Nuclear War and Computer-Generated Nuclear Alerts

Nuclear War and Computer-Generated Nuclear Alerts

Douglas Campbell

Both the U.S. and USSR military systems are based on two assumptions about computers and nuclear alerts: Everything will work the way it is supposed to work; Nothing will happen until it supposed to happen.

In the recent movie *War Games*, an ingenious teenager penetrates the Pentagon's computer codes and touches off a nuclear alert at the headquarters of the U.S. missile detection and launch facilities. The computer-generated screens indicate that Soviet missiles—launched from offshore submarines—will arrive in five minutes. The teenager tells the military officer in charge that the alert is an accident, that the "attack" is not real but is computer-generated, and that he should ignore all the computer data. Thus, the officer must decide within five minutes whether to believe the computer data so graphically displayed before his eyes or to believe that this multi-million dollar defense system upon which our security depends could accidentally trigger a nuclear alert. If the alert is real and the officer ignores it, the U.S. military offensive capacity could be destroyed, along with millions of citizens. If the alert is only a computer glitch and the officer acts as if it were real, he could accidentally launch World War III. At the last second, he rejects the computer system, trusts his own human judgment, and does not launch.

This sequence may seem implausible, but at the end of this article I will narrate a documented historical event that approximates the movie. Although the movie is farfetched in some respects, it is true that our entire nuclear arsenal is intimately and absolutely linked to decisions made by computer systems. How did this dependence arise? Do the inherent dangers point to a need for a change in national policy?

The Rise of the Computer National Defense

Our military dependence on computers goes back to World War II, to a time when Congress still declared war and the president was commander-in-chief, to a time when the Allies invented the computer for code-breaking and nuclear weapons for mass destruction. At the end of World War II, two huge oceans protected us from a surprise Soviet attack. To launch fleets of airplanes loaded with conventional bombs would involve tens of thousands of men, massive amounts of materiel, and numerous telltale signs available to ordinary intelligence gathering. Conventional bombers required twelve hours from takeoff to attack—twelve hours in which there would be time for diplomatic consultation, exchange of cables, rational thought; twelve hours in which the planes could be ordered to turn back or could be granted an emergency landing. At worst, if emergency negotiations failed, conventional bombs would cause modest damage but not annihilation.

In the sixties and seventies, however, the development and perfection of intercontinental ballistic missiles (ICBMs) capable of carrying nuclear warheads greatly increased the possibility of massive destruction by surprise attack. ICBMs can be launched without tipping off the other country by mobilizing tens of thousands of navigators, pilots, bombardiers, and supply officers. The time from launch to destruction could be as short as two hours—two hours to use the hot line to make sure that an "attack" is not a flock of Canada geese or the rising moon, two hours to make sure the attack is a government decision and not Dr. Strangelove in charge of an isolated squadron, two hours to moderate the response and have only a limited nuclear war, two hours to warn the civilian population to evacuate their cities. But even if hot line negotiations succeed, there is no way to call back the missiles, no way to provide them with an emergency landing field.

In the seventies and eighties, the perfection of submarine-launched ballistic missiles (SLBMs) on submarines cruising a few miles off the enemy's shoreline reduced the time from launch to destruction to fifteen minutes—no time for hot line negotiation, no time for recall of missiles, barely enough time for detection. From the moment the duty officer determines that an attack is under way, there are only two minutes to decide on the level of response and to issue the order to "launch on warning" to computer-controlled missiles aimed at computer-selected targets kept in computer databanks.

But in the eighties and nineties, new "Star Wars" technology will allow multiple nuclear warheads to be delivered by geostationary satellites in four minutes and twenty seconds—no time for human determination of an attack; no time for human evaluation of different responses; barely time for the computer to determine that an attack has been launched, to decide on the appropriate response, choose the weapons, and launch them; barely enough time for the computer to notify the human government of what it has chosen to do, is doing, and has done. Any modern military is dependent on C^{3}I (Command, Control, Communication, and Information). Modern technology has forced the complete interaction of these four elements into smaller and smaller windows of time using computer systems.

Computers and Control

In World War I, mobilization took months. Solzhenitsyn, in his novel *August 1914,* spends hundreds of pages describing the mobilization in Russia—months to create the paperwork to move each man, to create the paperwork to buy supplies, to create the paperwork to stockpile supplies, to create the paperwork to move supplies. No military machine could move faster than its paperwork.

Things moved somewhat faster in World War II. In a marvelous scene in Len Deighton's recent novel *Goodbye, Mickey Mouse,* the colonel in charge of a small group of American bombers stationed in England tries to discover whether his group will fly the next day. He phones an old friend at Eighth Air Force headquarters late in the afternoon for a chat. Sure enough, in the background he hears the teleprinters churning. He hangs up and announces to his group that they will fly.

> He could visualize the scene at Division, where they would be staring at the cryptic gobbledygook of closely teleprinted figures. It would take what was left of the afternoon to translate it all into specific orders routes, aiming points, bombing altitudes, timings, radio procedures, and detailed instructions about the formations, forming-up procedures and emergency measures.[1]

That was the sequence for just one ordinary bombing run of one small group under the Eighth Air Force.

No modern nuclear delivery system can depend on human paperwork for execution of defense or offense. Only computers can control the volume of information and the correct ordering of events within the narrow window of time in which events must occur.

Computers and Information

A modern nuclear delivery system digests vast amounts of information with the aid of a computer. For example, the U.S. Navy's Sound Surveillance System (SOSUS) is a "collection of underwater acoustic sensors" to locate ships by the sounds of their propellers, motors, and random noises. Vast amounts of real-time data are generated and coordinated with reports from spy satellites, reconnaissance flights, and ordinary covert intelligence.[2] Indexing, storing, retrieving, and assessing this volume of data by hand would take years, not hours.

Automatic computer interpretation of massive, seemingly worthless low-level data can provide important high-level information. For example, the German military machine was very carefully run during World War II. All tanks, planes, tires, and trucks were given serial numbers to provide for property control, billing, recalls, and internal quality control. By studying the serial numbers of captured German material and performing various mathematical analyses, the Allied forces were able to make reasonable estimates about the level of German war production, they could deduce which factories were responsible for what percentage of key items. This information changed the priorities on bombing runs.[3] Currently, the automatic analysis of literally thousands of different types of low-level data is done automatically for the military by the computer with minimal human intervention.

Another example of computer interpretation of massive data involves electronic eavesdropping on international telephone and embassy microwave information. The computer is programmed to save any conversation that uses such key words as nuclear, missiles, war, or whatever may be of current interest. Conversations that do not involve a key word are discarded. The recorded conversations are then evaluated by humans. The sheer volume of mostly routine conversations would swamp any human attempt to do this screening.[4]

Computers also simulate and then analyze nuclear attacks and counterattacks. The analysis is crucial to assessing the consequences and probabilities of particular attack plans. In the event of a real attack, the United States has a computer model known as SIDAC (Single Integrated Damage Assessment Capability) at the Pentagon as well as at the protected underground Alternate National Military Command Center.[5] SIDAC is programmed to take data from satellites, ground stations, weather stations, and other sources to estimate damage and to plan our second-round attack. However, a nuclear explosion produces an electromagnetic pulse (EMP) which may cause widespread damage and disruption to computers.[6] Such damage means that computers may not be available for a second-round attack. Since the EMPs of a surprise attack may knock out computers and prevent a first-as well as a second-round counterattack, both sides must plan to launch everything as soon as an attack is detected. This necessity eliminates the possibility of a "limited nuclear war" strategy.[7]

Computers and the Human Element

Humans foul up. "Seemingly inexplicable, inconsistent, and unpredictable human 'goofs' account for 50–70 percent of all failures of major weapons and space vehicles."[8] The loss of the submarine *Thresher*, for example, was due to a relief valve's being installed backwards. It would obviously be very desirable if human errors could be reduced or eliminated by the use of computers.

But replacing people by computers does more than minimize human goofups. The U.S. volunteer military, one of the finest in the world, has about 115,000 people who are closely connected with nuclear duties. Each year the Defense Personnel Reliability Program removes from nuclear duties those persons whose reliability, trust-worthiness, and dependability become inconsistent with standards. The number of people removed for various causes is surprisingly large. Here, for example, are the figures for a three-year period in the mid-1970s:[9]

Persons Removed from Nuclear Duties in Defense Personnel Reliability Program

Reason	1975	1976	1977
Alcohol abuse	169	184	286
Drug abuse	1970	1474	1365
Negligence or delinquency in performance of duty	703	737	825
Court martials or civil conviction of a serious nature	345	388	350
Behavior or actions contemptuous of the law	722	945	885
Significant physical, mental, or character trait or aberrant behavior, medically substantiated as prejudicial to reliable performance	1219	1238	1289
Total	5128	4966	5000

Humans in a nuclear alert system operate under stress, boredom, and Isolation, performing repetitive tasks for hours at a stretch and interacting only with a terminal. For weeks, nothing happens as they wait in a silo outside of Bismarck, North Dakota, staring at an unchanging green screen, waiting alongside missiles with the equivalent of millions of tons of explosives. Although five thousand is a large number, it is amazing that under such circumstances only that many people a year are found unsuitable for service.

In contrast to humans, a computer does not suffer stress, is not subject to boredom, and does not care about isolation. It would seem highly desirable, then, to replace people with computers that don't take drugs, won't go schizoid, don't drink, aren't subject to blackmail, and will obey orders automatically.

Problems with Computers

The types of warning sensors that feed data to NORAD (North American Aerospace Defense Command) in Colorado Springs are as sophisticated as they are varied. They include infrared warning satellites, the Ballistic Missile Early Warning System, a phased array radar system, Perimeter Acquisition Radar Attack Characterization Systems, Cobra Dane (a radar system on Shemya Island, Alaska), and Cobra Judy (a floating version of Cobra Dane, located in the Arctic). In addition, we have three Defense Support Program satellites in fixed orbit providing overlapping coverage of the USSR and China for ICBM launches and the Atlantic and Pacific oceans for SLBMs. The real-time information supplied by these satellites is sent to Denver or to Alice Springs, Australia, for processing before being forwarded simultaneously to NORAD, SAC, and the Pentagon.

When the sensors indicate sufficient strange data, NORAD holds one of three types of conferences: Missile Display, Threat Assessment, or Missile Attack. No Missile Attack conference has ever been held. The exact number of the other two conferences has not been declassified. However, a declassified section of a 1980 Congressional Report states that there were 147 Missile Display conferences and five Threat Assessment conferences in the eighteen months from 1 January 1979 to 30 June 1980.[10]

Descriptions of most such conferences are classified, but a few have appeared in various printed sources. Rather than discuss the DEW-line (Distant Early Warning) false alerts in the 1950s caused by a flock of Canada geese or the BMEWS (Ballistic Missile Early Warning System) false alerts in the 1960s from meteor showers and lunas reflections, I will concentrate on incidents from the 1970s and 1980:

> *20 February 1971:* A human operator at NORAD accidentally transmitted the emergency message, authorized by the proper code for that date. All radio and television stations were ordered off the air by presidential order. It took forty minutes to find and send the proper cancel code.[11]
>
> *27 February 1972:* While President Nixon was in China, a hoax message that the president had been assassinated and that World War III had been declared by Vice President Agnew was sent to twenty-two units of the Eighth Coast Guard District.[12]
>
> *1973:* A computer misinterpreted sensor data about a Soviet test missile fired from a site near Iran. The computer predicted it would land in California and sparked a United States alert. The missile landed instead near Kamchatka, Siberia.
>
> *3 October 1979:* Mount Hebo radar station picked up a low-orbit rocket body that was close to decay and generated a launch and impact report that forced NORAD to hold a Threat Assessment Conference.
>
> *9 November 1979:* A NORAD technician inadvertently put on a tape that contained data simulating a mass Soviet attack. NORAD sent a warning of Soviet submarine missile attack to defense command centers across the U.S. Ten fighters were scrambled, and missile and submarine bases were automatically switched to a higher level of alert.[13]

> *15 March 1980:* As part of a troop training exercise, the Soviets launched four SS-N-6 missiles from submarines. One of the launches generated an unusual threat fan and forced NORAD to hold a Threat Assessment Conference.
>
> *3 June 1980:* SAC received computer data indicating SLBMs and ICBMs had been launched toward the United States. NORAD was forced to hold a Threat Assessment Conference even though nothing was appearing on its screens. It turned out to be a hardware failure.
>
> *6 June 1980:* Three days after the 3 June hardware failure, SAK again received computer data indicating that a Soviet missile attack had been launched, and NORAD was forced to hold another Threat Assessment Conference.[14]

As we can see, accidental alerts have been generated by human carelessness, jokes, decaying satellites, computer hardware errors, computer software errors, and wrong computer tapes being loaded.

Problems with Complex Systems

Murphy's law—If anything can go wrong, it will—functions in our defense warning systems. Surely the reader, living in the modern world, has experienced the computer-generated error that cannot be changed, the computer-produced mislabeled utility bill which seems impossible to correct. A dozen telephone calls to as many individuals only generates the infuriating response, "The computer is doing it, and no one seems to know how to make it stop." Computer-controlled multi-state power grids have failed; computer-controlled trains have derailed, computer-engineered bridges and dams have fallen down; computer-controlled nuclear power plants have come close to meltdowns. The best-intentioned complex systems have failed. Ford Motor Company did not intentionally put bad gas tanks in the Pinto. But despite "sophisticated testing systems, computer simulations, an army of quality-control procedures, engineers, and inspectors," despite having built other fine car systems, despite the enormous potential liability, the design of the complex system was flawed. The Three Mile Island nuclear power plant was not built until every aspect of the design had been examined by dozens of regulatory agencies and innumerable engineering studies had been conducted. The defenders of atomic power plants asserted that "getting hit by a meteor was far more likely than a major nuclear plant accident." And yet the complex system failed.[15]

A complex computer system can go awry for many reasons. One is that the large amounts of money spent put tremendous pressure on proponents of the system to deliver something that is working, even if this means patchwork that goes against "the rules" of the system. Especially in complex military systems, there is a tendency for informal and usually oral understandings to circumvent the procedures specified in the rulebooks. For example, with SAGE, one of the early radar warning systems, if rulebook procedures were followed to the letter small amounts of radar jamming paralyzed the system. Oral agreements between operators solved this problem, but the agreements never showed up in official reports.[16] The system that was designed, the system that was built, and the system that was used were all different. Congressional oversight committees and the generals in charge, often lacking technical computer skills, only evaluate written plans, not the kludged-up versions actually used.

No complex system would ever run if rule books were followed to the letter. System analysts, designers, programmers, coders, and operators all circumvent official procedures at times in order to get a system up and running within the time and money constraints. Such rule-cutting is oral, informal, and undocumented. No wonder, then, that a complex computer system, which barely works under ordinary circumstances, does bizarre things in crisis mode.

An incredible number of things can go wrong in a system, things obvious in retrospect but not at all obvious before. The NORAD system, upon which all of our C^3I for nuclear defense rests, is a chilling example. The system was built in 1965 and is completely dependent on computers which shut down automatically if there is a drop in the power supply. As of 1981, NORAD still had no reliable emergency power supply.[17] Duty officers at NORAD have four recent historical reminders to evaluate carefully what apparently may be erroneous data. Despite the power and thoroughness of the system, it is difficult for it to detect surprise attacks. In fact, despite what in retrospect seem to be clear warning signs, the U.S. global satellite warning system failed to give advance notice of the "Soviet intervention in Czechoslovakia, the Tet offensive in Vietnam, . . . the 1973 Yom Kippur War,"[18] and the Argentine invasion of the Falkland Islands.

Compound Stimuli to Complex Systems in Crisis Mode

It is feasible to make plans for a computer system to handle single unplanned incidents—plans to prevent inadvertent releasing, arming, or launching of a missile with a nuclear warhead; plans which systematically remove humans from the sequence of events launching a nuclear-tipped missile; plans to prevent accidental detonations by wiring safety switches that arm the warhead; plans for a computer-scheduled launch when humans may be panicking or thinking of the wife and kids for one last time. But it is not feasible to design a computer system that will correctly handle multiple unplanned incidents. The number of different ways *N* incidents can interact is governed by the combinatorial explosion and rapidly goes beyond any possible computer technology even for such small values of *N* as 60 or 70. There has been at least one such multiple incident event involving our early warning system.[19] The British and French invasion of the Suez occurred at the same time as the Hungarian uprising in November 1956. On 5 November, Moscow issued a statement strongly hinting possible rocket attacks on London and Paris and inviting the U.S. to join the USSR in a joint action in the Suez. That night, the U.S. military command in Europe reported that unidentified aircraft over Turkey had put the Turkish Air Force on alert. A hundred MiG-15s were reported over Syria; a British Canberra bomber was reported as downed over Syria; and the Russian fleet was reported moving through the Dardanelles.[20]

If NORAD had existed back in 1956, it is highly probable that these multiple reports combined with the high state of international tensions due to the Hungarian uprising would have increased the alert status of U.S. forces. Let us see why a warning system does not necessarily mean better security in such a situation.

A warning system may accidentally become part of the offensive system by issuing an alert erroneously. Two mutually linked warning systems may unintentionally amplify such mistakes. The outbreak of World War I provides a concrete example of what can happen with mutually linked systems. The decision to mobilize in the early months of 1914 set thousands of orders into operation, each of them ratcheting the military system to a higher level until it reached a state where the system reacted to itself. When country A went on alert at a time of tensions, country B reacted to the changed state and went on alert to protect itself. When country A observed that country B had gone on alert, country A had added reason to believe its earlier interpretations of the data which had forced it to go on alert. Country A therefore took additional preparatory steps. As each country went to a higher level of alert, both countries had to take actions to make sure they could perform after an attack. Both countries therefore prepared to be attacked, interpreting the other's preparation to be attacked as a step in preparing to launch an attack.[21] In effect, the European political leaders' decision to mobilize in early 1914 was a declaration of war months before the hostilities actually broke out. "The most appalling feature of World War I was not the destruction; . . . but rather it was the war's pointlessness. Ten million men died and monarchies were swept from power simply because governmental leaders did not think through the implications of their actions and the institutions they had constructed [for the prevention of] war!"[22]

The reality of the events of 5 November 1956 was as follows: The jets over Turkey were a flock of swans. The hundred MiGs over Syria were an escort for the Syrian president returning from a state visit to Moscow.

Britain's Canberra bomber landed in Syria because of mechanical failure. The Soviet fleet was going through the Dardanelles on fleet exercises that had been scheduled long in advance.

The warning system in a crisis situation had accidentally amplified multiple independent, unpredictable events into a nonexistent pattern.

Nuclear Alerts and Accidental Nuclear War

Modern military systems are complex, geographically dispersed, and technologically sophisticated. The development of nuclear weapons has advanced faster than the development of reliable control of nuclear weapons. In an attempt to provide control, both the U.S. and the USSR have used computers. Thus the reliability of the mutually linked nuclear systems depends on the reliability of the underlying complex computer systems. But humans designed, programmed, coded, and now operate these systems that systematically replace humans as much as possible and bypass a constitution designed for an isolated and sparsely settled nation. Although the Constitution asserts that only Congress can declare war and that the president is commander-in-chief, these provisions have been made irrelevant. The decision to go to war must be made in less than fifteen minutes by an unelected, presidentially authorized duty officer dependent on computer-generated data.

The president of the United States and the premier of the Soviet Union may be compared to the president of a nuclear power plant.[23] As long as things are running normally at the power plant, the president has both real and symbolic powers. But if it is announced that a core meltdown could occur in fifteen minutes, the president—who doesn't know heavy water from drinking water—will do exactly what he or she is told to do, if he or she is consulted at all. Technicians and institutional procedures take over. Split-second decisions are made based on massive amounts of ambiguous technical information. Some humans will question whether this isn't a test or a mistake, and some computer systems will not quite cover what is happening. These parts of the system will hang suspended awaiting orders from someone who has—or will take—responsibility. The figurehead president cannot take action and issue technical orders because of the sheer volume and ambiguity of the information and the incredibly narrow time window. Similarly, at the moment of a nuclear alert, the massive amounts of highly technical and ambiguous information from warning and intelligence systems would be gibberish to a technically naive president to respond. The political leader can only hope that the duty officer making the final evaluation is competent.

If the duty officer sees either an expected pattern or a pattern that is manifestly absurd, the system will probably work as it is supposed to. On the other hand, if the pattern is ambiguous, strange, unexpected, or contradictory; if it occurs during a brownout, or shortly after a new system has come on line, or shortly after one of the satellites has been moved, or just before, during, or just after a training exercise, then the complex system will be in an untested configuration with unpredictable results. Only one thing is certain—Murphy's law will hold.

If the Soviets attack in a stylized and highly predictable way, NORAD will probably react correctly. But if the attack is ambiguous, or if it occurs in conjunction with a flock of geese, a lunar reflection, a NORAD simulated tape accidentally inserted, a defective computer chip, or any other pattern that does not fit the NORAD notion of a Soviet attack, it may not be discerned in time.

Both the U.S. and the USSR are hostages to the fear that their forces will be eliminated by a preemptive attack occurring so quickly that they cannot respond. Game-playing strategy suggests that both sides will move to a "launch on warning" mode in which each side warns the other that upon detection of attack the order will be given to launch automatically. Both sides will then be at the mercy of every forty-six-cent chip bought at lowest bid and of every software error that accidentally generates a warning of an impending attack.

The 3 June 1980 Nuclear Alert

The event that occurred on 3 June 1980 was in fact generated by a forty-six-cent computer chip malfunction. At approximately 2:26 A.M., Eastern Daylight Time, the fluorescent display screens connected to a Nova Data General computer at SAC headquarters flashed a warning indicating that two SLBMs had been launched toward the United States on a "depressed trajectory" from submarines positioned offshore. Eighteen seconds later, the SAC display system showed an increased number of SLBM launches. The SAC duty controller scrambled 116 B-52 crews and directed them to start their engines and to prepare for takeoff if it became necessary to survive. Nuclear submarine commanders were also alerted. The SAC display then indicated that Soviet ICBMs had been launched toward the United States. The separate NMCC command post confirmed that it too was receiving indications that SLBMs had indeed been launched toward the U.S. NORAD still reported nothing on its screens. The airborne command post of the Pacific Command took off. NORAD was forced to hold a Threat Assessment conference even though nothing was appearing on its screens.[24]

Had the episode lasted a few minutes longer, the president would have been awakened at 2:30 A.M. He would have been informed that he had only a few minutes in which to get to his plane, decide and issue a retaliatory plan, and get on the hot line to Moscow.

Possible Solutions

Perhaps peace is not so much a technological problem as it is a political and moral problem.

The United States and the Soviet Union have previously made arrangements concerning accidental nuclear war. Before President Nixon's 1971 visit to China, the USSR feared that China might try to provoke a U.S.—USSR confrontation by arranging for a submarine off the U.S. coast to launch a missile which would be blamed on the Soviets. Therefore, on 30 September 1971 the two governments signed an agreement designed to prevent the accidental outbreak of nuclear war. Article 3 states:

> The Parties undertake to notify each other immediately in the event of detection by missile warning systems of unidentified objects, or in the event of signs of interference with these systems or with related communications facilities, If such occurrences could create a risk of outbreak of nuclear war between the two countries.[25]

This 1971 agreement was made when there were perhaps thirty minutes between detection and retaliation. If it appeared that either side's computers had detected a launch, there was time-time to evaluate the data, time to notify the opposing side, time for the opposing side to show the error in the data. Since 1971, reaction time has decreased from thirty minutes to fifteen. With space war technology, it will go from fifteen minutes to five.

Instead of asking whether nuclear war can be avoided, we should first tackle the more manageable, but equally important, question, can nuclear alerts be avoided? Going on alert when the window of time is a mere fifteen minutes may be so provocative that the other side will be forced to go on alert to protect itself. At this point, the side with the weaker C^3I computer system may be forced into a "use it or lose it" preemptive launch. What a tragedy, especially if the alert is generated by a computer chip malfunction or a software error!

Douglas Campbell is a professor of computer sciences at Brigham Young University.

[1] Len Deighton, *Goodbye, Mickey Mouse* (New York: Ballantine Books, 1982), 115.

[2] Paul Bracken, *The Command and Control of Nuclear Forces* (New Haven: Yale University Press, 1983), 14.

[3] Richard Ruggles and Henry Brodie, "An Empirical Approach to Economic Intelligence in World War II," *Journal of the American Statistical Association* 42.

[4] Nicolas Danieloff, "How We Spy on the Russia," *Washington Post Magazine,* 9 December 1979,25; Harry Rositzke, *The KGB: The Eyes of Russia* (Garden City, N.Y.: Doubleday, 1981), 197–98.

[5] United States Joint Chiefs of Staff, *Catalog of War Gaming and Military Simulation Models, Studies Analysis and Gaming Agency,* 1977, 217–18.

[6] "Nuclear Pulse I, II, and III," *Science,* 29 May 1981, 1009–12; 5 June 1981, 1116–19; 12 June 1981,1248–51.

[7] Ibid., 12 June 1981, 1249.

[8] Charles E. Cornell, "Minimizing Human Errors," *Space/Aeronautics* 49 (March 1968): 72.

[9] House Committee on Appropriations, Subcommittee on Military Construction, *Hearings on Military Construction Appropriations for 1979,* 95th Cong., 2d sess.

[10] Senate Committee on Armed Services, "Recent False Alerts from the Nation's Missile Attack Warning System," 96th Cong., 2d sess., 1–3.

[11] "War Alert, a Comedy of U.S. Errors," *London Times,* 22 February 1971; "Why America Ignored This Message of Doom," *London Times,* 28 February 1971.

[12] "On the Alert on a Hoax," *Newsday,* 8 March 1972.

[13] A. O. Sulzberger, Jr., "Error Alerts U.S. Forces to a False Missile Attack," *New York Times,* 11 November 1979, 30; "U.S. Aides Recount Moments of False Missile Alert," *New York Times,* 16 December 1979, 25.

[14] Richard Butt, "False Nuclear Alarms Spur Urgent Effort to Find Flaws," *New York Times,* 13 June 1980, A16; "Missile Meets Traced to 46-Cent Item," *New York Times,* 18 June 1980, A16; "Pentagon Identifies Cause of False Missile Alert," *Soviet Aerospace,* 23 June 1980, 58.

[15] Bracken, *Command and Control of Nuclear Forces,* 49–51.

[16] N. F. Kristy, *Man in a large Information Processing System—His Changing Role in SAGE* (Santa Monica, Calif.: Rand Corp., 1963), 8–10, 31.

[17] "Fears of NORAD Blackout Chill Panel," *Baltimore Sun,* 21 May 1981, 8.

[18] Bracken, *Command and Control of Nuclear Forces,* 34.

[19] Ibid., 65–66.

[20] Herman Finer, *Dulles over Suez* (New York: Quadrangle Books, 1964), 418–21.

[21] Bracken, *Command and Control of Nuclear Forces,* 53.

[22] Ibid., 2.

[23] Ibid., 58.

[24] Burt, "False Nuclear Alarms Spur Urgent Effort to Find Flaws," *New York Times,* 13 June 1980, A16;18 June 1980, A16; "Missile Alerts Traced to 46-Cent Item," *New York Times,* "Pentagon Identifies Cause of False Missile Alert," *Soviet Aerospace,* 23 June 1980, 58.

[25] Gerald C. Smith, *Doubletalk: The Story of the First Strategic Arms Limitation Talks* (Garden City, N.Y.: Doubleday, 1980), 518.