LA-UR -86-4320

CONF-861215--1

Los Alamos National Laboratory is operated by the University of California for the United States Department of Energy under contract W-7405-ENG-36

LA-UR--86-4320

DE87 003749

TITLE THE LIMITS OF TECHNOLOGY IN NUCLEAR CRISIS MANAGEMENT

AUTHOR(S) Paul C. White

SUBMITTED TO Center for Strategic & International Studies
University of Georgetown, Washington, DC,
December 5, 1986, Workshop on Directions in the
Study of Crisis Management.

DISCLAIMER

Los Alamos National Laboratory
Los Alamos, New Mexico 87545

FORM NO 836 R4
ST NO 2629 5 81

THE LIMITS OF TECHNOLOGY IN NUCLEAR CRISIS MANAGEMENT

Paul C. White
Associate Center Director
Center for National Security Studies
Los Alamos National Laboratory

ABSTRACT

For some purposes, one may consider the roles of technology in nuclear crisis management to fall into four categories. Certain technologies, such as signals intelligence, may assist in monitoring for the emergence of crisis precursors. Other kinds of surveillance, such as that by certain satellites, are intended to detect phenomena, such as missile launches, which clearly signal the transition from pre-crisis to mid-crisis. During this phase, communications and surveillance technologies may be called upon to aid in managing the crisis. Finally, communications technologies will play a vital role in crisis resolution, preferably ;during the pre-crisis phase, but in mid-crisis if necessary. It has long been recognized that a large fraction of these technical means are vulnerable, both to selective, direct attack, and to the unintended, collateral effects of conflict itself. Systematic efforts are underway to make these systems more robust and survivable in crisis environments, but one must clearly recognize the limits of technology. In particular, one must weigh very seriously the implications and possible consequences of intentional, direct attack, including decapitation, on just those means which may permit timely crisis resolution. In the end, these technologies may prove so vulnerable, that nations may be forced to rely on pre-crisis planning, including force structuring, clearly defined options planning, and clear statements of intent, in order to permit any sort of mid-crisis resolution and conflict termination.

INTRODUCTION

The possible roles of technology have been a constant, but muted theme in most of the recent discussions of crisis management. Quite naturally, these fora have emphasized the human elements: the need for relationships and joint ventures; the requirements for training and practice in crisis situations. Implied in all of these analyses has been the minimal, though indispensable roles of technology in both providing and processing information: information essential for any human action.

The purpose of this simple effort is to focus briefly on a few important aspects of these crucial tools for nuclear crisis management. What roles should be envisioned for technology? What limits should be understood for technological capability, and what might these limits imply for possible management frameworks. To some degree, this discussion overlaps previous studies of C^3I, but the focus here is to examine particularly those aspects necessary for control, especially such aspects of control as might permit escalation management and conflict termination. In any case, the examples considered are in no sense complete, but it is hoped they are suggestive of further study.

CLASSIFICATION OF ROLES OF TECHNOLOGY

For some purposes, it may be useful to consider the roles of technology in nuclear crisis management as falling into four categories. Certain technologies, such as imaging or signals intelligence, may assist in monitoring for the emergence of crisis precursors. In October, 1973, Soviet military preparations for unilateral intervention on behalf of Egypt were clearly monitored by the US, and provided a measure of the extent of the developing crisis. Other kinds of surveillance, such as that by certain satellites, are intended to detect phenomena, such as missile launches, which would clearly signal the transition from pre-crisis to mid-crisis. The distinction here between monitoring and detection may be rather artificial, intended only to mark the difference between some sort of continuous tracking of events, ultimately by people, and systems designed to alert their human attendants only when some signal threshold has been exceeded. For example, were any of the DSP series satellites to confirm the infrared signatures of ICBM launches, then there would be no doubt about the gravity of the situation. At this point, one could only hope that some form of restraint on the part of leadership might permit early crisis stabilization. During this phase, communications and surveillance technologies may be called into play. KH-series, rhyolite, or other space systems may be able to track the extent of the attack, permitting, in principle, an appropriately measured response. Communications technologies would, of course, play a vital role in the resolution of such a crisis, preferably during the pre-crisis phase, but in mid-crisis, or mid-conflict, if necessary.

One must not attempt to push the significance of this sort of classification too far. After all, most of these technologies involve one or another means of acquiring, processing and disseminating electromagnetic signals. Rather, such a scheme is useful only insofar as it provides some distinctions in the characteristics demanded of technical systems in these roles: the kinds of environments in which systems must function, the time urgency of their data, the required endurance, the relationship to human operators, and so forth.

MONITORING AND DETECTION: REQUIREMENTS AND ISSUES

Consider, then, what are the requirements for monitoring and detection technology? Imagine what is demanded of satellites or other listening devices monitoring for the signs of increased military activity. Certainly these systems must be in continuous operation, constantly on alert for predetermined signs. Appropriate allowance must be made for mechanical or electronic failures: this might involve self diagnosis, a certain degree of internal redundancy, and even complete backup systems. Perhaps more importantly, such systems must be comprehensive, that is, they must provide complete coverage of potential action areas In a certain sense, they should also be overdesigned, capable of responding to signals below anticipated thresholds. This kind of elasticity would allow both for the all too frequent overextensions of system lifetimes, and for a measure of allowance for the unexpected. It would seem reasonable also to expect that such systems would normally be operating in relatively benign environments. Finally, let us not neglect the relationship with sentient observers. These people must be prepared to respond quickly to any electronic alarm, comprehending, analyzing, and then communicating promptly through the appropriate chain of command. Furthermore, one must also consider that these responsibilities may lie in the hands of multilateral teams. A little imagination might easily extend this list; for now, however, let us consider a few of the issues associated with these requirements.

First of all, the characteristics of continuous operation, comprehensive coverage and extreme sensitivity for a monitoring system could easily permit it to function in an intelligence gathering mode. This ambiguity might be acceptable for unilateral, or national technical means, but the problems in multilateral usage have already been noted by a number of analysts. Would the US reveal the extent of its surveillance capability to other nations, particularly the Soviet Union? Or, in a cooperative venture, would the US provide its latest technology to the Soviet Union to help it better monitor US activity? Then too, there is the possibility that a survivable monitoring system may, in fact, be interpreted as a warfighting capability.

Then there is the problem of data interpretation. The above requirements call for extreme sensitivity which, when combined with the demands for prompt reaction, will lead to a certain false alarm rate, with all the ensuing dangers, and demands on human interpretation. Even with the luxury of time and

detailed analysis, some events will defy unambiguous interpretation. Witness the September 22, 1979, flash in the South Atlantic. An issue closely related to the problem of physical interpretation, is that of translating raw data into underlying purpose or intent. What, for example, was going on when a Soviet ship moved into the Mediterranean on October 22, 1973, apparently with radioactive materials on board? Was this a routine movement, or a portent of a dangerous escalation in the mideast conflict. Similarly, how does one distinguish between routine military exercises and potentially threatening alerts? Technology will always have its limits in this respect. Planned human interactions will be required in order to transcend these limitations, and to minimize the risks of overreaction in ambiguous circumstances.

A certain amount of overlapping coverage, or redundancy may serve to minimize another vexing problem: that of how to interpret a sudden loss of data transmission. Is it a relatively benign system failure, or a deliberate action to hide offensive maneuvers? Again, redundancy can help, but so too can informal or formal restraint on development and exercise of certain technologies, such as ASAT capability.

MANAGEMENT AND RESOLUTION: REQUIREMENTS AND ISSUES

If we turn now to a consideration of the technology required to support the management of an existing crisis, or to abet its resolution, then we discover a slightly different set of characteristics. To begin with, such management will certainly demand a certain amount of monitoring capability, although with rather different characteristics than early warning systems. At the very least, some damage assessment capability will be required. The harsh environment of nuclear conflict will place severe demands on electronics and sensor technology. Even so, the desirability of current data may require extensive redundancy or reconstitution capability. In addition to the desirability of monitoring crisis developments, it will prove essential to maintain two-way communication with remote military and political authorities. These communication links must be as hearty and survivable as the sensors. In fact, especially during the incipient phases of a crisis, it is essential that these links both maintain continuity and include direct connection with national leadership, again both military and political. After all, such linkage is essential for any sort of bi- or multilateral crisis stabilization and resolution.

What then are some of the issues associated with these roles for technology? First of all, given that the crisis has evolved to the point of overt hostilities, the environments in which both sensors and communication links must operate will hardly be benign. Essential electronic components tend to be rather sensitive anyway, and even collateral effects are likely to cause extensive attrition. Most troublesome, however, is the growing possibility that improvements in a variety of areas of weapons technology may enable the intentional severing of key communications links essential for escalation control and crisis management and resolution. It is generally accepted that no

satellite can be made sufficiently hard to resist direct attack. And even extensive efforts at command center hardening may not prove sufficient to prevent successful attack.

It has long been an important tactical principle that advantage is to be gained by eliminating an opponent's battlefield leadership. (Shoot at the guy wearing the star; destroy the tank with the antenna.) But in any conflict actually, or potentially, involving nuclear weapons, continuity in national command authority will be vital to maintain any semblance of escalation control, much less stabilization and resolution. I think that this issue transcends all of the recent arguments for robust and redundant C^3I. One should not underestimate the capability for technology to enable decapitation, should it be desired. Several reporters have noted that among the most stressing US intelligence requirements are those for tracking Soviet leadership with sufficient accuracy and timeliness to permit direct attack. So at least some people are thinking about it. I submit that such attack may not be desirable, and that perhaps only mutual restraint, and not technology, can ensure the survivability of vital communication links necessary for crisis resolution.

FUTURE POSSIBILITIES FOR TECHNOLOGY

In spite of this concern, technology will continue to advance the capabilities, and thus the possibilities for crisis control in some areas. And of course , much of this improvement will be in the vital area of C^3I: enhanced sensitivity and resolution, along with the (apparently contradictory) improvements in component hardening. At the system level, greater redundancy and regeneration capability will evolve.

It may be imagined that in a crisis, leaders will be confronted with an information overload. Shear quantity, without pre-selection, weighting, or context , may make useless a great deal of potentially valuable data. Information processing and management techniques may thus be essential to informed crisis control. The development of artificial intelligence, or expert system tools may prove invaluable in this area.

An often overlooked, but not to be underestimated, role for technology in crisis management involves the provision of a broad technology base, a reservoir of unorthodox options in a crisis. US naval capability, including communications and surveillance, enabled a relatively passive sea blockade, instead of a direct military confrontation during the Cuban missile crisis. Even earlier, it was US aviation capability that permitted a sort of end-run around the Berlin Blockade. Such options for sidestepping confrontation, and thus avoiding crisis escalation, along with the kind of thinking that spawns such options should be actively nurtured and developed through gaming and other forms of simulation.

CONCLUSIONS

What then can be said about the roles of technology in crisis management. Perhaps most obvious, is the observation that the utility of technology has limits. In the first place, there are limits to sensitivity, resolution and survivability. There are also limits to what a small set of observables can contribute to understanding a given crisis situation. In another sense, there are also certain technologies, such as antisatellite weaponry, which could do much to disrupt the means for crisis stabilization and resolution, unless those technologies are themselves limited.

Technology is merely a tool, and a meager one at that, to assist human observers, analysts and leaders in dealing with crises. In the end, the most important tools in this arena may be those of political and social skills, the real-time exercise of personal knowledge, experience, understanding, and creativity, together with a practiced relationship of trust between the leaders called upon to act in crisis situation.