Established 1845 SCIENTIFIC AMERICAN January 1985 Volume 252 Number 1

The Command and Control of Nuclear War

Nuclear weapons and strategic policy attract increasing public concern, but systems for command, control, communications and intelligence may be just as important in deterring nuclear attack and preventing escalation

by Ashton B. Carter

Weaponry tends to dominate discussions of nuclear war. Missiles and bombers, throw weights and flight times, and the elaborate counting rules of arms-control agreements provide the grist of public debate. After the weapons themselves come the plans for their use, bearing such names as minimum deterrence, flexible response and countervailing strategy. Weapons and strategic doctrine are meaningless, however, unless the superpowers also have the means to know what is happening in the chaos of crisis or war, to provide for decisions by legitimate authorities and to have orders carried out precisely and faithfully. In military parlance these capabilities form the system of strategic command, control, communications and intelligence, or C^{3}I (pronounced "see cubed eye"). Although C^{3}I has been largely neglected outside a narrow circle of experts, it is an all-important facet of the problem of deterring nuclear war, fully as important as weapons and doctrine.

All concepts of nuclear war have built into them important assumptions about C^{3}I. For example, deterrence presupposes that the nation attacked can communicate retaliatory orders to its weapons in spite of the destruction of its national capital and normal communications facilities. The idea that retaliation should be appropriate to the attack presupposes that national leaders would in fact have a clear idea of the extent of the damage inflicted; it further assumes that the counterattack would resemble what the leaders had in mind and that its "appropriateness" would be recognized by the enemy leadership.

Scenarios describing how a "limited" nuclear war might be fought imply that escalation from less than total to total nuclear war is not automatic and that limited wars can therefore be waged purposefully and coherently. The concept of protracted nuclear war levies an even stronger requirement than a single exchange of warheads does: coherent command, control and communication must persist for weeks or months after a major nuclear attack. According to Secretary of Defense Caspar W. Weinberger's Annual Statement for Fiscal Year 1983, the U.S. must possess the means "to impose termination of a major war on terms favorable to the United States and our allies even if nuclear weapons have been used." Yet U.S. military leaders have also suggested the U.S. might attack the Soviet leadership. If this vital element of the C^{3}I system of the U.S.S.R. were to be eliminated, who would be available to cooperate in terminating the war?

Such considerations raise the question of whether the C^{3}I problem renders futile many prevailing theories about nuclear war and plans for using new weapons. Some nuclear strategists imagine that a nuclear war would unfold like a chess game. Chess players, however, have complete knowledge of the positions of all the pieces, can execute precisely every move they want to make and can work out the possible consequences of each move. An analogous clarity in nuclear war is most unlikely. In addition to its importance for the deterrence of nuclear war, C^{3}I forces planners to think through the potential course of such a war in vivid detail. Consideration of C^{3}I thus lends a needed concreteness to the abstractions of nuclear strategy.

Until a few years ago public discussion of C^{3}I by knowledgeable Government officials was rare, since the issue was rightly regarded as extremely sensitive. This situation began to change, apparently because many officials believed that without more prominence C^{3}I would never get the attention it deserved. Consequently in recent years analysts have explicated the C^{3}I problem in lurid detail, even putting forward a number of alarming possibilities: the U.S. is a paper tiger that could not in fact retaliate after a nuclear attack (since the command structure could be "decapitated"); reliance on a strategy of launch under attack for ICBM's could invite disaster if warning sensors mistakenly indicated a Soviet attack; electromagnetic-pulse (EMP) effects could disrupt so much electronic equipment that most communications and computer systems simply would not work. Less common at this stage of the evolution of the C^{3}I issue is constructive advice about what can be done to make these probabilities smaller. And looming behind the quest for solutions to C^{3}I problems is the unsettling suggestion that no matter

how good the C³I equipment is and how well trained its users are, an ineradicable residue of uncertainty will always remain about the unprecedented circumstance of nuclear war.

As C³I has begun to enter public discussion it has also begun to receive renewed emphasis in actual planning. The Reagan Administration has made C³I a key aspect of its strategic modernization program, which includes the MX intercontinental ballistic missile (ICBM), the Trident II submarine-launched ballistic missile (SLBM), sea-launched cruise missiles (SLCM's), the B-1 and Stealth bombers, air-launched cruise missiles (ALCM's) and the Strategic Defense Initiative, or "Star Wars" antimissile defense research plan. C³I, however, still accounts for a small part of the budget spent on strategic forces. About a dime out of every dollar allocated to strategic forces goes to C³I, which means somewhat more than a penny out of every dollar in the defense budget.

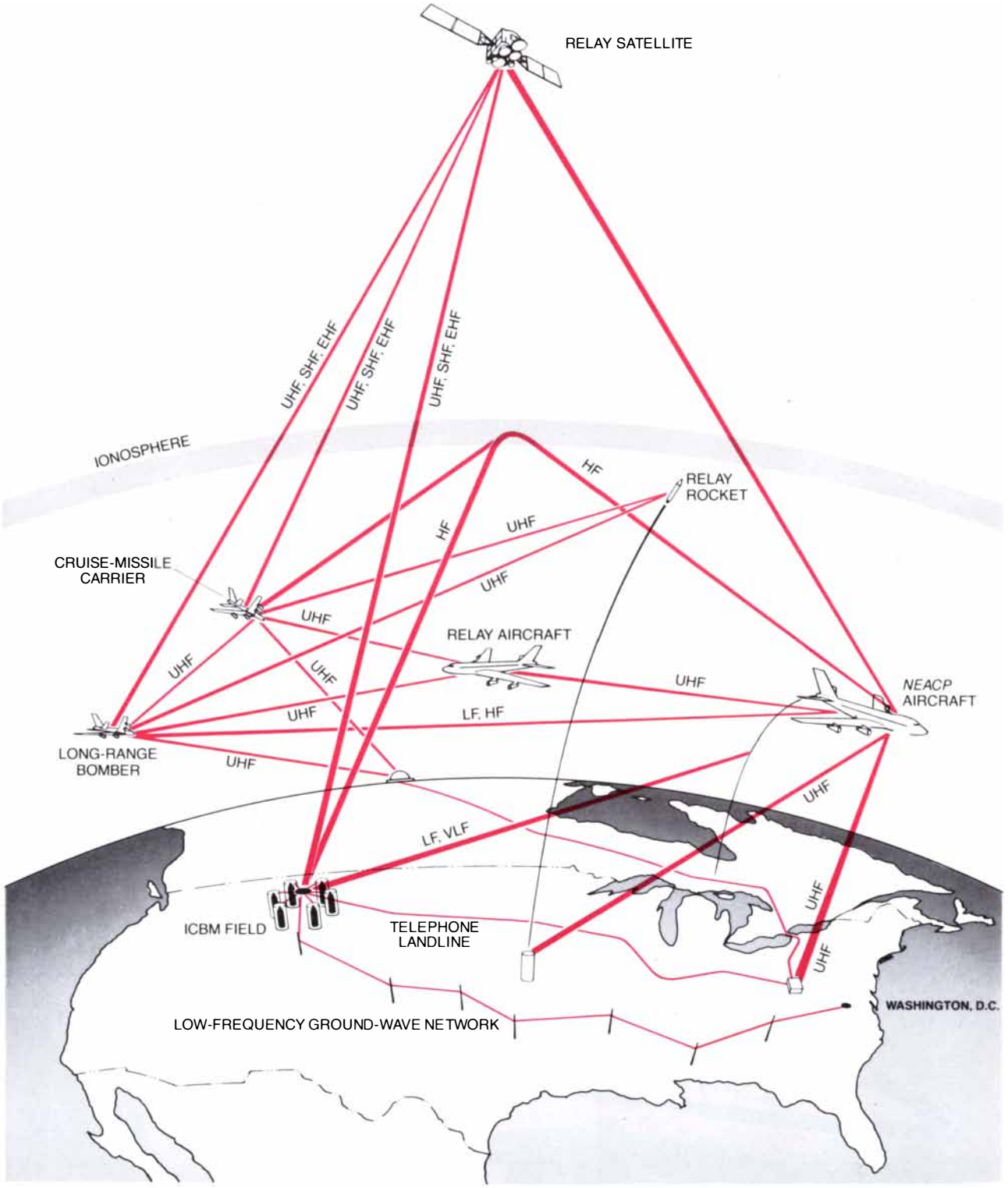
Concretely, the C³I system consists of four parts: command posts, sensors, communications links and procedures for the use of all this equipment. Command posts are needed to keep national leaders alive and in touch with the situation. Sensors provide both "strategic" warning, indicating imminent Soviet attack, and "tactical" warning, indicating that attack is already under way. The collection of strategic-warning data is allied with peacetime intelligence collection; this aspect of the "I" in C³I will not be discussed further here. In addition to sounding the alarm, warning sensors can also record for those who make decisions (and for history) where the bombs fell. Communications links carry warning data from sensors to command posts and orders from command posts to the nuclear forces. Procedures need to be worked out well in advance to rescue the leadership from Washington. Procedures must also be devised to reconcile the military's duty to exercise negative control over nuclear weapons ("Do not shoot until told") with positive control ("But respond reliably to authentic orders"). Nuclear forces must be managed in crises without unwanted provocations. Even such minutiae as tuning to a common radio frequency must be prescribed in advance. This article deals mostly with the first three elements of the C³I system, since they present well-defined technical problems and opportunities for improvement.

In approaching this task it should be kept in mind that even elaborately engineered systems can produce catastrophic results when they are faced with unexpected circumstances and pressures. In a celebrated incident in the summer of 1980 a faulty component in a data processor at the command post of the North American Aerospace Defense Command (NORAD) in Cheyenne Mountain, Colo., began generating spurious warnings of a Soviet missile attack. This incident was unimportant in itself, since the spurious data stream did not simulate a plausible attack. (The signals changed erratically with time, and the international situation was calm.) All participants in the alert agreed that the U.S. came nowhere near to "accidental war." A less easily recognized malfunction in tenser circumstances, however, could be more troublesome.

Furthermore, military operations are rife with opportunities for C³I foul-ups. The likelihood that something will go awry is compounded by the fact that the military system is so vast and complex that senior officials cannot oversee its every move. Moreover, since no one has ever been in a nuclear war, leaders would have to rely largely on preconceived notions rather than on experience and reflection. A healthy regard for Murphy's law is probably the better part of wisdom in strategic C³I.

The first technical ingredient of any strategic C³I system is a set of survivable command posts. A command post is not just a "Führer bunker" in which to hide the national leaders. They would be helpless without warning-sensor displays, communications

PRESIDENTIAL "DOOMSDAY" PLANE, officially known as the National Emergency Airborne Command Post, or NEACP (pronounced "kneecap"), is one of a fleet of specially modified Boeing 747's maintained in a high state of readiness by the U.S. Air Force for possible use in a nuclear war. In an emergency the National Command Authorities—the president and the secretary of defense (or their duly deputized alternates or successors)—would board the plane, which would then fly to its cruise altitude, where it would be in a position to communicate with the nation's strategic forces by various line-of-sight techniques (*see illustration on next page*). The plane is also capable of transmitting low-frequency (LF) and very-low-frequency (VLF) signals over the horizon by means of a long antenna trailed from the back of the plane. In addition each NEACP plane carries a satellite-communications terminal and an assortment of other gear. Although there is no way at present for the Soviet nuclear forces to target such an airborne command post once it is in the air, the plane is considered quite vulnerable to a surprise submarine-launched missile attack when it is on alert on its airstrip.



VARIETY OF COMMUNICATIONS LINKS are available to enable U.S. leaders to stay in touch with the nation's nuclear forces in an emergency. In this idealized scene the NEACP aircraft has already taken off from an air base near Washington, D.C., following the receipt of an early warning of an impending missile strike by the U.S.S.R. The aircraft is shown in communication with two components of the U.S. nuclear forces: a field of Minuteman strategic missiles in Montana and a detachment of long-range bombers and cruise-missile carriers that have taken off from their bases and flown north over Canada, where they await the order to proceed to their targets in the U.S.S.R. (If they receive no message, they will automatically return to their bases.) Because each method of communication has its own drawbacks, the system must be designed with several redundant links. For example, since telephone landlines could be severed in a nuclear attack, satellites and relay aircraft would be used to provide line-of-sight communications links over the horizon. Satellite signals, on the other hand, could be disrupted by high-altitude nuclear explosions; the resulting "blackout" effect would be particularly severe at lower frequencies. Furthermore, nuclear explosions could inject enough extra electrons into the lower ionosphere to cause high-frequency (HF) signals to be absorbed rather than refracted back down to the earth. Broadcasting at lower frequencies would require that the NEACP plane reel out a transmitting antenna several miles long. An alternative communications method calls for reading the presidential command into a tape recorder and launching the recorder on a rocket high enough to have line-of-sight contact with the strategic forces. Not all the technical possibilities shown have actually been deployed.

terminals, codes for preparing appropriate orders and a highly trained staff conversant in the arcana of fighting a nuclear war. Strategic command posts therefore must be substantial facilities, providing much more than just physical protection.

The U.S. has considered the entire spectrum of technical possibilities for survivable command posts, from deep-underground war rooms and mobile surface vehicles to ships and submarines, but it has acknowledged particular reliance on airplanes. The Air Force maintains a fleet of specially modified Boeing 747's known as National Emergency Airborne Command Posts, or NEACP's (pronounced "kneecaps"). Once such a plane is in the air it cannot be targeted. By flying at high altitude it can communicate effectively by various line-of-sight techniques over a wide area, and it can transmit very-low-frequency (VLF) signals over the horizon by means of a long trailing-wire antenna. Each NEACP plane also carries satellite-communications terminals, warning-data receivers, EMP detectors and an assortment of other gear, as well as seats for the presidential entourage.

Although a command post of this type is comparatively safe when it is airborne, it is quite vulnerable when on alert on its airstrip. An SLBM fired from a submarine just off the coast of the U.S. could arrive over the air base within 10 minutes of its launching; since it would take several minutes for the crew to get into the plane, bring the engines up to speed, taxi to the runway and take off, the ability of NEACP to survive a surprise attack depends on extreme vigilance.

One safeguard against such a surprise attack is another fleet of airborne command posts, code-named Looking Glass and operated by the Strategic Air Command. Since 1961 at least one Looking Glass plane with an Air Force general on board has been in the air at all times, 24 hours a day, 365 days a year. Presumably some of the NEACP fleet would also take to the air in a time of crisis.

Notwithstanding the fact that NEACP and Looking Glass cannot be targeted in flight, there are problems inherent in relying excessively on aircraft for survivable command posts. Even in flight such command posts are vulnerable to some nuclear-weapon effects, such as EMP, radioactive clouds, turbulent air from thousands of fireballs rising all over the country and harmful dust inhaled by their jet engines. Without aerial refueling or a place to land and refuel, the president could not wait long to make decisions involving communications by means that require NEACP to be airborne, such as line-of-sight techniques or VLF trailing-wire antenna. New airframe designs may help to alleviate this problem by making it possible to deploy aircraft that can "loiter" aloft for longer periods. Looking to the future, emerging technologies could enable the U.S.S.R. to track NEACP and give in-flight commands to missiles to home in on its position.

Clearly a vital question about a national command post is "Who is to be in it?" U.S. officials understandably avoid public comment about the sensitive issue of how continuity of government is to be ensured in a nuclear war. The authority to order the use of nuclear weapons is lodged formally with an entity called the National Command Authorities, which under normal circumstances consists of the president and the secretary of defense. Lines of succession for these offices are established, and so in theory the body would continue to exist even after the death of the principal officeholders. How the U.S. would in fact ensure the survival of an authorized command entity in the event of a nuclear war is a matter of top-secret procedures worked out in peacetime.

Warning sensors are the second major category of C^3I equipment. There is very little the U.S. could do in the 10-minute flight time of an SLBM or the 30-minute flight time of a land-based ICBM to prepare American society for a nuclear attack. Nevertheless, missile-warning sensors do serve certain crucial strategic functions. Bombers, cruise-missile-carrying aircraft and airborne command posts all need immediate warning to enable them to escape from their bases before SLBM warheads begin to explode above them. If a launch-under-attack threat is to be credible, the U.S. must show that it can reliably receive early and accurate evidence of an attack by the U.S.S.R. The most important use of the data from early-warning and attack-assessment sensors could well be the record such information provides the president about the nature and scale of the attack on the U.S. Without this information, which is not likely to be readily obtained after the warheads have fallen, the president cannot choose an appropriate response.

As in the case of command posts, there is a wide variety of technical possibilities for early-warning and attack-assessment sensors. It would be reassuring to deploy a number of sensors operating according to different physical principles, since their output is to be put to such a momentous purpose. The sensors must obviously survive long enough to do the job, as must the communications links from sensors to command posts.

A novel attack-assessment system called the Integrated Operational Nuclear Detection System (IONDS) is scheduled to be launched by the U.S. in the late 1980's aboard the NAVSTAR navigational satellites of the Global Positioning System (GPS). The IONDS sensor package will include visible-light sensors, X-ray sensors and EMP sensors to detect nuclear explosions in the atmosphere and in space. A nuclear explosion in the atmosphere produces a characteristic double-peaked light pulse with a structure that depends on the explosive yield of the nuclear warhead. By measuring the time of flight of the flash to several satellites it should be possible to locate each burst to within a fraction of a kilometer. The IONDS data would serve not only to characterize an attack on the U.S. but also to verify that the U.S. warheads launched in retaliation had reached their targets in the U.S.S.R.

In addition IONDS would record the detonation of Soviet SLBM's on U.S. territory some 10 to 20 minutes before the expected arrival of the more accurate "silo killing" Soviet ICBM's. The U.S. leadership would have additional information to use in making the dangerous decision of whether to save the threatened ICBM's by launching them promptly. NAVSTAR satellites will incorporate features designed to increase their resistance to nuclear-weapons effects and also to possible future Soviet antisatellite weapons.

Each kind of nuclear force has distinctive communications requirements. For example, the C^3I system must be capable at a minimum of transmitting launching orders to the Minuteman ICBM fields in the Middle West from Washington or from some other over-the-horizon location. The Emergency Action Message, or "go code," is a short, preformatted, encrypted message. More demanding would be the rapid response needed to launch the U.S. ICBM's that were under attack before the Soviet ICBM warheads arrived to destroy them in their hardened silos. Some strategic planners have suggested that any missiles surviving an attack should be retargeted to ensure that the highest-priority targets in the U.S.S.R. would be covered in the retaliatory strike. Such retargeting would impose yet another sophisticated communications demand.

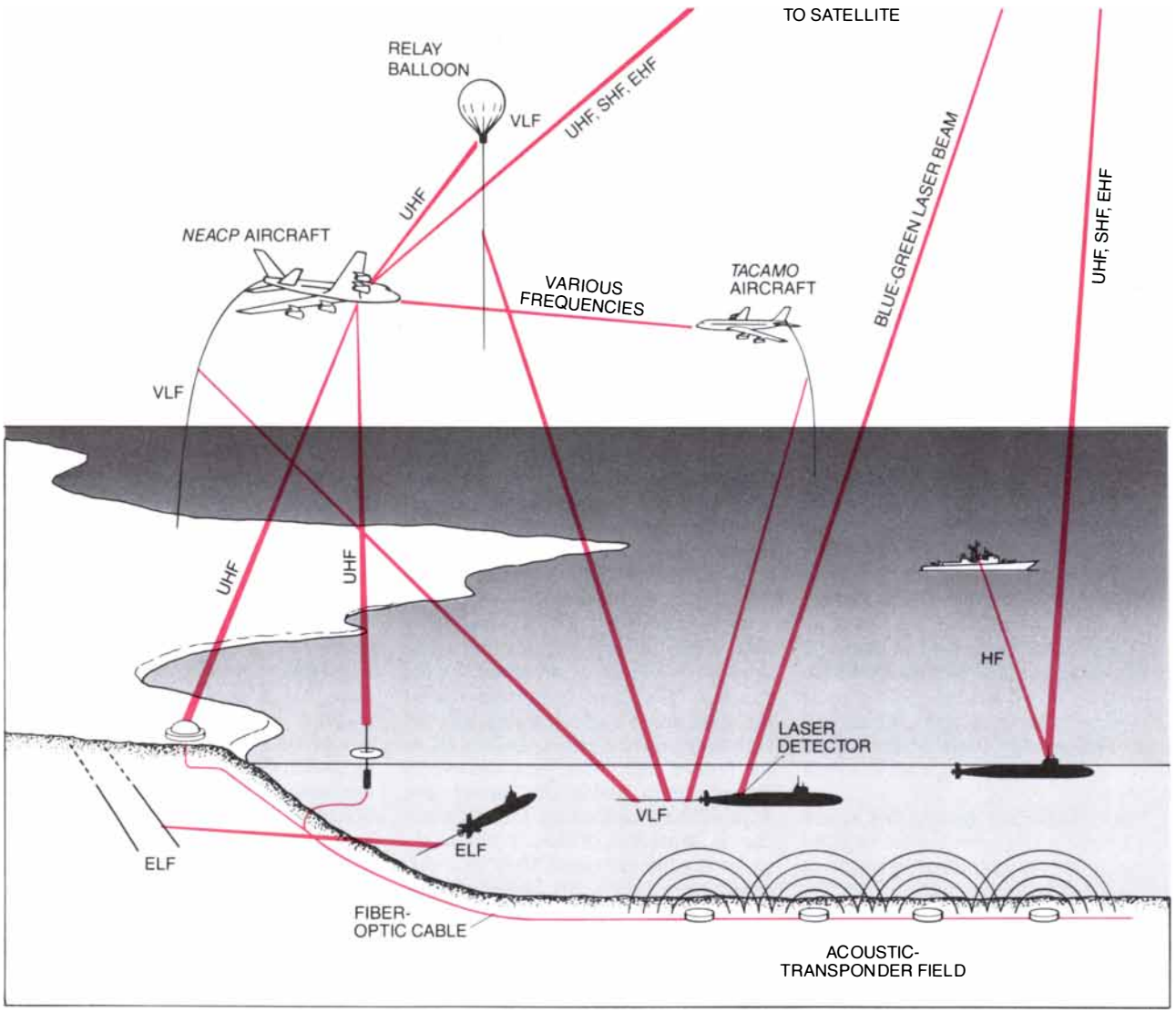
Bombers and cruise-missile-carrying aircraft have even more complex needs than ICBM's. Rapid and reliable communications from missile-warning sensors are necessary to enable the aircraft to take off and avoid destruc-

tion on the runway. Once they are airborne, the planes would head north to predesignated locations, where they would loiter aloft and await an Emergency Action Message. If they received no order to continue on to their targets, they would return to their bases. It is not clear whether bomber crews that had carried out their bombing runs over the U.S.S.R. could expect to land on the territory of U.S. allies near the U.S.S.R., refuel and return to whatever airfields remained in the U.S.; if they could, they would need additional C^3I facilities to do so.

The task of communicating to missile-carrying submarines is complicated by the long distances involved, by the paramount need for the submarine to remain hidden and by the opacity of seawater to all electromagnetic radiation except extremely-low-frequency (ELF) and VLF radio waves and blue-green light. On the other hand, the survivable submarine force would not need to depend on rapid communications or reliable warning to do its job.

In peacetime U.S. missile submarines are normally tuned to VLF broadcasts from large land-based transmitters, which could be readily destroyed at the outbreak of a nuclear war. In wartime the U.S. would rely heavily on an airborne relay system named TACAMO (for "Take charge and move out"). The TACAMO plane receives an Emergency Action Message from the national leadership and rebroadcasts it over a VLF antenna several miles long, which it trails from its tail. The submerged submarine must trail a long receiving antenna a few meters or less below the ocean surface, within the seawater penetration depth of VLF radio waves. Although the submarine itself can remain deeper than the antenna, it still must limit its depth and speed if the antenna is to work properly.

Proposals exist to exploit the two other seawater "windows," which lie in the ELF and blue-green parts of the spectrum. A radio antenna operating in the ELF range (between 70 and 80 hertz) is known to excite the character-



COMMUNICATIONS WITH MISSILE SUBMARINES are limited by the fact that seawater is transparent to electromagnetic radiation in only three parts of the spectrum: at extremely low frequencies (ELF) and very low frequencies (VLF) in the radio region and at blue-green frequencies in the visible region. Radio broadcasting at the long wavelengths characteristic of ELF and VLF transmission has two disadvantages: it requires very large antennas and power supplies, and it is limited to very low data rates. On the other hand, radio waves at these frequencies would propagate well over long distances even if the ionosphere were to be disturbed by nuclear explosions. The U.S. Navy now relies primarily on VLF relay aircraft code-named TACAMO (for "Take charge and move out").

istic modes of vibration of the resonant cavity formed by the earth's surface and the ionosphere. This phenomenon makes it possible for an ELF signal to propagate worldwide. Since the depth to which an electromagnetic signal is able to penetrate a conducting medium such as seawater increases with the wavelength, a deeply submerged submarine can in principle receive such an ELF signal.

For the sake of efficiency, however, the diameter of a transmitting antenna must be approximately equal to the wavelength of the radiation it broadcasts. Its data rate in bits per second is usually limited to a fraction of its carrier frequency in hertz. Hence an ELF antenna for a system with an effective data rate of only a few bits per minute must nonetheless be many miles in diameter. One such system has been built by the U.S. Navy in Wisconsin; its main disadvantage is that it is extremely vulnerable to nuclear attack.

Another communications scheme involves blue-green laser light beamed from a satellite to sensitive detectors mounted on the hull of the submerged submarine or towed closer to the surface. This idea is still in the research stage, and its usefulness is uncertain. Such a communications system would obviously depend on the satellite's ability to survive a direct attack.

It is possible that long VLF antennas trailed from balloons could supplement or replace TACAMO aircraft in certain circumstances. If the submarine were to tow a small buoy with an antenna, it could receive an Emergency Action Message by satellite or by high-frequency (HF) radio relay from other Navy ships at sea. Still another possibility involves sowing areas of the ocean floor with acoustic beacons linked by fiber-optic cables to floating buoys or ground stations. Altogether there is quite a rich array of technical possibilities for postattack submarine communications and no fundamental reason why an appropriate ensemble of these links should not be as reliable as the postattack links to ICBM's.

A strategic communications system must be designed to resist all kinds of interference, including physical destruction, jamming, interception or mimicking by enemy intelligence, disturbance by the ionosphere and disruption by the EMP effect. It must be assumed that radio antennas, land-line switching centers and ground-based satellite-control facilities would all be targeted in a major nuclear attack. Satellites can malfunction or fail completely without periodic "housekeeping" signals sent from ground-based control stations. As a consequence the U.S. military is planning a new generation of autonomous spacecraft that will generate most of their own control instructions with the aid of an onboard computer; in addition control facilities will be deployed in trucks that would roam the nation's highways to avoid being targeted.

Antisatellite weapons present a special kind of threat to strategic communications systems. For example, the U.S.S.R. could in the future plan to attack U.S. communications satellites with interceptor missiles, laser weapons, particle-beam weapons or remote-controlled "space mines" placed in orbit next to U.S. satellites [see "Antisatellite Weapons," by Richard L. Garwin, Kurt Gottfried and Donald L. Hafner; SCIENTIFIC AMERICAN, June, 1984]. A nuclear explosion in space could produce enough X-radiation and gamma radiation to damage a satellite at a range of many hundreds of kilometers.

Jamming a radio link means transmitting "noise" to the receiving antenna in order to drown out meaningful signals from "friendly" transmitters. A distant transmitter can jam effectively at high frequencies and very low frequencies, since these signals can propagate over the horizon. For the highest frequencies, however, the jammer must have a clear line of sight to the receiver being jammed. Operating in this way, Soviet forces in Cuba or on board ships off the U.S. coast could seek to jam the "uplinks" to satellites positioned over the U.S.

The most direct way to thwart jamming would be to increase the power of the friendly transmitter. Another way would be to use directional antennas. A directional transmitter could focus the radiated energy toward the receiver; a directional receiver would readily accept energy from the friendly transmitter. Because the directional gain of a satellite antenna depends on the ratio of the signal wavelength to the antenna diameter, extremely-high-frequency (EHF) and superhigh-frequency (SHF) communications links would be easier to protect with directional antennas than the longer-wavelength ultrahigh-frequency (UHF) links in widespread military use today.

Radio transmissions typically occupy a narrow range of frequencies called the bandwidth. A jammer must radiate noise throughout much of this bandwidth or enough of the message may reach the receiver through the unjammed part of the band to make it intelligible. Accordingly another way for the sender to improve jamming protection is to increase the bandwidth of the signal. Since the available bandwidth increases with increasing frequency, EHF satellite links would again be superior to UHF.

Still another way to protect against jamming is to lower the data rate, in effect repeating the message several times to ensure reception. Since such methods use a larger bandwidth to support the data rate than would be needed in the absence of jamming, they are called spread-spectrum techniques. The repetition pattern must be kept secret or the hostile jammer could concentrate his jamming effort in just those time and frequency intervals that contain a crucial part of the message.

Spread-spectrum antijamming techniques are closely related to methods used to encode messages. Communications security is necessary to prevent the enemy from listening in to communications among U.S. leaders or sending false messages to U.S. forces. Spread-spectrum techniques can also be used to spread a low-power transmission over such a wide bandwidth that the enemy, ignorant of the pattern needed to process the message, cannot ferret the signal out of the background noise. Using this technique with satellite communications at extremely high frequencies, submarines might in the future be able to communicate back to shore without having their transmissions detected and located.

A nuclear war would present some special communications problems. Ordinarily HF radio signals pass through the lower ionosphere, where the electron density is low, and are refracted back to the earth by the electron-density gradient in the upper ionosphere. High-altitude nuclear bursts and the radioactive clouds from lower-altitude bursts would increase the electron density in the lower layer of the ionosphere. HF signals passing through the ionized lower layer would then be absorbed, since in this layer there would be a high density of ions and neutral atoms. This "blackout" of HF signals could last for long periods.

UHF satellite signals and VHF and UHF radar beams passing through severely ionized regions could also suffer absorption. Since the absorption coefficient is inversely proportional to the square of the radio frequency, EHF and SHF signals would suffer far less from blackout than UHF signals. Nevertheless, even these frequencies could be subject to the transient interruptions called scintillations, caused as parts of the signal wave front that pass through regions of different electron density (and therefore undergo different phase shifts) interfere at the receiver.

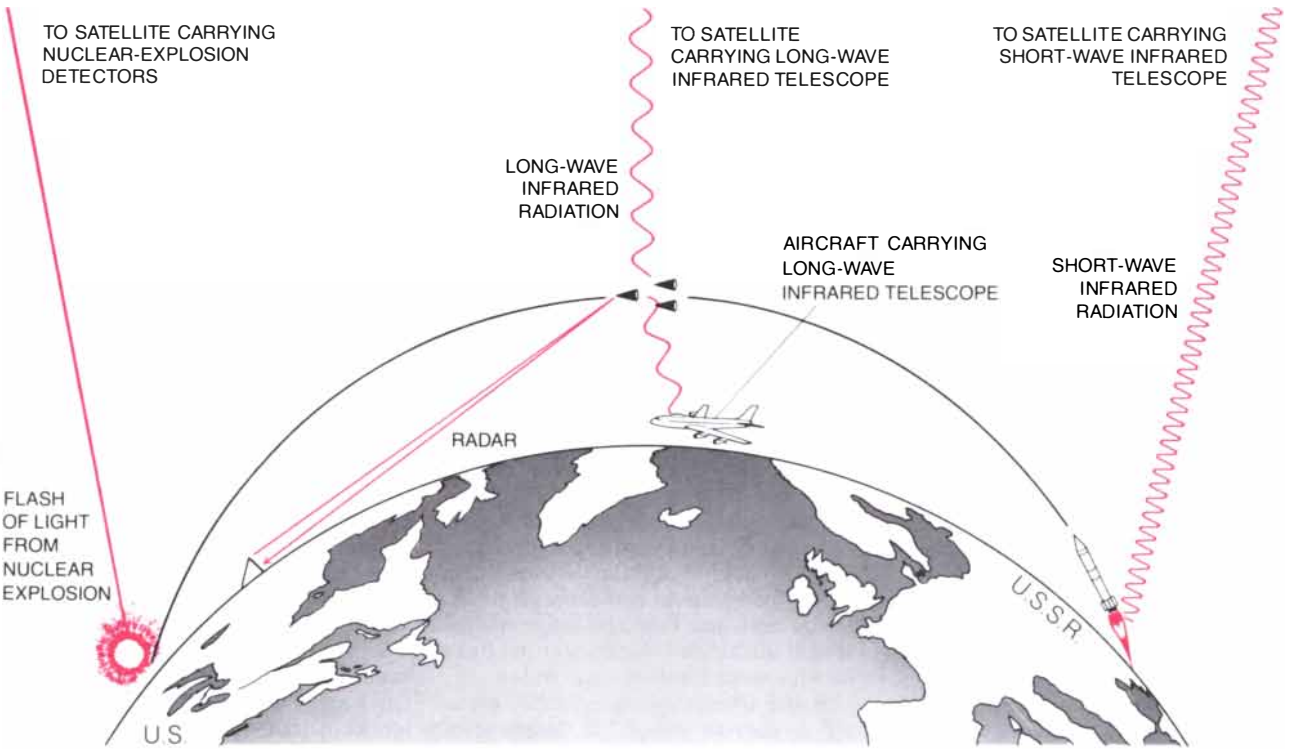
Electromagnetic pulse is a well-publicized form of interference. It is generated when gamma rays from a high-al-

titude nuclear explosion induce strong electric currents in the upper atmosphere. The resulting intense radiated fields would contain frequency components ranging from ELF all the way up to VHF. The EMP effect from a single burst at an altitude of several hundred kilometers could blanket the entire U.S. Such a pulse would enter electronic equipment through apertures and along power lines and other conductors, causing potentially harmful voltage surges. Although this effect has been analyzed intensively, complex electronic systems have so many possible failure modes, each differing in many particulars from others, that predictions are hard to make.

The many potential vulnerabilities of the C^3I systems for the support of strategic nuclear forces demonstrate that it is difficult to guarantee that the U.S. could carry out the most rudimentary aspect of its nuclear deterrent policy: to discern the nature of an attack by the U.S.S.R. and to retaliate according to a prearranged plan. More detailed doctrines for conducting possible nuclear wars require correspondingly more ambitious C^3I systems. For example, strategists who foresee a nuclear war beginning with a less than total exchange and continuing through further exchanges must also envision a C^3I system capable of supporting repeated cycles of attack and counterattack. These strategists must assume, for example, that attack-assessment sensors damaged in a first strike could still collect information and transmit it to command posts to enable leaders to make what the strategists prescribe as the appropriate response to the second attack. In a single exchange, in contrast, the warning systems might still be undamaged at the time they had to do their job. One positive note is that the situations in which the U.S. would want to make a limited response to a Soviet attack would probably be those where the attack was itself limited, and hence where damage to the U.S. C^3I system was less than total.

If the war were to be protracted, continuing "tit for tat" for several weeks or months, new problems would arise: bombers and airborne command posts would have to find surviving airfields at which to land, refuel and prepare for the next round; generators and batteries used to power support equipment in the ICBM silos after power lines were down would go dead, and satellites would be lost without ground-control commands. At the other end of the time spectrum of possible nuclear wars lies a launch of ICBM's under attack. Such a move would require near-perfect confidence in warning sensors, qualified leaders on hand at the moment of attack and rapid transmission of launching orders over the communications links.

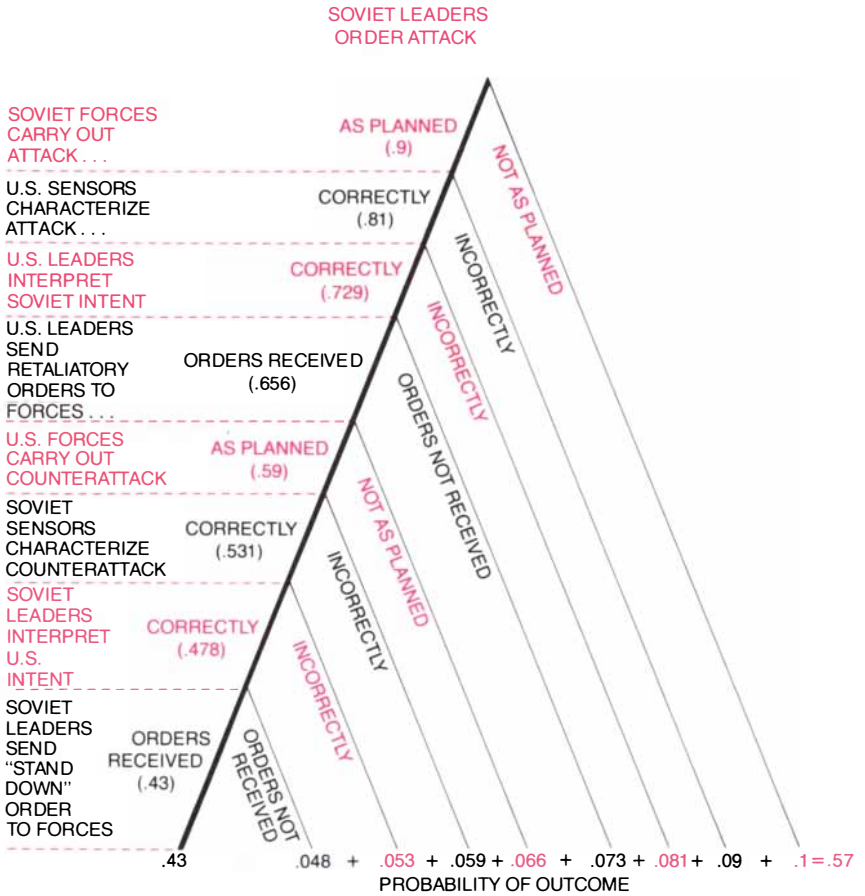
When one turns from purely military C^3I to the broader needs of governments in responding to the desperate circumstances of nuclear war, one encounters further complications. The coordination of civil defense and recovery efforts, perhaps hopeless in any event, could only be made harder by the destruction of the nation's communications infrastructure. Deciding to use the nuclear weapons deployed in Europe might involve a complicated conference of the leaders of the North Atlantic Treaty Organization (NATO). Such a conference is not likely to be



VARIETY OF SENSORS are available to provide early warning of an intercontinental-ballistic-missile (ICBM) attack and to assess the nature of the attack. U.S. leaders would presumably respond to such a warning by ordering airborne command posts, bombers and cruise-missile carriers into the air before they could be destroyed on the runway. They might also decide to give the launch-under-attack order to U.S. ICBM's before they could be destroyed in their silos. Perhaps the most important use of the warning data, however, would be made after the attacking missiles had arrived at their targets: since the output of the sensors might be the only clear indication the president ever gets about the scale and intent of a nuclear attack on the U.S., this information could be instrumental in determining whether and how the U.S. would retaliate. Short-wave infrared sensors would first detect the hot exhaust plumes of the missiles. Radars would later observe the approaching warheads and missile fragments. Later still, other satellite-based sensors would detect the actual nuclear explosions. Long-wave infrared sensors, which could record the infrared glow of the warm warheads against the cold background of space, have not been deployed, but they and other advanced sensors are currently being developed by the U.S.

any easier to arrange than communications within the more cohesive U.S. military, which would be hard enough in the circumstances.

The leaders of the U.S. and the U.S.S.R. would communicate, after a fashion, through the violent actions they ordered. Beyond that, it is unclear how they could confer in order to bring hostilities to an end. In peacetime the hot line serves this purpose. This teletype system linking the capitals of the two countries is being upgraded to include facsimile transmission, enabling the leaders to trade charts and maps. Proposals to add voice or video links have been consistently turned down for fear that such intimate, real-time contact between leaders in a crisis could foster subjective reactions and misunderstandings. All the hot-line terminals in the U.S. and the U.S.S.R. are in prime target areas. From these terminals the signals would go out over vulnerable landlines and from satellite ground stations. Two-way HF radio communication requires nothing more than that the ionosphere recover from its nuclear-explosion-induced disruption. It could therefore serve to connect the leaders of the two sides after a nuclear exchange, if appropriate agreements were made beforehand between the two countries.



HYPOTHETICAL PROBABILITY TREE illustrates schematically the possible outcomes of a limited nuclear attack on the U.S. According to the prevailing strategic doctrine, an "appropriate" U.S. counterattack would induce the U.S.S.R. to end hostilities without triggering an all-out nuclear exchange. In a real war, however, there would be a chain of individual events involving command, control, communications and intelligence (C³I), any one of which could divert this simple scenario into other outcomes. None of the unexpected outcomes "makes sense" in terms of strategic theory, and yet taken together they are actually somewhat more likely than the predicted "coherent" outcome. At each stage in this hypothetical model the "wrong" outcome was arbitrarily assigned a probability of 10 percent.

In many ways the most vital C³I challenge is not war itself but the prelude to war. Effective crisis management presents a host of C³I issues. Good crisis communications within the U.S. Government and between governments is essential. "Hair triggers" built into nuclear forces put excessive demands on the C³I system in a crisis. The realization that nuclear weapons are subject to preemptive destruction (as in the case of silo-based ICBM's) or to capture (as in the case of battlefield nuclear weapons) may lead some national leaders to conclude that rapid decisions based on spotty information are necessary. In such conditions the choices might appear to be "use 'em or lose 'em."

In peacetime the very possession of nuclear weapons imposes on the nations having them the gravest demand for responsible C³I. Procedures and technical systems must prevent unauthorized individuals, be they technicians or generals, from launching nuclear weapons. The U.S. military requires that all tasks involving nuclear weapons, from routine repairs to missile countdowns, be accomplished by two people rated in the same specialty. Many nuclear weapons have additional technical devices to prevent their crews from arming them without "enabling" codes from higher commanders. Nuclear-weapons systems must also be immune to accidental launching or detonation. Finally, nuclear weapons must be protected from theft by terrorists, foreign nations or even an ally who abruptly turns hostile.

If advanced technology sometimes seems to heighten the dangers of nuclear war, it seems to have a clear opportunity to help in improving strategic C³I. Improvements in reliable sensing and data processing, resilient communications systems and survivable command posts deserve public support. No single component can be made absolutely invulnerable, but disruption can be made difficult, time-consuming, costly and above all uncertain to the adversary. Just as important is sensitive attention to procedures. Arms-control agreements, by limiting the deployment of "hair trigger" weapons, by enacting confidence-building measures and perhaps by limiting antisatellite systems, could also help the C³I system to do its job.

Although money and effort can and should be spent to improve C³I, no level of effort can ever dispel the fundamental unpredictability of nuclear war. In most cases one cannot foresee precisely the physical effects that would determine the C³I system's behavior, much less predict the interaction of people and machines in chaotic circumstances they can never fully anticipate. Some observers go so far as to suggest that improving C³I will foster an illusion of control over nuclear war. Although this is probably too extreme a view, it is impossible to have confidence in any one theory about nuclear war, and confidence in strategic theories invariably declines as they are elaborated and detailed. In a fundamental sense there are no experts on nuclear war and no predictable details. One can only hope that the situation remains that way.