of the CGSR-IISS Y2K Seoul Conference, October 17-18, 1999, discussion among participants from southeast and east Asia indicated a range of approaches regarding publicity of Y2K: from reporters finding their own stories, to government telling the media what the news was, to no publicity which unnecessarily alarmed a population that was not heavily dependent on computer systems.

[3]See, for example, Nancy Leveson, *Safeware: System Safety and Computers* (Menlo Park, CA: Addison-Wesley, 1995); and Ronald L. Enfield, "The Limits of Software Reliability", *Technology Review*, Vol. 90, No. 3 (April 1987), pp. 36-43.

[4]Presentation by Bruce McConnell, Director, International Y2K Cooperation Centre (IYCC), for CGSR-IISS conference "International Security Aspects of the Year 2000 Issue: Preliminary Assessments of "What Really Happened" and Lessons To Be Learned", January 24-25, 2000, at LLNL at http://cgsr.llnl.gov/Y2KLessonsAgenda.html; and *Y2K: Starting the Century Right*, Final Report of the IYCC, February 2000, at http://www.iy2kcc.org.

[5]"Taking a Hard Line On the Year 2000", *International Herald Tribune*, 12 October 1998, p. 3.

[6]Bruce F. Webster, "The Predicted Impact of the Year 2000 Problem in the United States", The Spring 1999 Survey of the Membership of the Washington D.C. Year 2000 Group, released 10 June 1999, on internet at http://www.wdcy2k.org.

[7]"Millennium Woes", *The Economist*, August 21, 1999, p. 90.

[8]Robert Guy Matthews, "Factories Plan to Halt or Scale Back Operations for Y2K", *Wall Street Journal*, December 20, 1999, p. B4.

[9]Appendix C - International Y2K Glitch Report, *Y2K: Starting the Century Right*, Final Report of the International Y2K Cooperation Centre; see also Appendix II - Summary of Y2K Glitches by Sector, in *Y2K Aftermath – Crisis Averted: Final Committee Report*, Summary of Committee Findings, United States Senate Special Committee on the Year 2000 Technology Problem, S. Prt. 106-XX, February 29, 2000, pp. 37-49.

[10]For preliminary lessons to be learned from Y2K see *Critical Infrastructure Protection: Comprehensive Strategy Can Draw on Year 2000 Experiences* (GAO/AIMD-00-1, October 1999); the UK also produced an excellent report focusing more on IT infrastructure critical for government computer systems and e-commerce in *Modernising Government in Action: Realising the Benefits of Y2K*, Cabinet Office report to Parliament, Command Paper 4703 (London: HMSO, April 2000).

[11]For example, see Timothy Braithwaite, *Y2K Lessons Learned: A Guide to* Better *Information Technology Management* (New York: John Wiley & Sons, Inc, 2000).