Science & Global Security, 1990, Volume 2, pp.1–20
Photocopying permitted by license only
Reprints available directly from the publisher

Printed in the United States of America

Aborting Unauthorized Launches of Nuclear-armed Ballistic Missiles through Postlaunch Destruction

Sherman Frankel[a]

The establishment of postlaunch controls on nuclear-armed missiles, which would enable a country to destroy its missiles in flight in case of an accidental or unauthorized launch, would add another safeguard to the control of nuclear weapons. A system of postlaunch control could be made secure against attempts by another country to use the system to destroy *authorized* launches in flight.

ALTHOUGH THE UNITED STATES and the Soviet Union have always been concerned over the possibility of *accidental* or *unauthorized* launches, the history of the introduction of new technologies teaches us that questions of performance invariably precede questions of safety. (Witness the early stages of the introduction of steam engines, autos, airplanes, chemicals, drugs, and even nuclear power plants.) In the case of nuclear weapons, it was not until the 1960s, after the United States' arsenals had risen to 20,000 weapons, that locks were placed on US nuclear weapons overseas. These locks, called "permissive action links" (PALs), are designed to separate possession of weapons from permission to use them.[1] PALs contain electronic locks, and closely held codes have to be used to unlock a weapon. Yet, 30 years later, PALs are still not installed on the thousands of nuclear weapons deployed on US naval vessels. There, we depend solely on human procedures for *pre*launch controls.

a. Department of Physics, University of Pennsylvania, Philadelphia PA 19104

As we look back at the Cold War period, many of us would conclude that the probability of an *authorized* launch during this period may not have differed appreciably from the probability of an *un*authorized launch. Yet the financial and intellectual resources devoted to *negating* the effects of an accidental or unauthorized launch are negligible compared with those devoted to ensuring authorized launches. Even now, with the chance of authorized launches receding, we pay scant attention to the question of postlaunch control (PLC) of nuclear-armed ballistic and cruise missiles.

This is not to ignore the large number of safety features built into nuclear weapons. Some controls are designed to forestall simple accidents, such as fires or shock, that might set off a nuclear reaction. Others are designed to eliminate human error. For example, it is impossible to send a signal that would detonate the warhead of a modern intercontinental ballistic missile (ICBM) when it is resting in its silo, because weapons are armed only in flight.

Nevertheless, a range safety officer with destruct-button in hand can abort missile tests or even flights of a space shuttle,[2] whereas no such postlaunch remote-destruct capability exists on nuclear-armed missiles.

HISTORY

Surprisingly, there already exists an agreement between the United States and the Soviet Union, usually referred to as the 1971 Accidents Agreement, that specifies what is to be done in the event of an accidental or unauthorized launch of a nuclear weapon.[3]

Article 2 of that agreement states: "The Parties undertake to notify each other immediately in the event of an accidental, unauthorized or any other unexplained incident involving the possible detonation of a nuclear weapon which could create a risk of outbreak of nuclear war."[4] It continues: "In the event of such an accident, the Party whose nuclear weapon is involved will immediately make every effort to take *necessary* measures to *render harmless or destroy* such weapon without its causing damage" [emphasis added].

What makes this second sentence so remarkable is that, in the ensuing decades, *no capability* to remotely divert or destroy a nuclear-armed missile resulting from an unauthorized launch has been deployed by the US govern-

ment. Yet there is no other way to negate a mistaken launch. Gerard Smith, chief US negotiator of the Accident Agreement, remarked in 1980 that the agreement "establishes in international obligation that every feasible effort be taken to prevent nuclear war as the result of accidents."[5]

Further, pursuant to Article 7, which provides for implementing or amending the agreement, there is no evidence that, in ensuing meetings of the Standing Consultative Commission, the wording of Article 2 has been modified to change its clear intent.

Many of US arms-control negotiators and much of the US arms-control community do not remember or pay little attention to this requirement of Article 2 of the Accident Agreement: it is not mentioned in the Arms Control and Disarmament Agency summary of treaty features,[6] nor in articles and books dealing with arms-control agreements.[7] Searches of archives of the US Air Force, and of US defense contractors including Aerospace, Rand, and TRW, as well as discussions with program managers at Mitre, IDA, and the Pentagon, fail to reveal any official studies of postlaunch control of nuclear weapons. In discussions with high-ranking members of past administrations, who would have known of or had access to such a study,[8] nothing has been unearthed.

A DESTRUCT-AFTER-LAUNCH SYSTEM

By analogy with "permissive action links," we call postlaunch controls "destructive action links" (DALs). They have also been called "destruct after launch" or "command–destruct" systems.[9] We refer to the center where the abort decision is made as a DAL control center or DALCC.

A system for remote negation of an unauthorized launch would comprise hardware and procedures to a) detect unauthorized launches, b) relay the information to an appropriate control center, c) make the decision to abort, d) relay the appropriate destruct signals to the errant missile, and e) provide realtime information of the event to relevant countries.

Detection of Launch

In order to negate an undesired launch it is necessary for a country to have unambiguous and timely notification of all of its launches. Only partial capability of early detection now exists, but there are no technical problems in achieving the appropriate early notification.

ICBMs

The launch of an intercontinental ballistic missile could be detected by radar at a special detection center in the home country that was positioned at or near the missile field, by sensors near the individual silos, or by special circuits at the normal launch control center. The launch detection information would be sent immediately to a local DAL control center or to other DALCCs higher in the command chain. Independently, the near-infrared (IR) radiation from the booster exhausts would be detected by early-warning satellites in the same way that Soviet launches are routinely detected today by the US.[10] US early-warning satellites are already positioned so that they could detect US as well as Soviet launches.*

SLBMs

Sea-launched ballistic-missile launches could similarly be observed by satellite IR detectors or by radars placed on other naval vessels.

Cruise Missiles

Cruise missiles cannot be detected by IR sensors in satellites because they do not emit strong infrared signals. One way to solve this problem would be to utilize a small transmitter to announce the launch of a nuclear-armed cruise missile, sending a signal back to the home country via satellite transponder. Because cruise missiles take hours to reach target, the announce signal could be delayed to avoid betraying the launch position.

---

* Actually, as we shall discuss later, there are reasons to deploy special satellites that are dedicated to postlaunch control functions.

Response to Unauthorized Launch

The responsibility for authorized launches of nuclear weapons by the US lies in the hands of the President and the National Command Authorities (NCA). Clearly only those authorized to make the launch decision may define what is meant by an unauthorized launch and issue a destruct order. Therefore, at the NCA level, these decisions must lie in the same hands.

Postlaunch control must be intimately connected with operational methods for devolving authority in time of crisis—methods that are highly classified. However, the general structure of devolution of both launch and destruct authority must follow the rules that a) the launch and destruct operational functions be separated at any command level that is not authorized to make a launch decision and b) if launch authority is legally devolved, destruct authority must also be devolved to the same level. The introduction of DALs will require careful integration with present operations.

Communicating the Destruct Signal

To destroy a missile remotely in flight requires the transmission of a coded destruct signal, which we call the DALcode. Because of the earth's curvature and the use of high-frequency transmissions, the signal must normally be transmitted from a DALCC to the missile via transponders located in satellites. (Under certain circumstances, discussed later, missiles might be aborted in boost phase, using direct short-range transmissions.) Most mislaunched ICBMs or their re-entry vehicles would need to be destroyed in space, far from the launch point but before re-entering the atmosphere. Near apogee the re-entry vehicles (RVs) carrying nuclear warheads could be destroyed with commands relayed via geosynchronous satellites. (Two or three properly positioned geosynchronous stations, like the early-warning satellites positioned over the Atlantic, Pacific, and Indian oceans, would cover most missile flight paths.[11]) Relays on lower-altitude polar-orbiting satellites might also need to be deployed.

It is not difficult to calculate the power required for a transmitter on a geosynchronous satellite to transmit to an antenna located on an RV.[12] For an S-band (10 centimeter) wavelength to cover the earth with a variation of less than a factor of two in uniformity requires only a single 40-centimeter-

diameter dish, mounted on the satellite. We assume no gain in the RV antenna, which also ensures reception from almost all directions. We assume a 300-K noise-temperature receiver, although lower–noise-temperature gigahertz receivers are available commercially. The remaining quantity needed to be specified is the bandwidth of the receiver. This depends on the length and number of messages. To get an upper limit to the power required, we have assumed 50 separate DALcodes, each transmitted six times with a "quiet time" between messages that is 10 times the message length. Allowing 10 minutes in the ICBM flight for receipt of 32-bit messages sets the message length and yields a bit rate of 160 per second. We also add in a factor of 10 for transmitter circuit and other power losses.

With these assumptions we find that the required *peak* transmitted power is not more than 12 watts. Even this estimate is conservative since this power could be divided between several satellites at different longitudes with narrower beams. Transmitters on polar-orbiting satellites would be much closer to the missiles and would require less power (see appendix 1).[13]

We conclude that the required electronic receiving or transmitting systems are quite conventional. The major costs will lie in the deployment of satellites and the modification of RVs to contain the antenna and receiver.

The Destruct Method

To prevent an unauthorized launch from causing damage, one could arrange a signal to disarm the nuclear weapon in flight. That would surely be the cheapest and technically simplest way. Unfortunately this method cannot be the only option. To manage the crisis attendant on a mislaunch and to forestall any possibility of a retaliatory launch on warning, the targeted nation would have to be convinced that the missile and its warhead had been destroyed.

Ballistic Missiles

The destruct method could involve the booster, the postboost vehicle (PVB), or the re-entry vehicles, depending in part on the system response time. If the system response time from launch to detection to abort-decision was negligible, the missile could be destroyed in the boost phase. The apparatus for this

task already exists for test launches, and transponders in satellites would not be needed. Conventional explosives would be used. The missiles would not have traveled far enough to be seen on the radar screens of the targeted nation, even if the IR signals had been detected.

However, this is not a safe scenario if used alone, since appreciable time is needed to detect a remote launch, evaluate the legality of the launch, and carry out destruct orders. That time could easily outlast the boost phase.

Destruction of the weapons in midcourse, far above the earth, would both allow time for the decision to be made and to minimize the impact on the earth that destruction might have. In this event the threatened side would have to be informed since the missile would have appeared on its radars. It should be notified of the position, time, and trajectory, to enable it to observe that the missile had indeed been destroyed. The warhead could be destroyed by conventional or nuclear explosion:

Conventional Explosion: This would require high-explosive (HE) charges on a re-entry vehicle sufficiently powerful to prevent detonation of the nuclear charge as well as to produce an explosion of the RV body that could be detected by the other side's radar. For a small weight-loss penalty, one could add an explosive charge. Or one might use the HE already in place in the implosive system on the warhead. Unfortunately, a conventional explosion might be contrived that did not destroy the warhead or alter its path but only simulated a destructive explosion.

Nuclear Explosion: Observation of x-rays from a nuclear detonation at the position of the re-entry vehicle would prove that the weapon had been destroyed. It would be best to detonate the warhead with very low nuclear yield and preferably near apogee for the least effects on earth. A low-yield detonation could be obtained by effecting an inefficient explosion of the primary fiission stage so that the thermonuclear secondary would not be ignited. This might be done by initiating a firing option that resulted in an inefficient implosion of the high-explosive trigger. Alternatively, it might be accomplished by shutting the valve that allows introduction of tritium to the fission primary.

X-ray detectors in geosynchronous orbit or on other space platforms could verify that the weapon had been detonated, even at very low yield.

Cruise Missiles

The destruct method for cruise missiles would be quite different from that used for ballistic missiles. Microprocessors are built into cruise missiles that control the path of the missile using either inertial guidance or terrain-following radar. The destruct message could direct the microprocessor in the missile to: disarm the nuclear weapon, change course away from the target to a new, uninhabited destination (over an ocean or the North Pole, for example), climb to an altitude at which it could be more easily observed, and use the built-in altimeter or a special transmitter as a beacon to announce the change in course. Alternatively the destruct message could simply initiate an HE detonation or a crash.

The changes required to install remote-destruct systems in cruise missiles would result in only minor range penalties and considerably less redesign than the corresponding modifications of RVs.

SECURITY ISSUES: CRYPTOGRAPHY AND ESPIONAGE

We now turn to the security concerns that inevitably surface in discussions of postlaunch control of nuclear weapons. Could the DALcode be discovered and used by an enemy to abort an authorized launch?

It is important to appreciate that an instruction containing intelligence—for example, the encrypted message "destroy the weapon"—is quite different from a random number, agreed on beforehand by both sender and receiver, to be *equivalent* to the message "destroy the weapon." If the message "destroy the weapon" were encrypted before being sent over insecure lines, a cryptanalyst could use the intercepted encrypted message to "break the code." The enemy could then use that information to recognize words in future encrypted messages. However, an enemy receiving a random number learns nothing about any other random number that might later be sent.[14] Thus the DALcode is just a random number that matches an identical number inside the missile.

The DAL system must be designed to prevent an enemy from guessing a DALcode in time to destroy an authorized launch. Also, since the DALcode must be changed periodically to reduce the chance of espionage, some means

are needed to send the new DALcode from the missile to a remote control center in an unconditionally secure way (see appendix 2).

Guessing the DALcode

The reason that bank vault combination locks can be made secure from the "keep trying" method of finding the combination is that there is simply not enough time to try all the combinations at random. Suitably applied, this restriction can also prevent an enemy from being able to remotely trigger the DAL destruct mechanism.

Consider a weapon containing a "lock" or switch controlled by a "combination," which can be a binary digital number (for this discussion, a 32-bit string of 1s and 0s), which we have called the DALcode. The switch can be closed (and the DAL system activated) if it is supplied with a recognized DALcode.

There are about four billion combinations in a 32-bit string of 1s and 0s. Although it might only take a few seconds for a modern computer to broadcast these codewords until the correct one was found to activate the DAL, this presents no real problem of security. The DAL designer can arrange to open the path to the lock for a time very short compared with the flight time of the missile. Suppose the system is designed so that it is open to allow the signal to be accepted only enough times to be sure that no error in transmission has taken place (that is surely a requirement for a reliable system). If there are only n tries allowed, the chance of opening a lock with N possible combinations is n/N. In our example of a 32-bit combination, the chance of the enemy finding the combination would be much less that one in a million even if the system permitted 100 tries. Thus we conclude that the chances of guessing a DALcode are negligible.

Intercepting the DALcode

The possibility of interception of a DALcode is a concern, since a command center would be communicating with the missile in its launcher periodically to determine that the DAL circuitry was functioning properly and to change the DALcode periodically to reduce the possibility that espionage had compromised it.

The codes could be changed by generating a new random number at the

missile—a replacement DALcode—which could be inserted into the missile in place of the old. The new DALcode must then be sent securely to the DAL control centers. In order to avoid the DALcode being intercepted en route, it would be encrypted with a random number key to produce yet another random number that would be of no use to an eavesdropper. The key would reside at both the missile field and the control center.[15] (The procedure could also be reversed, the new codes being generated at the DAL control centers.)

DALcode Protocols

Aside from the cryptographic security of the DALcodes, the message "protocol" could also be used to keep the system secure.

The following are examples of such protocol information: 1) At what clock time and for what period is the DAL circuit open to receive the signal? 2) What length of signal contains the message? Are there blank bits and are portions of the word filled with other useful information? 3) At what frequency is the signal transmitted from the land transmitter, and what frequency from the satellite transponder?

Since these are facts that the enemy would need, and the parameters could be changed on a periodic basis, they add to security without appreciably adding to the complexity of the destruct system.

Espionage

One source of risk is espionage in DALCCs located at the missile field. However, missile fields are secure military installations, already "espionage hardened" against interference with release codes and emergency action messages. Even so, since only a small fraction of the arsenal would be at a particular missile field, espionage there would not affect a large fraction of the retaliatory ICBM force.

Another risk is espionage higher in the chain of command. While the National Military Command Center (NMCC) may be more secure than a missile field, as one goes higher in the command chain the number of DALcodes residing in one physical area will increase. Such centralization of codes always results in higher risk that a large fraction of weapons might be compromised. Recall that the US President has with him (or in the possession

of an accompanying officer) the appropriate release codes needed to launch all US strategic nuclear weapons. Since the President is the ultimate authority for release of the codes, they can not be stored in a remote place even to secure them against espionage: the President must not be separated from the PAL codes by any link that can be destroyed or compromised.

DALcodes have a somewhat different role. If a DALcode is needed to abort an *accidental* launch, it is likely to be when there is no all-out attack and when communication links are intact, so there will be less difficulty in contacting the President or his advisers. If the need arises to counter an unauthorized launch, it is possible that some communications channels might have been broken. However, by separating the codes into groups, storing them at separated hardened locations, and using the most survivable communications channels, the probability of losing the ability to transmit the codes to the President could be made small. Also, a system of using separated storage centers, each controlling only some of the codes, would make it extremely difficult for another country to steal enough of the codes to even begin to disarm its adversary.

Security could be increased still further by the use of "split" codes, with pieces of the same DALcode residing at more than one center, so that two or more centers would be needed to piece together one entire DALcode. Another way would be to send the split words via different transmitting stations, combining them in the missile. The reliability of split codes can also be increased by requiring only n out of m subcodes to reconstruct the full DALcode.

Getting Around Espionage

There are no general principles that can be invoked to guarantee that the probability of espionage can be reduced to zero. However, as McGeorge Bundy has remarked, "The President would want to be told that there is *no* risk."[16] To provide the possibility of such an assurance, DALs could play different roles in peacetime and times of crisis than they do in wartime. In time of peace, one would have the DAL circuits activated and ready to act on the DALcode destruct signal. This would also be the mode in time of crisis, when the possibility of unauthorized launches would increase. However in case an

irreversible decision were made to launch, the DAL circuitry could be designed to accept in addition to the destruct code a "disable code". The disable code would turn off the DAL; that is, it would block the DAL from acting on a legitimate DALcode. No provision would be made to subsequently re-enable the DAL circuitry remotely. The possibility that the enemy could destroy one's weapons by clandestine possession of the destruct code could thus be eliminated by disabling the destruct mechanism itself.

Once the DAL control center learns that a weapon has been fired, as the result of a legitimate launch order, (but not in a "launch on warning" mode—see below), it is free to send the disable code rather than the DALcode. Or it can choose to do so even before the Emergency Action Message (EAM) is sent, if the decision to attack at some later hour has been irrevocably made. Adding disable to destruct capability may add to the operating instructions, but it provides a final level of assurance that could be invoked if desired to guarantee that the enemy could not destroy a weapon that the launcher did not want destroyed. This is an important component of the DAL system.

Since the disable method would only be needed if there were a real fear of breakdown in the DALcode security, one could consider keeping the disable codes high in the chain of command even when the launch codes were devolved to a lower level of command. In this way the DAL control center could still destroy a weapon fired by some misunderstanding at a lower level of command.

There therefore does not appear to be any scientific, cryptographic, or logical basis for rejecting postlaunch controls on grounds of national security. The remote possibility that an enemy could gain possession of even a fraction of the destruct codes can be countered by designing in the possibility of remotely disabling the DAL circuitry when the decision to wage nuclear war was made.

OTHER CONCERNS

PALs and/or DALs

At least two former secretaries of defense, Harold Brown and Robert McNamara, have argued for the deployment of PALs on naval weapons. The

political will of the President is probably required to achieve their introduction. Nevertheless, a DAL system may be able to change the boundaries of the discussion. After all, the presence of DALs in no way impinges on the operations of a naval commander. Once his weapon is launched he has no further responsibility. We have found that retired submarine commanders are implacably opposed to PALs and extremely uncomfortable with DALs (mainly because they threaten to add weapon complexity and unreliability), but if forced to choose, show some preference for DALs over PALs. Preventing a naval commander from firing a weapon under his command is not the same as reversing his action after the fact. Thus DALs might accomplish the same ends as PALs, where no PALs now exist, without raising emotional issues that may have prevented PAL deployment. In any event, a serious public assessment of the value of deploying DALs may re-energize discussion of naval PALs, which has remained dormant. (Putting PALs on naval weapons would, however, be much cheaper than deploying a DAL system.) Even if PALs were in place, DALs could serve as another independent level of safety.

Launch on Warning[17]

It is generally believed that both the US and USSR have operational arrangements in place that allow for retaliation against a first strike before the incoming weapons have actually reached their targets.

Proponents treat launch on warning as a deterrent to a first strike, serving to dissuade the enemy from attacking MIRVed ICBMs in their silos. Opponents fear that mistakes and misinterpretation in time of crisis will result in actual launches in response to incorrect information of attack, resulting in an inadvertent nuclear war.

The weakness of the proponents' argument is that it is based on the assumption that the launch on warning posture is *credible* to an enemy. The main reason to doubt its credibility is that the actual time available to the national command authorities to decide that an attack has taken place is very small. By the time the information is collected and transmitted and the authorities are assembled, precious few minutes are left for such crucial decision making. Thus an enemy may believe that launch on warning would never be used and not be deterred from a first strike. However a DAL system

would materially alter the equation since it would allow the authorities the additional ICBM transit time (about 20 minutes) to come to a correct assessment. With that time available, launch on warning of some fraction of the ICBMs becomes more credible and thus gains value as a deterrent.

On the other hand, it could be argued that a president of the US or the Soviet Union might use his ability to abort weapons in flight to "play chicken" with nuclear weapons, although the nuclear history of the past 40 years hardly suggests this as a realistic scenario.[18] Whether one favors launch on warning or not, a DAL deployment would considerably alter the arguments about the wisdom of such a strategy.

Cooperative Measures

DAL deployment may be an attractive area for cooperation between nuclear powers to improve nuclear weapon safety, especially since it is to each side's advantage that the *other* side deploy DALs.

Listed below are some possible areas of cooperation:

Joint Technical Collaboration

One obvious area of cooperation would involve joint US–Soviet launching of the transponder satellites to relay the destruct signals to an errant missile. For example, separate packages containing the classified circuitry of each nation could be installed on the satellite. Satellite, booster rockets, and launch costs could be shared.

Crisis Management

Any DAL system must rely on prompt notification to the target country that an unauthorized launch has taken place. It would be desirable to provide details of the exact time, position, and trajectory of the missile to allow verification of the destruction. "Hot line"-like communications should therefore be built in automatically at the DAL control level.

International Agreements

A consideration of postlaunch controls helps focus the question of responsibility for accidents, since it implies a responsibility on the part of the negligent

party to negate a launch. Consideration of a DAL deployment would help begin the debate on economic and legal implications of unauthorized launch.

RECOMMENDATIONS

The executive branches in the US and USSR should initiate high-level parallel studies of postlaunch controls. Alternatively, the US Senate or House Armed Services Committee and its Soviet counterpart could commission such studies. These studies should not be carried out solely by those presently entrusted with the safety of nuclear weapons. The groups should include independent experts versed in the entire spectrum of technical, strategic, and policy questions that must be addressed.

Even before the studies are complete, the US State Department and/or the Soviet Foreign Ministry should put the more general problem of nuclear weapon safety on the arms-control negotiating agenda at Geneva. While the START agreements will start the world towards a reduction in nuclear armaments over the next few decades they will have little (positive or negative) effect on the danger posed by unauthorized launch.

ACKNOWLEDGEMENTS

Discussions with B.G. Blair, R.L. Garwin, and T. Postol are gratefully acknowledged, as is support from the John D. and Catherine T. MacArthur Foundation, the University of Pennsylvania Research Foundation, and the Ruzena Bajcsy Fund.

Appendix 1

POWER REQUIREMENTS FOR SATELLITE TRANSPONDERS

The power required to get certain reception of destruct signals by an antenna and receiver located on a missile depends on the distance between the missile and the transponder on the satellite. To get an upper limit to the required power we present calculations for the case of a satellite in geosynchronous orbit 42,000 kilometers from the earth's center (1/7 of the way to the moon). Since the power varies inversely with the square of the distance, it is easy to scale down the power requirement for satellites in lower orbits.

To detect a signal reliably, we require that the received signal be larger than the "noise" in the receiver. The noise power $P_n = kT\Delta\nu$, where $k = 1.38 \cdot 10^{-23}$ joules per kelvin is Boltzmann's constant, T is a characteristic temperature that depends, among other things, on the temperature of the components in the first amplifier stage, and $\Delta\nu$ is the bandwidth, a measure of the range of frequencies to which the receiver responds. If destruct signals are transmitted over a long period of time (seconds rather than microseconds) narrower bandwidth receivers can be employed. Since codes are sent as computer bits, the larger the number of bits that must be sent per second, the larger will be the needed bandwidth.

If the transponder concentrates power in a small cone aimed at the receiving antenna in the missile, rather than sending the power out in all directions, less power will be needed. The ability to concentrate the power is called the "gain" G of the antenna. Similarly, the larger the "effective area" of the antenna on the missile, the larger the fraction of the transmitted power it will intercept and the less power that will have to be transmitted. The effective area of the antenna is also called its "absorption cross section" σ.

For good reception, the ratio of the received power P_r to the noise power P_n, called the "signal to noise ratio," must be large. Usually a ratio of 10 is considered to be adequate.

To calculate the required power is straightforward, using simple formulas from electricity and optics. Since we choose the transmitted power to cover the earth from the satellite with little variation (at most a factor of two) over the surface of the earth, the "diffraction" properties of a parabolic antenna set the ratio

$$\frac{\lambda}{D} = \frac{r}{0.6R} \tag{1}$$

where r is the earth's radius (6,370 kilometers), R the distance from satellite to the earth's center, D the diameter of the parabolic "dish" antenna on the satellite and λ the wavelength of the transmitted radio wave. We also know that the gain G of a properly designed antenna with $D > \lambda$ is given by

$$G \equiv \frac{4\pi\sigma}{\lambda^2} = \left(\frac{\pi D}{\lambda}\right)^2 = \left(\frac{\pi 0.6R}{r}\right)^2 \tag{2}$$

Thus the antenna gain is fixed entirely by the size of the earth and the distance to the satellite. In the present case it is 158. Since the ratio of λ to D is fixed, choosing the wavelength then fixes the physical size of the antenna.

The remaining choice concerns the receiving antenna. In order that there be no need to "point" the antenna to track the satellite, an antenna array that would receive uniformly from all directions is preferred. Such an antenna has unity gain. Whatever

the antenna configuration used to obtain this isotropic coverage, the absorption cross section σ (the "effective area") given by equation 2 for $G = 1$ is:

$$\sigma = \frac{\lambda^2}{4\pi} \tag{3}$$

The absorption cross section times the incident power flux represents the amount of power available to a matched receiver connected to the antenna.[19]

Approximating the distance between the missile and satellite as R,

$$\frac{P_r}{P_n} = \frac{P_0 G \sigma}{4\pi R^2 k T \Delta\nu} \tag{4}$$

where P_0 is the transponder power. We will assume $P_r/P_n = 100$ to allow for antenna drive efficiency and other unanticipated losses.

To be conservative, we choose a noise temperature of 300 K (27° C) although receivers with noise temperatures four times smaller are available off the shelf. We also choose a wavelength $\lambda = 10$ centimeters, which is quite common, having been the radar wavelength employed in World War II. The bandwidth $\Delta\nu$ is determined by the number of bits in the destruct message, the number of *different* destruct messages, the number of times the message is transmitted to minimize reception errors, the open time between messages, and the time interval over which the destruct message is transmitted. We assume broadcast of 50 distinct DALcodes, each of 32 bits, with six repeats of each message, allowing a factor of 10 for open time and ten minutes for the destruct interval after the abort decision is made. This yields $\Delta\nu = 50 \times 32 \times 6/[(10 \text{ minutes}/10) \times 60 \text{ seconds}] = 160 \text{ s}^{-1}$, and $P_n = 6.6 \cdot 10^{-19}$ watts. We then obtain from equation 4 a power requirement of 12 watts.

We conclude that the power requirement offers no impediment to deployment of practical transponders.

Appendix 2

DALCODES AND DALKEYS

Consider a DAL codeword that is simply a string of 1s and 0s. Each position in the string is called a bit. A way to check that two codewords are the same is to compare their bits using the simple rule: if both bits at the same position in the string (or word) are the same (either two 0s or two 1s), assign a 1 in that bit position. If the bits are different (a 0,1 or 1,0 pairing), assign a 0 in that bit position. (The name for this operation is "exclusive or" or "XOR" because 0 is assigned to the result of the operation if and only if one operand or the other, but not both, is 0.)

If the inserted codeword matches the DALcode the XOR result will be a string of 1s with no 0s and the DAL system will be activated. Any pair of bits giving a 0 indicates a mismatch. The following example shows the arithmetic for a 6-bit word:

DALcode	0 1 1 0 1 0
DALcode	0 1 1 0 1 0
XOR	1 1 1 1 1 1

Another use of the XOR occurs in sending a codeword over an insecure line using what is known as a "one time pad"—another random number—here called the DALkey. This resides in the DAL control center with an exact copy residing at the missile field. If a DALcode and the DALkey are combined using the "exclusive or" arithmetic defined above, a new codeword will be generated. That new codeword can be safely transmitted over insecure lines to the center, since, without having the key, the new word cannot be used by anyone to extract the DALcode. To anyone else it is just another random number. However, it can be combined again with the DALkey residing at the center by the same XOR operation to extract the original DALcode.

An example of the arithmetic used is shown below:

DALcode	0 1 1 0 1 0	a random number
DALkey	1 1 0 1 1 0	a random number
XOR	0 1 0 0 1 1	sent via insecure line

Here is the decoding:

XOR	0 1 0 0 1 1	this number received at destination
DALkey	1 1 0 1 1 0	same as used to encrypt the DALcode
new XOR	0 1 1 0 1 0	same as original DALcode

In other words, XORing a DALkey on a DALcode *twice* will always recover the original DALcode.

NOTES AND REFERENCES

1. The history and technology of PALs is treated in Peter Stein and Peter Feaver, *Assuring Control of Nuclear Weapons*, (Boston: University Press of America, 1987).

2. Shortly after the 1985 explosion aboard the space shuttle *Challenger*, a range safety officer remotely destroyed the shuttle boosters. In the test of the third Trident II missile a range safety officer was within seconds of destroying it in flight.

3. *Agreement on Measures to Reduce the Risk of Outbreak of Nuclear War between the United States of America and the Union of Soviet Socialist Republics*, 30 September 1971.

4. The method of notification was to be the USA-USSR Direct Communication Link—the hot line—which was upgraded in an agreement that went into effect at the same time.

5. Gerard C. Smith, *Doubletalk*, (New York: Doubleday, 1980) p.297.

6. *Arms Control and Disarmament Agreements, Texts and Histories of Negotiations*, (Washington DC: ACDA, 1980).

7. Sam Nunn, *Arms Control Today*, March 1988, p.6; Henry Kissinger, *White House Years*, (Boston, Massachusetts: Little, Brown, 1981); Barry Blechman, "Efforts to Reduce the Risk of Accidental War", in Alexander L. George, Philip J. Farley, and Alexander Dallin, eds., *US–Soviet Nuclear Cooperation*, (New York: Oxford University Press, 1988) pp.472–473; Raymond L. Garthoff, "The Accidents Measures Agreement", in John Borawski, ed., *Avoiding War in the Nuclear Age* (Boulder, Colorado: Westview Press, 1986), pp.56–71.

8. For example, William Colby, Harold Brown, Robert S. McNamara, and McGeorge Bundy.

9. See R.L. Garwin, "Launch Under Attack to Redress Minuteman Vulnerability," *International Security*, 4, 3, (1979).

10. Information on Soviet launches is believed to reach the National Military Command Centers (NMCCs) in less than a minute after launch.

11. Such satellites could also contain the infrared detectors used for boost phase launch detection.

12. See the detailed calculation in Appendix 1.

13. For example, a satellite in orbit 2,000 kilometers from the earth's surface would require 1/25th the power.

14. See Whitfield Diffie and Martin E. Hellman, *Proc. of IEEE*, **67**, 3 (1979), for a simple treatment of encryption techniques.

15. This is called a "one time pad" and is described in appendix 2.

16. Private communication, February 1989.

17. The relationship between DALs and launch-on-warning are also discussed by R. L. Garwin, op.cit.

18. See for example, McGeorge Bundy, *Danger and Survival*, (New York: Random House, 1988).

19. See, for example, S. Siller, ed., *Microwave Antenna Theory & Design*, Radiation Lab Series (New York: McGraw-Hill, 1949).