AN ABSENCE OF MALICE: COMPUTERS AND ARMAGEDDON

Perry R. Morrison

This paper addresses the impact of computers on the nuclear arms race and argues that improvements in computer technology have directly led to the diminishing warning and decision period available to human commanders in the event of an accidental outbreak of nuclear war. To support this thesis, a brief and general history of the application of computers to strategic weapons systems is given and evidence is presented which confirms the unreliability and error proneness of current computer-based weapons control systems. The main point of discussion however, involves an emerging proposal to completely automate the strategic systems of the United States and the associated problems and dangers, given present inadequacies.

Keywords: computers, computer error, nuclear war

It is sobering to think that after thousands of years of civilisation, current circumstances indicate that its end could take place with perhaps no more than five minutes warning. Further, if present trends continue, the destruction of life, our civilisation and our planet, may occur without any warning at all. It may also be the supreme irony that, after centuries of war, revolution and oppression, such an event may happen without the slightest trace of human malice to accompany it. This situation is due almost entirely to the past, present and likely future application of computers in the strategic defence systems of the superpowers and this paper will briefly discuss some of the relevant historical antecedents to this situation and focus on the consequences of present developments.

THE SHORT HISTORY OF COMPUTERS AND NUCLEAR WEAPONS

Historically, the application of computers has allowed us to speed up whatever process we happened to apply them to, and this is also true for their use in strategic weapons systems. In the 1950s, it would have taken almost three hours to begin a nuclear war. B-52 bombers, which were at that time the front line deterrent of US strategic forces, would

have taken that long to fly to Soviet territory and drop their freefall weapons. Obviously, the Soviet Union was similarly constrained. However, with the development of smaller, more powerful computers, there emerged the possibility of placing them inside missiles so that the warhead the missile carried could be released at the appropriate moment in order to hit its target. This meant that enemy forces would have a harder time preventing warheads landing because they were harder to intercept than bombers carrying gravity weapons. It also meant that the time needed to conduct a nuclear war had shrunk to around half an hour or less. However, as we shall see, although changes in weapons technology and strategy (in this instance a change in the weapons vehicle itself) have appeared as major factors in the arms race, such changes have emerged basically as a result of advances in computer technology and application.

By the late 1960s it became clear to US strategic planners that a relatively cheap way of staying ahead in the nuclear arms race was to abolish the idea of placing one warhead on one missile. Instead, it was more cost effective to piggyback a number of warheads on the one missile and release them at different points so that they could explode over different targets. Thus, the MIRV (multiple independent re-entry vehicle) was born, but again only after computer technology had become smaller and sophisticated enough to handle the extra complexities of multiple warheads.

Since that time, improvements in computer technology have markedly increased the accuracy of warheads. For instance, there is a 50 per cent chance of a Mark 12A re-entry vehicle (carried by the Minuteman III missile) landing within 200 metres of a target, after travelling 13,000 kilometres.[1] The newer Trident and MX missiles have even better performance, and Soviet missiles are reputed to be slightly less advanced. However, the latest trend to increase missile accuracy is called MARVING. In this scheme, the warheads have the ability to control their own aproach to the target and make small corrections to their trajectory based on navigational information. Once more though, the application of this technique depended upon the development of ever smaller and more powerful computers and the application of artificial intelligence techniques of pattern recognition.

Finally, the controversial cruise missile also relies heavily on sophisticated computer technology so that it can track the terrain over which it flies, thereby remaining on course while it travels low and fast to avoid enemy defences. Even with such technology, this weapon has had extensive teething problems, but without it the mission of cruise would be quite impossible.

Clearly then, as in most other applications of computer technology, the end result of these efforts has been the creation of weapons

systems which are smaller (hence transportable), more accurate and very powerful. This has directly led to the situation where small, mobile and very powerful weapons such as Cruise, SS-20, and Pershing II are now deployed in Europe,[2, 3] thereby reducing the time it takes to begin a nuclear war (at least in a European context) to around seven minutes, since the in-flight time of these weapons is of that order. However, if one considers that surveillance satellites designed to detect missile launches need between two and two and a half minutes to process launch data,[4] then the decision period in a European conflict dwindles to somewhere between four and five minutes. Missiles from Soviet submarines operating off the US coast have similar flight times, and at the time of writing have shown increased activity in these waters.

The major and most obvious point, however, is that the application of computers to nuclear weapons systems has directly reduced the time allowed for proper detection of an attack, let alone the period needed for dialogue in the event of an accidental outbreak of nuclear war. Ironically, as we shall see, such an accident is more likely to be generated by computer error than human agency.

COMPUTER ERROR AND EMERGING POLICY

Increases in Soviet missile accuracy have caused US authorities to become concerned about the possibility of a Soviet first strike destroying American missiles in their silos. This is one of the major considerations behind the development of the MX missile and its various novel (but now abandoned) deployment strategies and has also prompted support for the 'launch on warning' policy whereby missiles are launched as soon as an attack is detected.[5] Considering the short flight times that now exist with the deployment of weapons like Pershing and SS-20, it is obvious that we are now placed in a very much more precarious position than even at the height of the cold war. With a 'launch on warning' strategy in these circumstances, we are placing an unprecedented amount of trust in our computers. Is this trust justified?

Consider the following facts. In October 1960, the US early warning system detected incoming missiles and proceeded to pass through all five levels of alert. After 20 minutes (and some coolness on the part of the commanders involved) it was discovered that the system had detected the moon emerging above the horizon and the computer system involved had lost the most significant digits of the radar return, so that a distance of a quarter of a million miles had been reduced to around 2,500.[6] On 3 June 1979, the NORAD computer issued a warning that the USSR had launched ICBMs against the US.

This alert lasted three minutes. In October 1979, a piece of space debris re-entered the atmosphere and was mistaken for a submarine launched ballistic missile. In December 1979, a test tape was accidentally loaded into the early warning system and bombers carrying nuclear weapons took off before the error was detected. Six months later in June 1980, within a period of four days, two computer-related false alarms sent B-52 bombers and battle control aircraft into the air. A congressional enquiry determined that a single faulty circuit was to blame.[7] Another enquiry into the Strategic Warning System headed by Senators Goldwater and Hart determined that during an 18 month period the system suffered 151 false alarms, one of which lasted six minutes.[8, 9] The General Accounting Office established in 1979 that the World Wide Military Command and Control System (of which the Early Warning System is a part) was 'not reliable' and the testimonial of a former WIMEX chief engineer indicated that the system failed on average, once every 35 minutes.[10] Using such freely available figures, Kochen has calculated that there is a 50 per cent chance of an accidental outbreak of nuclear war occurring within the next 19 years.[11]

Clearly, one cannot deny that computers are inherently more reliable than humans, yet despite this, their record in safeguarding the world is not enviable and in the situation now emerging through their application, where the opportunity for human intervention is becoming severely limited, one could strongly argue that the only adequate system will be one that is completely error free. Obviously, as many computer specialists are aware, such a system is impossible to construct. Perhaps of even greater relevance is the degree to which present systems fall short of this ideal.

THE REALITIES OF COMPUTER CONTROL

The US Department of Defence is troubled by the existence of many different makes of computers, most of them with some degree of incompatibility, running completely different languages, different versions of the same language, or with nonstandard, local hardware and software modifications. For example, while the Naval Material Command may not be a fighting unit, nevertheless it has over 450 different systems and subsystems (the number is doubling every year), and utilizes about 50 million unique lines of computer code. It is conservatively estimated that for every 1000 lines of code written there are between ten and 80 defects which have to be identified and eliminated.[12] The way in which this debugging is carried out is almost completely empirical in nature. Although these techniques are often quite sophisticated, for programs with over a million lines of code,

complete testing of all the possible input/output combinations is beyond the capacity of even the fastest computer and a programmer's confidence that all flaws have been weeded out is based more on hope than fact. This problem, which is essentially the difficulty in proving that a program actually does what it was designed to do (and nothing more or less) has been termed 'program verification' and obviously becomes even more problematic the longer and more complex a piece of software becomes. Despite some attempts on the part of mathematicians to prove programs correct through formal logic and careful program specification, in real world applications this approach fails under the weight of practical needs, time constraints and the limitations of available systems. In short, the ability of human designers to guarantee the correctness, integrity and infallibility of their software is severely limited. The problem of software errors in isolated computers is magnified further in strategic weapons systems where many computers charged with different tasks run different programs and are required to interact and respond on the basis of other computers' information.

One of the more illuminating examples of military computer error occurred during the 1973 Yom Kippur war, when the Israeli Air Force requested replacement canopies for some of its damaged Phantom jets. The US Air Force's Advanced Logistics System, which was intended to provide management and control of more than six million spare parts, failed to locate the needed components. A manual search of the warehouses by hundreds of personnel managed to find the canopies — but only after the war had ended.[13]

The Department of Defence is of course not unaware of these problems and has attempted to resolve most of them by designing a standard language for all applications. This language, called Ada, is a structured PASCAL-like language meant to enforce logical program design (and hence easier debugging) by its very nature. There have been several criticisms of this language however, particularly in regard to its complexity and immense size. Some have argued that the designer's attempt to create a language that is all things to all people, has made the language so complex and large that most programmers could not learn it in its entirety.[14] Hence, Ada may not be the solution that the DOD is counting on.

ARTIFICIAL INTELLIGENCE AND ARMAGEDDON

The above discussion has attempted to demonstrate that the computer's general effect in speeding up the rate of a process has dangerously diminished the time factor involved in nuclear war, so that the potential for human decision-making, dialogue or

intervention is almost precluded. Quite paradoxically, our shrinking capacity to effectively command in such circumstances will require us to become even more dependent upon automation for the detection and conduct of nuclear conflict. Hence, given this vicious circle that is eroding the capacity for human command and replacing it with automation, and the imperfect nature of computers, it is not difficult to see that world peace will be placed increasingly in jeopardy by the emergence of systems for automated control of a strategic response.

Some developments on the horizon may also lend additional belief to such a notion. One could argue that given the above failings of present systems, further efforts to embody the detection and control of nuclear war within computing machinery, must be based on an adequate technology. There are some indications that the techniques involved in artificial intelligence (AI) may be judged as the most appropriate for the next generation of strategic control systems.

Such a notion cannot be discarded offhandedly. To begin with, one needs to be aware that AI has (after a thirty-year childhood) finally emerged into the realm of commercial venture and usefulness. Indeed, the 1983 US market for AI products reached 66 million dollars and is estimated to be worth eight and a half billion dollars by 1993.[15]

Undoubtedly the most successful AI products to date have been the so called expert systems (ESs). These are complex pieces of software that have incorporated within them the rules or logical inferences that human experts use to come to decisions in their fields of expertise. Indeed, the construction of an ES requires detailed and careful interrogation of human experts in order to discover the rules they actually use in their decision making process.

A few examples may lend credence to the utility of ESs and the general field of AI. One of the most well-known ESs is MYCIN, a program which assists physicians by providing a specialist's knowledge of infectious diseases. MYCIN was developed in the mid 1970s at Stanford University by Buchanan and Shortliffe.[16] It has the ability to consider symptoms and provide possible diagnoses, as well as the rules and logic that led it to these inferences, thereby allowing the consulting physician the opportunity to reject the offered diagnoses on rational grounds.

There are many other successful ESs in existence[17] which perform functions in areas such as taxation,[18] internal medicine,[19] identification of the chemical structure of unknown compounds,[20] and geology.[21] Interestingly too, several expert systems have been modified to allow the easier creation of other expert systems in different fields. For example, MYCIN's 'inference engine' — EMYCIN, helped develop PUFF, a system for analyzing results of pulmonary function tests. Digital Equipment Corporation and IBM are building ESs for

the diagnosis of faulty computers and General Electric now uses an ES for troubleshooting locomotive repairs.[22]

Despite these successes, AI researchers are still some years away from the development of systems which possess adequate knowledge representations of the real world (rather than restricted knowledge domains) and the processing capacity to rival the general purpose abilities of humans in widely different tasks and environments. It is evident too that past attempts at providing computers with natural language understanding have been largely inadequate. While some successes have been achieved with restricted domains of discourse, the problems of context-dependency of language and of supplying the implicit real world knowledge that its understanding requires remain as major stumbling blocks. However, such problems have not diminished the military's faith in the eventual practical uses of AI.

The American Defence Advanced Research Projects Agency (DARPA) is actively supporting research into expert systems, speech recognition, machine vision and natural language understanding, as well as the proposed new parallel architecture for fifth generation computers which is predicted to enable the extremely fast processing speeds needed for full-blown AI applications. Ultimately, it is hoped that the fruits of this research can be applied to military needs such as fast, driverless reconnaissance vehicles, cybernetic co-pilot systems, and expert systems for battle management and control.[23] All of these schemes have been selected for support under a four year $US600 million Strategic Computing Program.[24]

Given these trends, it is likely that as the pace of modern warfare inevitably moves into yet another higher gear, and the decision load and response requirements thrust upon combatants approaches overload levels, the application of artificial intelligence to military purposes will become very apparent. Because of the command, control and communication difficulties already experienced with strategic weapons systems, it would seem obvious that this application would be of primary concern.

THE EFFECT OF DEFENSIVE SYSTEMS

In accordance with the 'launch on warning' rationale, in some quarters there is a degree of interest in building particle beam weapons to destroy enemy missiles in the boost phase of their launch (the first 30 seconds), before they have released their warheads. Such weapons would either be based in space, or else built on Earth and have their beams reflected to their targets via orbiting mirrors. Similar proposals are also being considered, and while there are still serious doubts about their feasibility, all share the common aim of providing an anti-missile capability upon detection of launch.[25, 26]

What is of concern is that these proposals are in congruence with the notion of automatic control of a strategic response, simply because their priority of destroying incoming missiles as early in their flight as possible would quite possibly eliminate the potential for any human intervention. Indeed, as processing speeds inevitably increase, and despite enemy countermeasures, destruction of missiles may occur almost as soon as they are detected.

THE PARANOIA OF EMP

There is a further phenomenon which may also lend credence in the minds of some to the utility of an automated strategic response. EMP, or Electromagnetic Pulse occurs when a nuclear device detonates high in the atmosphere and has the effect of damaging exposed conductors on the ground (including computers and circuitry of all kinds), by inducing massive electrical surges. Obviously the true power of this phenomenon is not completely known because of the current ban on atmospheric testing. However, some analysts have calculated that in principle, a single one megatonne warhead detonated at an altitude of 300 miles above the continental US could have destructive electromagnetic effects on command, control and communications across the entire nation.[27] Given the number of warheads available to the superpowers, it is not difficult to identify the support this phenomenon lends to the notion of particle beam weapons and an automated strategic defence.

SUMMARY

Some of these problems have existed for many years and we have still managed (perhaps only through good fortune) to avoid an accidental outbreak of nuclear war. It is clear though that we have entered a new era, with several factors operating to support the credibility of an automated strategic control system and its associated dangers, namely: (1) the alleged vulnerability of US ICBMs to a Soviet first strike (perhaps mediated through the effects of EMP) and the short decision time available to human commanders have contributed to the credibility of a 'launch on warning' strategy; (2) such a strategy is in accordance with an automated response and proposals for defensive systems such as particle beam weapons; and (3) the promise that AI presents in constructing systems with the degree of intelligence needed for the emerging scenario.

However, what has been presented here argues that some of the problems that have plagued the control of nuclear war in the past

cannot be eliminated in any future scheme. If anything the problems will be exacerbated. The system proposed would almost of necessity be based on AI principles if it were to function to the degree demanded of it. The complexity of the software needed to drive it would surpass even that currently running in the US DOD and verification of the correctness of that software would be impossible.[28] When the unknown hardware problems associated with a completely new computer architecture for the execution of this software and the inevitable human errors of testing and maintenance are added, it is not surprising that many computer professionals have expressed grave doubts concerning this and other developments.[29, 30, 31]

CONCLUSION

In an extensive and noteworthy analysis of the history and motivations of the nuclear era, Schell[32] has concluded that the development of nuclear weapons has made the continued existence of separate nation states a dangerous anachronism. In his view, in the pre-nuclear era, the existence of nations was defined by their ability and willingness to wage war, and in turn, war was seen and used as an extension of political and economic policy. Now that nuclear weapons have largely eliminated the economic and political utility of war, Schell has quite logically asserted that the sovereignty of nation states cannot be mediated through armed conflict. Hence, the existence of nations which continue to regard nuclear war as an instrument of political and economic policy, represents a danger to the world community. The answer, in his view, lies in global disarmament in both conventional and nuclear terms, driven by the heightened consciousness of the masses to the horrors and imminent danger of nuclear war. Thus, according to Schell, the prevention of nuclear conflict depends on a political solution involving an as-yet-to-be-discovered mechanism for making effective international decisions, the reduction and eventual abolition of all forms of weaponry, and a united world population sufficiently afraid of the possibility of Armageddon to effectively alter the global political framework.

Ultimately, dispelling the threat of nuclear war may indeed only be possible in the ways outlined by Schell. However, such strategies (which in practice represent a reorganisation of the entire planet) will take an enormous amount of time to implement. In the short term, the most consistently prevalent danger is the outbreak of accidental nuclear war as a result of computer generated error. In the author's opinion, any first use of nuclear weapons which is the outcome of human decisions, would most likely follow a protracted period of strained relations and finally crisis. In the current circumstances,

however, it is possible that an accidental nuclear exchange could occur at any time, with little or no warning and perilously few opportunities for intervention.

Clearly, the role of computers in the control and management of nuclear weapons is an issue that has received insufficient attention. From declassified documents and the like, it is known that the peacetime uses of nuclear weapons, reactors and even the transportation of radioactive materials, is quite appalling.[33] But for its even more sensitive nature, the failures of strategic detection and weapons control systems would surely be better known to us and appear equally unacceptable. The answer for many lies in technology, yet as we have seen, the limitations of technology in this application are already so dangerously apparent that to invest even further power in them is quite foolhardy. In a balance of power that operates upon mutual distrust, shortening the period for dialogue to minutes is inherently destabilising. Yet to go further and entrust decisions of such magnitude to less than perfect systems can in no way be seen as a solution. Finally, although there are many other relevant issues not focused on here, and at the risk of over-simplification, it should be obvious that extricating ourselves from our current situation (and the more dangerous ones that current proposals may yield), will not be achieved through technological means alone. The most successful mechanism is likely to be quite different: human reasoning carried out by humans for the sake of humanity as a whole.

NOTES AND REFERENCES

1. D.M.O. Miller, W.V. Kennedy, J. Jordan and D. Richardson, *The Balance of Military Power,* Lansdowne Press, London, 1981.
2. R.J. Smith, 'Missile deployments roil Europe', *Science,* 223, 1984, pp. 371-376.
3. R.J. Smith, 'Missile deployment shakes European politics', *Science,* 223, 1984, pp. 665-667.
4. J. Steinbruner, 'Launch under attack', *Scientific American,* 250, 1, 1984, pp. 23-33.
5. R.J. Smith, 'Pentagon moves towards first strike capability', *Science,* 216, 1982, pp. 596-598.
6. C. Beardon, 'The last bug in the world', *New Zealand Interface,* July, 1983, pp. 33-34.
7. J.W. Verity, 'Nuclear war and the computer', *Datamation,* February 1984, pp. 50-61.
8. C. Beardon, 'The use of computers in weapons systems', paper circulated to members of *International Federation of Information Processing Societies,* Technical Committee 9 (Computers and Society), 1984.
9. G. Hart and B. Goldwater, *Recent False Alerts from the Nation's Missile Attack Warning System,* United States Senate Committee on Armed Services, Washington D.C., 1980.

10. Beardon, 1984, *op. cit.*
11. M. Kochen, 'Information and society', in M.E. Williams (ed.), *Annual Review of Information Science and Technology,* Vol. 18, Knowledge Industry Publications for American Society for Information Science, 1983, pp. 279-304.
12. I. Peterson, 'Superweapon software woes', *Electronics Australia,* October, 1983, pp. 12-14.
13. W.J. Broad, 'Computers and the US military don't mix', *Science,* 216, 1980, pp. 599-602.
14. C.A.R. Hoare, 'The emperor's old clothes, *Byte,* 6(9), 1981, pp. 414-425.
15. T. Manuel and S. Evanczuk, 'Artificial intelligence: commercial products from decades of research', *Electronics,* November, 1983, pp. 127-137.
16. R.O. Duda and E.H. Shortliffe, 'Expert systems research', *Science,* 220, 1983, pp. 261-268.
17. E. Garfield, 'Artificial intelligence: using computers to think about thinking', Part 2, *Current Contents,* 52, 1983, pp. 5-17.
18. R. Michaelson and D. Michie, 'Expert systems in business', *Datamation,* November, 1983, pp. 240-246.
19. R.A. Miller, H.E. Pople and J.D. Myers, 'Internist-I, an experimental computer based diagnostic consultant for general internal medicine', *New England Journal of Medicine,* 307, 1982, pp. 468-476.
20. R.K. Lindsay, B.G. Buchanan, E.A. Feigenbaum and J. Lederberg, *Applications of Artificial Intelligence for Chemical Inference: The DENDRAL Project,* McGraw-Hill, New York, 1980.
21. R. Duda, J. Gaschnig and P. Hart, 'Model design in the PROSPECTOR consultant system for mineral exploration', in D. Michie (ed.), *Expert Systems in the Microelectronic Age,* Proceedings of the 1979 ALSB Summer School, July 1979, Edinburgh, Scotland. Edinburgh University Press, 1979, pp. 153-167.
22. C. Pratt, 'An artificially intelligent locomotive mechanic', *Simulation,* 42, 1, 1984, pp. 40-41.
23. W. Schatz and J. Verity, 'DARPA's big push in AI', *Datamation,* February, 1984, pp. 48-50.
24. R. Rosenberg, 'Pentagon shopping for walking vehicle', *Electronics,* April 19, 1984, p. 56.
25. R.J. Smith, 'The search for nuclear sanctuary (I)', *Science,* 221, 1983, pp. 30-32.
26. R.J. Smith, 'The search for nuclear sanctuary (II)', *Science,* 221, 1983, pp. 133-136.
27. Steinbruner, *op. cit.*
28. B. Bereanu, 'Self-activation of the world nuclear weapons system', *Journal of Peace Research,* 20, 1, 1983, pp. 49-57.
29. Beardon, 1984, *op. cit.*
30. Verity, *op. cit.*
31. J. Jacky, 'The use and misuse of new technologies', *Communications of the Association for Computing Machinery,* 27, 6, 1984, pp. 526-527.
32. J. Schell, *The Fate of the Earth,* Picador, London, 1982.
33. M. Kidron and D. Smith, *The War Atlas — Armed Conflict, Armed Peace,* Pan Books, London, 1983.