AP 237
STC (97) 7
Original : English

# INFORMATION WARFARE AND THE MILLENNIUM BOMB

## DRAFT GENERAL REPORT

***LORD LYELL (UNITED KINGDOM)***
***GENERAL RAPPORTEUR****

International Secretariat 1 September 1997

---

* Until this document has been approved by the Science and Technology Committee, it represents only the views of the Rapporteur.

# TABLE OF CONTENTS

# INTRODUCTION[1]

1. In warfare, adversaries often attack each other's military and civilian infrastructure. Attacks on railways, roads, bridges, power stations, supply depots, communications systems etc. can severely erode an opponent's ability to wage war. Similarly, terrorists often attack civilian infrastructure in order to publicise their cause or try to force a government to change its course. Physical attacks entail physical destruction of the opponent's assets and the attacker risks losing his own personnel and equipment during the attack.

2. Recently, however, concerns have arisen that an attacker could mount severely damaging attacks without using traditional methods of destruction and even without jeopardising his own assets or personnel. The fear is that using information technology alone, an adversary could disable, disrupt or even destroy substantial portions of military and civilian infrastructure. Furthermore, the attacker might well be able to conceal his identity, leaving the victim with no idea about who to retaliate against. This form of warfare - information warfare - is increasingly seen as a grave potential threat to international security. The first part of this Report looks at the nature of this threat and examines the measures that should be taken to minimise it.

3. The second part of the Report deals with another threat to information systems that is causing great concern. In this case, the threat is not disruption of critical information systems by some malevolent foe but rather the inadvertent consequence of an apparently trivial programming technique.

4. In short, when computers were becoming widespread, computer memory was - by today's standards - very limited and extremely expensive. Consequently, programmers frequently used only two digits to show the year, "72" for "1972" for instance. This technique persisted longer than it should have and many programmes have remained in use far longer than their designers expected. Furthermore, many computer chips with instructions built into them only use two digits for the year. If these programmes and microchips are running at the beginning of the next century, the date "1 January 2000" will appear as "1 January 00" and in many cases the programmes or equipment will assume that the date is "1 January 1900". Unless these problems are corrected, computer and component failures could occur on a massive scale but preventing them will cost billions of dollars globally.

5. Some experts fear that the consequences of this could be so severe that it has been labelled the "millennium bomb" or, more prosaically, the "Year 2000" or "Y2K" problem. The second part of this Report examines the extent of the problem, the actions being taken to deal with it, the costs involved, and the likely consequences of the "millennium bomb".

---

[1] The Rapporteur would like to thank Peter Barschdorff, Reto Haeni and Adrian Petrescu for their assistance in preparing this Report.

# I. INFORMATION WARFARE

6. Information Technology (IT) is vital to the functioning of developed societies. Virtually no aspect of modern life is unaffected. Telecommunications are routed by computer, and computer networks are used to control traffic on the roads, railways and in the air. Government departments, law enforcement authorities, international organisations, the military, companies, research institutions, universities, hospitals, banks, stock exchanges etc. store information and exchange information electronically. In the United States alone, about a trillion dollars are transferred every day via electronic networks. Furthermore, personal computers connected to the Internet are found increasingly in homes and businesses. In 1996 *Microsoft* estimated that 48 million people use the Internet, with 30 million using the World Wide Web. Seventy-five per cent of users were in the United States and eleven per cent in Europe.[2] In July 1997, *Scientific American* cited a study that put the number of Internet users at 57 million plus another 14 million who only have E-mail access. Only 17 nations with populations greater than one million are not connected to the Internet.[3]

7. It is, however, becoming increasingly clear that the dependency on information technology could be a critical vulnerability. The breakdown or manipulation of certain information systems could disrupt military operations, place lives at risk and cause the loss of billions of dollars. Yet while many systems are designed to cope with accidental failures or breakdowns, computer networks are increasingly based on standard, widespread technology, and alarmingly few seem well protected against wilful, hostile attack. Only recently have governments and industries begun to pay serious attention to the potential threat of "information warfare".

## A. DEFINING INFORMATION WARFARE

8. The use of information in warfare has been recognised since ancient times. Over two and half thousand years ago, the Chinese strategist Sun Tzu included the principle of denying an adversary his eyes and ears in his methods for winning war. Modern warfare also emphasises information manipulation and denial using, for instance, tactical and strategic deception, propaganda to undermine an enemy force's morale, and the jamming or physical destruction of command and control systems.

9. Information warfare, however, extends far beyond the traditional battlefield and its possible perpetrators and victims are by no means confined to the military. It is useful to look at a few definitions that have been put forward recently.

---

2 "Net Facts Burst Ads Bubble", *Financial Times*, 7 October 1996.
3 "Access to the Internet", *Scientific American*, July 1997, p. 18.

10. The United States Joint Chiefs of Staff have defined information warfare as:

> *"Actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems and computer-based networks while defending one's own information, information-based processes, information systems and computer-based networks."*[4]

A report by the German Bundestag describes it as:

> *"The comprehensive use of information and communication technology as well as technologies for the disturbance and destruction of hostile information and communications systems (IaC systems) in crisis and conflicts, in order to gain strategic and tactical superiority."*[5]

The *Economist* has described information warfare in more accessible terms by saying that:

> *"Information warfare could mean disabling an enemy by wrecking his computing, financial, telecommunication or traffic control systems. The relevant weapons might be computer viruses, electromagnetic impulses, microwave beams, well-placed bombs or anything that can smash a satellite."*[6]

11. All these definitions include the military dimension of information warfare. This can entail anything from deception and electronic jamming to the use of traditional military methods to attack or undermine an adversary's information systems such as military communication centres, information-gathering and communications satellites, telephone exchanges, railway control centres, etc. But the term information warfare as it is understood today extends the scope into a much broader field. In the same way that civilian physical infrastructure is often seen as a legitimate military target, so must civilian information infrastructure. In addition, the perpetrators of information warfare need not be a clearly defined, opposing armed force. Indeed, as will be examined later in this Report, information warfare could waged by an extraordinarily diverse range of foes based almost anywhere on Earth. Information warfare can be "invisible" and the perpetrator can be difficult, perhaps even impossible, to identify. Secrets can be stolen or information manipulated without the victim's knowledge. And even a more destructive attack which perhaps disables a computer network could be executed by a teenage hacker, a terrorist or a hostile government who conducts the attack in such a way that it cannot be traced. This Report focuses on the use of information technology as a means of attack and as a source of vulnerability.

## B. CATEGORIES OF INFORMATION WARFARE[7]

---

4 Reto Haeni, "Information Warfare: An Introduction", *Soldier-Scholar,* Vol. III, No.1 (Fall 1996), pp.3-10.; also quoted in a similar form in Cooper, Jeffrey R., "Another View of Information Warfare", in *The Information Revolution and National Security, Dimensions and Directions*, Schwartzenstein, Stuart J.D. ed., CSIS 1996, p. 114, the author quoting in turn a briefing by Barry Horton, PDASC C3I, March 27, 1995.

5 Assessment of the Consequences of Science - Report from the Committee for Education, Science, Research, Technology and the Assessment of the Consequences of Science of the German Bundestag, 9 December 1996, p.49

6 "Future of Warfare", *The Economist*, 8 March 1997, pp. 22-24.

7 This categorisation was formulated by Winn Schwartau in his book "Information Warfare: Chaos on the Electronic Superhighway",. *Thunder's Mouth Press*, NY, 1994

12. Information warfare is certainly not limited to military-versus-military engagements or even nation-versus-nation ones. Broadly speaking, it can be performed at three levels:

- Personal Information Warfare
- Corporate Information Warfare
- Regional or Global Information Warfare

13. Personal information warfare concerns attacks against an individual's electronic privacy. An enormous amount of personal information is stored on computer. This includes medical records, credit ratings, bank balances and account numbers and criminal records. Personal privacy can be invaded by simply accessing this information and making it public. But it is also possible to steal credit card information and use it to make purchases or even to create false information that at the very least could cause great inconvenience. It is even possible to envisage an extreme form of personal attack that has been labelled “stealing of identity”. This would entail registering changes of address for a victim’s identity papers, credit cards, medical records and other electronically-stored information, and re-routing or blocking all telephone calls. Apart from the obvious inconvenience, the victims could lose large amounts of money, lose his credit rating and perhaps acquire false criminal and medical records.

14. Corporate information warfare involves the use of information technology to obtain commercial secrets or harm a competitor. One scenario that has been used to illustrate this aspect is a company that invests $1 million to break into a competitor’s database and copy research results worth $15 million. The victim’s computer could then be sabotaged with a virus which might corrupt the original information and prevent the victim being the first to market products based on the research. Such action could apply to companies working in a research-intensive area such as pharmaceuticals, chemicals, aerospace or information technology, but less dramatic thefts of commercial information could also take place. Information about suppliers, customers and corporate strategy could also be very valuable for a competitor.

15. Global information warfare refers to larger scale information warfare targeted against a nation. Specific targets could include industries, government departments, military systems, banking and national infrastructure such as communications, transport, and energy supply. According to one estimate, a nation investing about $200 million a year for three years on information warfare would be able to cause untold damage to an advanced nation’s industry and infrastructure. Just one form of damage could be a Wall Street collapse that would dwarf all previous crashes.

## C. PERPETRATORS AND INSTANCES OF INFORMATION WARFARE

16. In 1996, the United States Defense Science Board produced a comprehensive assessment of the information warfare threat.[8] This identified the following possible sources of information warfare threats:

- Incompetent, inquisitive, or unintentional blunderers, mischief-makers and pranksters
- Hackers driven by technical challenge
- Disgruntled employee, unhappy customer intent on seeking revenge for some perceived wrong
- A crook interested in personal financial gain or stealing services
- Major organised crime operation interested in financial gain or in covering their crimes
- Individual political dissident attempting to draw attention to a cause
- Organised terrorist group or nation state trying to influence US policy by isolated attacks
- Foreign espionage agents seeking to exploit information for economic, political, or military intelligence purposes
- Tactical countermeasure intended to disrupt specific US military weapon or command system
- Multifaceted tactical information warfare capability applied in a broad orchestrated manner to disrupt a major US military mission
- Large organised group or major nation-state intent on overthrowing the United States by crippling the National Information Infrastructure

[8] "Report of the Defense Science Board Task Force on Information Warfare - Defense", Office of the Under Secretary of Defense for Acquisition and Techology, November 1996. http://jya.com/iwdmain.htm

17. The report also produced an estimate of the likelihood of each of these threats as shown in Table 1. It should be noted, however, that some independent analysts believe that this understates potential threats.

Table 1

| | Validated Existence* | Existence Likely but not Validated | Likely by 2005 | Beyond 2005 |
|---|---|---|---|---|
| Incompetent | W | | | |
| Hacker | W | | | |
| Disgruntled Employee | W | | | |
| Crook | W | | | |
| Organised Crime | L | | W | |
| Political Dissident | | W | | |
| Terrorist Group | | L | W | |
| Foreign Espionage | L | | W | |
| Tactical Countermeasures | | W | | |
| Orchestrated Tactical IW | | | L | W |
| Major Strategic Disruption of US | | | | L |

*Validated by the Defense Intelligence Agency. W= Widespread; L= Limited

18. The Defense Science Board Report cited several examples of information warfare that have already taken place.

19. During *Desert Storm*, Dutch teenagers modified or copied sensitive information related to military operations in the Gulf. In 1994, an international organised crime group used the electronic transfer system and the international phone network to gain access to a Citibank computer and transfer approximately $12 million to their own accounts. In a test of network security, a United States Air Force officer managed to access the command and control system of a navy vessel at sea via the Internet and Siprnet, a military version of the Internet. (The loophole that enabled this has since been closed.)

20. The Federal Bureau of Investigation (FBI) has also cited several incidents that fall into the category of information warfare. These include:

- A company controlled by an unspecified foreign government sought proprietary documents and information from its American competitors
- A foreign competitor acquired technical specifications from an American vehicle manufacturer
- A foreign company tried to acquire an American company's restricted radar technology
- Several American companies reported the targeting and acquisition of proprietary biotechnology information

- One American company reported the theft of microprocessor manufacturing technology

21. A few details of specific cases indicate why concern about information warfare has arisen. In September 1993, the computer systems manager for the United States National Weather Service discovered that hackers had penetrated the computers relied upon by American weather forecasters. After a long series of "cat and mouse" games involving other computer managers and specialists from the Federal Bureau of Investigation, the hackers were traced to Denmark and were arrested in December 1994. It turned out that the hackers - aged from 17 to 24 - had accessed computers all over the world. Although the hackers had done little damage, their calls had been paid for by charging over $1 million of telephone calls to users in the United States. Furthermore, they could have caused far more harm, for instance, by shutting down airlines in the United States by depriving them of weather forecasts.[9]

22. In another case, the United States had to shut down 200 computers at an intelligence and communications laboratory in Rome, NY when a hacker inserted "sniffer" programmes in the computer network. These programmes covertly gather user names and passwords which can then be collected and used by hackers. The shutdown cost $500,000 and it transpired that the same hacker had stolen secret information from computers elsewhere including South Korea's Atomic Research Institute. The perpetrator turned out to be a British teenager.[10]

23. Instances of teenage hacking should not be dismissed as just a new form of adolescent mischief. There are suspicions that some hacking groups - perhaps unknown to most members of the groups - have had connections to foreign intelligence services. And in any event, these cases of hacking illustrate just how easy it can be to penetrate important computer systems with modest equipment and little expertise. Dedicated specialists with more resources behind them could certainly penetrate computer systems in ways that would be more damaging and more difficult to detect.

24. In fact, a group of Dutch hackers approached Iraqi diplomats in Paris during *Desert Shield* and offered for a million dollars to disrupt the network handling logistics messages between bases in the United States and military units in Saudi Arabia. The offer was rejected but after the conflict Pentagon planners realised that 25 per cent of the message flow into Saudi Arabia was being handled, uncoded on the Internet and the supply system for vital spare parts could have been severely disrupted by an information warfare attack.[11]

## D. PROBLEMS OF INFORMATION WARFARE

---

9 John J. Fialka, "War by Information", paper presented at the conference on "Economic Espionage, CberTerrorism and Information Assurance", Brussels, Belgium 8-9 May 1997.

10 Ibid.

11 Ibid.

25. It is worth reiterating a few features of information warfare. One is the potential difficulty of tracing the perpetrator of an attack. Information warfare attacks can be launched from virtually anywhere. Furthermore, the equipment and expertise needed to conduct information warfare are extremely widely available. Standard computer equipment can easily be used as an information warfare weapon. Whereas a terrorist planting a bomb must acquire explosives and approach the vicinity of a target, an information warrior can obtain the tools of the trade without arousing suspicion and can be thousands of miles from his victim. Consequently, there is no reliable way of anticipating an attack since it could arise from innumerable sources and locations.

26. Another feature of information warfare is the rapid evolution of the "weaponry" involved. Information warfare does not depend upon the development of new hardware but instead relies on progress in software which can be extremely swift. An analogy can be drawn with computer viruses. Software to deal with viruses must be up-dated frequently because virus designers regularly produce new ones to defeat such software. Similarly, the development of information warfare techniques and tools requires constant attention to, and appropriate dissemination of, defensive measures.

27. It is very difficult to estimate the scale of the current and future threat of information warfare. There is evidence that violations of computer security are only rarely reported even when a crime is committed, perhaps to avoid attracting adverse publicity and undermining shareholder confidence. This problem also appears to be prevalent in the military sphere.

28. The Defense Information Systems Agency (DISA) reported that it had responded to 255 computer security incidents in 1994 and to 559 incidents in 1995. Of these, 210 were intrusions. In 1995, DISA attempted to use widely available computer hacking methods to attack 26,170 Department of Defense computers. DISA found that 3.6 per cent of these computers were easily exploited and that 86 per cent could be penetrated by exploiting the "trusted" relationships between machines on shared networks. Only 2 per cent of intrusions were detected and of these only 5 per cent were reported. These figures suggested that 200,000 intrusions might have been made during 1995.

29. Companies such as Exxon, Boeing, Motorola, and GTE have over 100 registered networks and the Department of Defense (which has more than 2.1 million computers) has over 10,000 local area networks and over 100 long-distance networks. So how many networks might be vulnerable? In a survey conducted in November and December 1996, a computer specialist conducted an unauthorised survey of 2,200 World Wide Web sites run by banks, credit unions, the United States government, newspapers and companies trading electronically on the Internet.[12] More than 60 per cent of the sites could be broken into using a widely available software tool that tests network security. Only three of the sites surveyed recognised that the attack was taking place. This survey probably overstates the problem since organisations that need to protect sensitive information usually "insulate" their publicly accessible Web sites from their internal networks. Even

[12] Mark Ward, "Web Sites Are a Hacker's Heaven", *New Scientist*, 18 January 1997, p. 18.

so, it shows a widespread disregard for the potential problems of unauthorised computer access.

30. Other problems have been illustrated by simulations. In 1995, the RAND Corporation conducted a military simulation exercise with the "action" taking place in the year 2000. In the scenario, Iran unsuccessfully demanded that Arab oil-producing states cut production by 20 per cent and it then mobilised for war. Against a background of domestic unrest in Saudi Arabia, a clash took place between Saudi missile boats and Iranian warships lurking near a Saudi naval base. Saudi and Iranian aircraft became involved and American aircraft in the area were targeted by an Iranian frigate. American forces destroyed the frigate and several Iranian aircraft.

31. Participants in the war game included senior experienced military personnel, Defense Department officials, representatives from think tanks and from high-technology companies. They were prepared to implement GREEN HORNET, a plan to send five heavily armed divisions and three carrier battle groups into the region, and NET MASTER, a plan using computer attacks and jamming to destroy Iranian telecommunications, energy, transportation, banking and information systems. NET MASTER's goal was to destroy Iran's economy with little physical damage and few casualties.

32. The scenario continued with American peace groups opposing United States involvement. Key civilian and military telephone systems failed and a passenger train from New York crashed into a freight train that was re-routed on to its track. CNN went off the air and the New York stock exchange plummeted as investors fled from electronically controlled markets. A French airbus crashed on approach to Chicago when its electronics failed and Pentagon technicians found an electronic "worm" that was disrupting computers controlling the deployment of military units. The Bank of England reported fears of massive losses after discovering that its computer controlling money transfers had been penetrated. A computer error triggered an explosion in Saudi oil-pumping station and Saudi television broadcasts were replaced by images of prominent underground leaders calling for the overthrow of Saudi Arabia's rulers. At the same time, the nation's cellular phone system failed completely.

33. As these events unfolded, the scenario's players argued about how to react. Although Iran seemed the obvious culprit, intelligence experts doubted that Iran had the necessary technical abilities and instead suspected American groups while other sources suggested unidentifiable groups in Europe and the Middle East. The result was that the players could not agree who to retaliate against or how to do so. One of the group leaders described the general tone as "bafflement" and noted that in the real world, leaders would have been forced to make decisions but would have been very frustrated with the "thin" basis upon which they had to make them.[13]

---

13 Fialka, op.cit.

34. The Defense Science Board Report acknowledges the validity of the type of scenario described:

> *"Unlike an attacker in conventional war, an attacker using the tools of information warfare can strike at critical civil functions and processes such as telecommunications, electric power, banking, or transportation and other centres of gravity or even at the stability of the social structure, without first engaging the military. Such a strategic information warfare attack can occur without forewarning or escalation of other events. In addition, attacks on the civil infrastructure could impede the actions of the military as much as a direct attack on the military's force generation processes or command and control."*[14]

## E. CONCLUSIONS

35. The Internet was originally created by the United States Department of Defense as a means of maintaining communications in the event of a large-scale nuclear attack. It is therefore ironic that what was once seen as a key element in national defence is now seen as a source of increased international vulnerability. For the moment, the main information warfare threats concern international and industrial espionage and theft. However, acts of terrorism and ultimately strategically damaging incidents seem set to emerge. In the United States, the Defense Science Board suggested spending about $3 billion over the next five years on measures to protect against information warfare and some analysts feel that even this would be insufficient.

36. At present, the United States - as the nation most heavily dependent upon information technology - faces the greatest threat, but other advanced industrial nations are not far behind. However, they seem ill prepared to deal with information warfare threats. Part of the problem is that it is by no means obvious which agencies should prepare to deal with information warfare threats. Military agencies are already acting in concert to defend military information systems from information warfare attacks. No doubt military organisations are also formulating measures to conduct offensive information warfare operations. However, while the military clearly must defend civilian physical infrastructure against military attack, it not clear that the defence of the civilian information infrastructure is a task best suited to the military alone or even that the military alone could mount an effective defence of the civilian information technology infrastructure.

37. An effective response to information warfare threats can only be devised by bringing together military and civilian agencies and industry. Although the military seems now to be well aware of the threats to military systems and to civilian systems upon which the military depend, it seems that there is a need to heighten awareness of the threats to civilian systems and to involve the operators of these systems in formulating appropriate responses. Furthermore, in view of the global nature of information technology, effective action will have to be international. Certainly, the NATO nations and their partners should make every effort to assess the nature of the information warfare threat and consider how best to develop effective countermeasures.

---

[14] Op. cit., Note 7.

* * * * * * * *

# II. THE MILLENNIUM BOMB

## A. THE YEAR 2000 COMPUTER PROBLEM DEFINED

38. Computer technology has advanced at a remarkable rate over the last two decades. Components have consistently increased in power while their size and cost has fallen. Computer power that once would have filled a large air-conditioned room, now sits comfortably on a desktop. At the same time, the applications for computers have grown dramatically so that in the industrialised world, computers now lie at the heart of devices from nuclear power stations to refrigerators.

39. It is easy to forget that in the early days of the information revolution, computer resources were far more limited - and expensive - than they are today. Programmers had to take great care to use the resources available as efficiently as possible, and one commonly used technique was to restrict the use of computer memory and processing time by using only two digits to show the year. This practice was particularly common in the 1960s and 1970s when the end of the millennium was a more distant prospect and programmers had every reason to believe that their programmes would be replaced long before the year 2000. This need to avoid using just two bytes of data sowed the seeds of the "millennium bomb", also known as the "Year 2000" or "Y2K" problem.

40. The essential problem is that when the new millennium begins, computers and computer chips that only use two digits to show the year, will revert to "00". Although it would be obvious to a human being that this means "2000", many susceptible computer chips will assume that the date is "1900". And it is believed that many computer chips, even those built more recently, will be vulnerable.

## B. THE EXTENT OF THE PROBLEM

41. Our lives depend on computers far more many people realise. Computers lie behind electrical power and mail distribution, financial institutions, telephone networks, air-traffic control, airline ticketing, traffic lights, social security systems, salary calculations and, of course, defence systems. Furthermore, machines such as satellites, cars, aircraft, video players, burglar alarms, lifts, and microwave ovens contain microchips that could be vulnerable to the Y2K problem.

42. The estimates of the costs of dealing with the Y2K problem globally are astonishing, with some as high as hundreds of billions of dollars.

43. In fact, the Y2K problem has already begun to manifest itself. Some companies have discovered that their computer systems will not accept dates after the millennium so

that computer operators attempting to register credit card expiration dates of “00” have been confronted by messages such as “Year must be in the future”.

44. Furthermore, many companies have begun to realise that because their computers interact with those of suppliers, distributors and other partners, even if they themselves have a system which is “Year 2000 compliant”, they will still encounter problems if their partner companies’ systems fail.

45. Unfortunately, awareness of the problem is often lacking and complacency is also a problem. Surveys have indicated that managers often do not understand the issue or its complex implications. Reactions such as “I retire before then”, or “Bill Gates will find a solution” are not uncommon. Those who do appreciate the problem find that solving it will be a difficult task. Many computer systems were programmed 20 to 30 years ago and the programming languages are no longer used. Many of the original programmers have retired or are dead and the documentation for the programmes is poor or non-existent. The number of companies offering solutions is increasing daily but it is difficult to know whether they actually possess the necessary expertise. Certainly, some questionable “silver bullet” solutions have appeared.[15] Analysts point out that the problem can manifest itself in a remarkable number of ways and each can require its own custom-made solution. There are no less than 30-40 different operating systems in use and a much higher number of programming languages used by various types of computer systems. Each of the possible combinations requires a different approach and, of course, differently qualified specialists to solve specific Y2K problems.

46. Moreover, these types of solution only apply where it is possible to solve the problem by programming. Many systems actually use computer chips which have their programming built in and which must be replaced. If the system in question is an old VCR, buying a replacement might be an irritating expense but with other systems, the consequences are far more severe. One example concerns medical infusion pumps. These have to be calibrated every six months and some types cease functioning if they have not been calibrated in that time. British hospitals use hundreds of thousands of these types of pumps and their simultaneous failure would clearly be both dangerous and inconvenient.[16]

47. Robin Guenier, the head of the British-Government-sponsored “Taskforce 2000” which has been charged with assessing and finding solutions to Y2K problems in the United Kingdom, has explained other circumstances where a microchip replacement can cost millions of pounds.

> *“The microchip controls when the bank vault can be opened and closed. It allows the vault to be opened during the working week but keeps it closed at weekends. For security reasons it has been buried inside the 20-ton-door of the vault, and can only be inspected by removing the whole door. The big problem arises because the bank*

---

15 For a comprehensively explained argument, see *“Biting the Silver Bullet”*, by Peter de Jager.

16 Alan Cane, “Microchip Inaction Makes a Date with Disaster", *Financial Times*, 6 March 1997.

*building has been built around the vault, again for security reasons. So to inspect or change the microchip requires half the building to be demolished and the door removed. The people who built the chip, the vault and the bank never imagined that the chip would have to be removed in the lifetime of the building... So, to ensure depositories have access to their deposits [after 1 January 2000], the bank building has to be demolished. That sums up the millennium problem."*[17]

## C. RESPONSES

48. Taskforce 2000's estimate of the costs for defusing the millennium bomb in Britain is £31 billion. This is based on the cost of employing an extra 263,000 specialists in the private sector to deal with the problem at an average £45,000 per year for two years, which comes to £24 billion. The public sector costs will amount to estimated extra £7 billion. Other sources suggest the costs could be even higher.[18] The National Westminster Bank has already set aside £100 million, and British Telecom expects to spend at least £300 million.[19]

49. Estimates of the global costs are as high as $600 billion and not dealing with the problem would be even more costly, so it is hardly surprising that the millennium bomb has been dubbed "the most costly computer error ever".

50. As noted earlier, responses to the Y2K problem vary greatly. With just over two years before the year 2000 companies or government agencies that have recognised and assessed the problem are still rare. A survey taken by Morgan Stanley & Co. Inc. in the United States concluded that "most of the Year 2000 spending still lies ahead. Many companies are still in the awareness (29%) and inventory-and-impact analysis (24%) phase; very few have re-implemented code back into production (6%)".[20] In the United Kingdom, Taskforce 2000 believes that only about 10 per cent of British businesses have started work on the issue.

51. As for government agencies, the United States Army, for example, has demonstrated its awareness of the problem with the Army Chief of Staff and the Secretary of the Army, issuing a priority memo which postpones all non-essential "sustainment and enhancement requirements" until systems have been "analysed, fixed tested and certified Y2K compliant".

52. Hardware and software manufacturers have, of course, started producing and advertising either Y2K compliant systems or Y2K "fixes". IBM announced in 1995 that it "will provide customers with a comprehensive set of services, tools and support for their

---

17 Frank Kane, "Moving to Millennium Meltdown", *The Sunday Times*, 11 May 1997.

18 Ibid.

19 Peter Warren, "Computer Chaos in 2000 May Stop Cars and Fridges", *The Sunday Times*, 6 April 1997 and Frank Kane, op. cit.

20 *US Investment Research: Year 2000 Watch: Survey at Year 2000 Conference,* Morgan Stanley & Co. Inc., April 1997.

Year 2000 transitions".[21] From a 180-page free Y2K resource guide available on the Internet and to fee-based "Transformation 2000 Services", IBM is offering a wide range of solutions.

53. Articles on the year 2000 problems abound in computer, management and financial magazines. Internet sites on the Y2K problem are increasing and one site alone listed 134 articles published in July 1997 alone. The first lawsuit regarding the Y2K problem has also been filed by an American retailer against a computer supplier. The retailer's computer system - installed in 1995 - has failed to recognise credit cards with expiration dates after the year 2000 and has shut down 105 times due to this problem.[22] Lawyers are expecting many similar suits.

54. Nations that are less dependent upon information technology face fewer problems but, even so, awareness of the problem seems limited. Former Soviet President Mikhail Gorbachev has said that Russia has not begun to address the problem systematically, and when it does, it will have little money to deal with the problem.[23] He has therefore solicited American assistance in assessing Russia's Y2K problem and dealing with it. Although raising funds will be an uphill struggle, it is worth pointing out that the West does have a stake in Russian financial and military stability which could be adversely affected by the Y2K problem.

## D. CONCLUSION

55. The Y2K problem is multifaceted and will be costly to put right. Experts are generally agreed, however, that it would be far more costly to try to solve the problems only when they appear. Awareness of the Y2K problem is still surprisingly low and the readiness to deal with it, even lower. Governments have a responsibility to ensure that their own information systems are Y2K compliant and to increase corporate awareness of the problem. Only a little time remains and - unlike many other problems - this one cannot be postponed. Many faulty clocks are inexorably ticking their way towards the year 2000 and the millennium bomb.

_____

21 *IBM Year 2000 Efforts Under Way*, Armonk, NY, October 30, 1995.

22 "Supermarket Sues over Tills that Fail to Handle Year 2000", *The Sunday Times*, 17 August 1997.

23 Brian Knowlton, "Will America Help Russia Reach 2000", *International Herald Tribune*, 26 May 1997.