© Journal of Peace Research, vol. 28, no. 2, 1991, pp. 135–159

Improving Communications Links Between Moscow and Washington*

DESMOND BALL
Strategic and Defence Studies Centre, Australian National University

The Direct Communications Link (DCL) between Moscow and Washington, established in 1963 and commonly known as the 'hot-line', is supposed to provide a continuous communications link between US and Soviet National Command Authorities in both crises and war. This article describes the principal rationales for the DCL (crisis management, escalation control and war termination) and the facilities and systems which presently constitute the link. It argues that the present system has significant deficiencies in terms of survivability and endurance which make it unable to satisfy the requirements for escalation control and war termination, and it outlines possible measures for rectifying these deficiencies. These include a dedicated geostationary satellite communications system, with two satellites, both fixed and mobile satellite ground control stations, and optical fibre cable links for the ground connections, and with an adaptive high frequency (HF) radio circuit as a backup. The recent political developments in the Soviet Union and in the US–Soviet strategic relationship have dramatically reduced the likelihood of strategic confrontation. However, this is not a reason for inaction. Both the US and the Soviet Union intend to retain thousands of nuclear weapons, at least in the foreseeable future, and crises and confrontations between them cannot be ruled out altogether. Rather, these changed political circumstances provide an opportunity for cooperative efforts to dramatically improve the communications links between Moscow and Washington.

1. *Introduction*

The maintenance of a continuous communications link between the respective US and Soviet national command authorities would be essential in both crises and war. Continued communications would enable the clarification of confusing events, and provide a channel for negotiations and the control of escalation, including the negotiation of war termination.

This article describes the strategic rationales for the maintenance of direct communications links between Moscow and Washington. These are essentially threefold: crisis management, escalation control and war termination. It next describes the current facilities and systems for communicating between Moscow and Washington, including their deficiencies, and assesses these links with respect to the strategic rationales. Finally, it suggests possible measures for improving the current links in terms of survivability, reliability, security and data transmission capabilities, and provides a critique of current US and Soviet strategic nuclear policies insofar as they relate to improvement of the communications links between Moscow and Washington.

2. *History and Purpose*

The possible consequences of the lack of a direct communications link (DCL) between Moscow and Washington became apparent during the Cuban missile crisis of October 1962, when President Kennedy and Chairman Krushchev were forced to communicate with each other through clumsy diplomatic channels, with messages sometimes being delayed many hours and often being overtaken by the rapid movement of events. As a result, agreement was reached to establish a so-called 'hot-line', which went into service on 30 August 1963.

The Washington terminal of the hot-line (designated MOLINK, a contraction of 'Moscow link') is in the National Military Command Centre (NMCC) in the Pentagon, from which there is a connection to the White House; the Moscow terminals are evidently in the government offices in the

* This article is a slightly revised version of a report prepared first for the Center for Strategic and International Studies (CSIS), Washington, DC, project on 'Improving Superpower Communications'.

Kremlin and in the Chairman's Office in the Communist Party headquarters building across Red Square from the Kremlin (Hudson, 1973, pp. 14, 18, 20, 24, 26, 29; Stone, 1988, p. 60). The hot-line originally had two main routings: the primary one – based on underwater and terrestrial cables running through London, Copenhagen, Stockholm and Helsinki – and a radio backup circuit via Tangier, Morocco. Both were duplex teletype circuits (Whitman & William, 1974, p. 52).

The value of the DCL was first demonstrated during the June 1967 war in the Middle East. On the morning of 5 June, at the very outset of the war, Premier Kosygin contacted President Johnson and expressed his strong interest in both the Soviet Union and the United States using their influence 'to bring hostilities to an end'. On 8 June, when Israel attacked the USS *Liberty*, President Johnson used the hot-line to inform Kosygin that the USA was aware that Israel was responsible and that US aircraft were scrambling from carriers in the area only to aid the stricken ship. And on 10 June President Johnson used the link to tell Premier Kosygin that the USA had received assurances that the Israeli counter-attack against Syria would stop short of Damascus – and hence that any Soviet intervention would be unwarranted. Without a hot-line, a direct US–Soviet confrontation would clearly have been a possibility (Johnson, 1971, pp. 287–303). The line was next used on 12 December 1971, during the Indo-Pakistani War, when the USA informed Moscow that unless pressure was put on India to accept a standstill ceasefire and immediate negotiations, the USA would proceed unilaterally, which might produce 'consequences neither of us want' (Kissinger, 1979, p. 909). It was also used by President Brezhnev in response to the US nuclear alert of 24–26 October 1973, during the Yom-Kippur War, which President Nixon has described as 'perhaps the most serious threat to US–Soviet relations since the Cuban missile crisis eleven years before' (Nixon, 1978, p. 938).

The cable and radio links that constituted the hot-line from 1963 to 1978 were quite vulnerable to accidental interruption as well as to possible sabotage or direct attack. Six separate accidental interruptions have been publicly reported for the period 1964–66 alone. In 1964, a thief snipped out a 20-foot section of the cable near Helsinki; later the same year a thunderstorm reportedly put the line out of commission by damaging a power station in southern Finland; in 1965 a fire in a manhole at Rosedale, Maryland, cut the circuit, also in 1965, a farmer in Finland ploughed through the cable; in 1966 a Finnish postal workers' strike interrupted the circuit for several hours; and a few months later a Soviet freighter severed the cable when it ran aground in Denmark (Hudson, 1973, p. 20). Although in none of these cases was the hot-line actually out of operation for more than a few seconds (since the radio backup was always available) they did prompt efforts to establish a more secure and reliable system.

On 30 September 1971 the USA and the USSR agreed to improve the hot-line by replacing the cable and radio teleprinter links with a satellite communication system comprising two independent and parallel circuits and four ground stations. This system became operational in January 1978. The United States provides one circuit via an *Intelsat* satellite, with ground stations at Etam in West Virginia and Moscow; the Soviet Union provides the other circuit through a *Gorizont* satellite, with ground stations at Vladimir and Fort Detrick, Maryland. Telephone cables and terrestrial microwave links from the ground stations complete the Washington–Moscow connection (Whitman & Davison, 1974, pp. 52–53).

The satellite link is probably more secure and reliable than cable from the point of view of accidental interruption, but it is probably also more vulnerable to disruption in the event of any nuclear exchange – the very situation in which it would be most desperately needed. As Secretary Rumsfeld testified in January 1977, 'the system is not designed to survive a direct attack' (Rumsfeld, 1977, p. 146). The ground stations are particularly vulnerable. Both the satellites operate at somewhat higher frequencies than the UHF band, so that the communication links between them and the ground stations would be relatively unaffected by any black-out induced by nuclear detonations. Hence, as Assistant Secretary of Defense for Command, Control, Communications and Intelligence, Gerald P. Dinneen testified in 1979, 'We may still have a propagation path after a massive attack' (US Congress, 1979, p. 105).

There would be little strategic rationale for any direct attack against the four ground stations. However, these stations and the associated ground links and terminals are naturally quite soft and could well be incidental casualties of strikes against nearby targets. As Dr Dinneen also testified in 1979:

> The ground terminals, of course, are here in Washington, so most likely they are not going to be there. Unless we have some way of getting into that hot-line from the Airborne Command Post, then you would have to assume that after the first impact on Washington that hotline is not available (US Congress, 1979, p. 105).

The irony is that the DCL is only likely to remain operational during the period in a nuclear exchange when restraint is already being exercised for other reasons: once restraint is abandoned, and an exchange progresses to any large-scale level, the availability of the hot-line could not be relied upon. Yet it is from this point on that casualties are likely to be several times greater than for the phase when the DCL was available.

3. *Strategic Rationales for the DCL*

The DCL provides a direct communications link between the governments of the United States and the Soviet Union for use in times of emergency. It is accepted that the emergency situations in which the DCL might be utilized should include those where nuclear accidents, ambiguous incidents, or unauthorized actions might lead to the outbreak of nuclear war. The communications link should be used for the clarification of confusing events in crises, and for negotiations during conflict between the USA and the USSR, particularly with respect to escalation control and war termination. The temptation to use the hot-line for communication between Moscow and Washington in other situations has generally and quite properly been resisted – with two reported exceptions: first, in December 1968, when President Johnson reportedly used the hot-line to send Moscow progress reports on the Apollo 8 mission that circumnavigated the moon (Hudson, 1973, p. 24); and, second, during the SALT II negotiations, when President Jimmy Carter and his national security advisor, Zbigniew Brzezinski, became concerned that General Secretary Brezhnev was not responding to personal letters from the President (Stone, 1988, p. 60).

There have in fact been some criticisms to the effect that the DCL should perhaps be used more often. For example, when a Titan II ICBM exploded at Damascus at Little Rock Air Force Base in Arkansas in September 1980, some officials were concerned that Soviet infrared early-warning satellites might have reported a missile launch and that the hot-line should have been used 'to tell the Kremlin what really happened' (USN&WR, 1980, p. 22). On the other hand, incidents such as this – and the shooting down of KAL 007 on 1 September 1983, and the aberrant Soviet submarine-launched cruise missile (SLCM) which on 28 December 1984 overflew Norwegian airspace before crashing in Finland (Evans, 1985, p. 1) – should more appropriately be addressed through communications at the military-to-military level. This is now possible at a theater level with the joint military communications links established in December 1989 in accordance with the Agreement on the Prevention of Dangerous Military Activities signed on 12 June 1989 (Carnahan, 1989, pp. 13–17, p. 6; CN, 1989, p. 6).

There are three principal strategic rationales for the DCL.

3.1 *Crisis Management*

The need for an assured and reliable direct communications link between the heads of the US and Soviet governments first emerged in the context of efforts to reduce the danger that accident or miscalculation during a crisis might trigger a nuclear war. As formally proposed by the USA on 12 December 1962, following the Cuban missile crisis, for example:

> In the view of the United States, such a link should, as a general matter, be reserved for emergency use; that is to say, for example, that it might be reserved for communications concerning a military crisis which might appear directly to threaten the security of either of the states involved and where such developments were taking place at a rate which appeared to preclude the use of normal consultative procedures (US ACDA, 1982, p. 29).

As is evident from Annex 1, almost all the uses of the hot-line to date have been to clarify events and to impress the other government of the gravity of avowed declarations in crisis situations. For this purpose, the hot-line has proved admirably successful. As Secretary of Defense Caspar Weinberger reported to Congress in April 1983, the DCL 'has proved invaluable in major crises' (Weinberger, 1983, p. S4364).

In June 1967, during the war in the Middle East, the hot-line was important in conveying reassurances which tempered both Soviet and US concerns. President Johnson believed that conflict in the Middle East was 'potentially far more dangerous than the war in Southeast Asia' (Johnson, 1971, p. 287). As mentioned above, the hot-line was used on 8 June 1967, following the Israeli attack on the USS *Liberty*, precisely to inform Premier Kosygin of the nature and purpose of US actions in order to prevent misunderstanding: As President Johnson has recorded:

> There was a possibility that the incident might lead to even greater misfortune, and it was precisely to avoid further confusion and tragedy that I sent a message to Chairman [sic] Kosygin on the hot line. I told him exactly what had happened and advised him that carrier aircraft were on their way to the scene to investigate. I wanted him to know, I said, that investigation was the sole purpose of these flights, and I hoped he would inform the proper parties. Kosygin replied that our message had been received and the information had been relayed immediately to the Egyptians.
>
> Ambassador Llewellyn Thompson reported [later] that this particular exchange had made a deep impression on the Russians. *Use of the hot line for this purpose, to prevent misunderstanding, was exactly what both parties had envisioned* (Johnson, 1971, p. 301). [Emphasis added].

On 10 June 1967, use of the hot-line was critical in removing the possibility of a direct confrontation between the USA and the Soviet Union in the Middle East. With the Israelis having counter-attacked into Syria and rumours that they would proceed to attack Damascus, Premier Kosygin activated the hot-line to inform President Johnson that 'a very crucial moment had arrived'. Kosygin spoke of the possibility of 'independent decision' by Moscow. He foresaw the risk of a 'grave catastrophe' and stated that unless Israel unconditionally halted operations within the next few hours, the Soviet Union would take 'necessary actions, including military'. Johnson's reaction was to order US carriers to move closer to Syria and to tell Kosygin over the hot-line that 'we had been pressing Israel to make the cease-fire completely effective and had received assurances that this would be done' (Johnson, 1971, pp. 302–303). At about this time, the Israelis did stop short of Damascus, and the tension in the Johnson–Kosygin messages over the hot-line began to subside. It is quite conceivable that without the reassurance Kosygin received over the hot-line, the Soviet Union might have intervened to prevent what it thought meant the fall of Damascus. Soviet intervention could well have led to direct US–Soviet conflict. Kosygin later told Johnson that through the use of the hot-line they had 'accomplished more on that one day than others could accomplish in three years' (Johnson, 1971, p. 484).

Similarly, in subsequent crises – from the Indian-Pakistan war in 1971, through the Yom Kippur war in the Middle East in 1973, the Turkish invasion of Cyprus in 1974, and the Soviet invasion of Afghanistan in 1979, to the crisis in Poland in 1981 – the hot-line has been used for communication between Washington and Moscow.

For more than a quarter of a century, the hot-line has functioned as a successful and important instrument of crisis management.

3.2 *Escalation Control*

In the early 1970s, US strategic nuclear planners developed the concept of *escalation control* (Ball, 1986a, pp. 70–75). A wide range of limited nuclear options (LNOs) were incorporated into the Single Integrated Operational Plan (SIOP) to enable the US National Command Authorities (NCA) to employ strategic nuclear forces in very limited and selective operations. Plans were developed to provide the NCA with the potential to 'hold some vital enemy targets hostage to subsequent destruction' and to control 'the timing and pace of attack execution, in order to provide the enemy opportunities to consider his actions' (Nixon, 1974, p. 73). Improvements in strategic command, control, communications and intelligence (C^3I) systems were sought to enable the US strategic nuclear forces to be employed in a deliberate, controlled and informed fashion throughout the progress of a strategic nuclear exchange.

It was recognized at the outset of this effort that control of a strategic nuclear exchange between the USA and the Soviet Union would be rather easier if a continuous communications link could be maintained between the respective NCAs. As Secretary Schlesinger testified on 4 March 1974 in support of the doctrine of limited nuclear war-fighting:

> If we were to maintain continued communications with the Soviet leaders during the war, and if we were to describe precisely and meticulously the limited nature of our actions, including the desire to avoid attacking their urban industrial base, . . . political leaders or both sides will be under powerful pressure to continue to be sensible (US Congress, 1974, p. 13).

The hot-line was thus subjoined with the demands of limited nuclear war-fighting and escalation control.

3.3 *War Termination*

The hot-line is the principal system which has been officially identified with facilitating war termination in the event of a strategic nuclear exchange between the USA and the Soviet Union (Brown, 1980, p. 140). However, despite the system's critical importance for war termination, no special measures have been taken to protect it from the collateral effects of a nuclear exchange.

Hence, as Robert Leahy has recently argued:

> The hot line is not likely to be useful for war termination communications for the same reason that it is useful for crises resolution communications: one end is in Washington, and the other presumably is in Moscow. The hot line's ground entry points, like its user terminals, are collocated with high value military assets near Washington, DC, and Moscow. The wartime destruction of both cities, together with the hot line terminals and ground entry points, is nearly certain. None of the survivable US command centers has an independent hot line capability. There is no indication that the Soviets have installed a hot line terminal in any of their survivable command centers. So, the destruction of either Washington or Moscow will preclude use of the hot line.
>
> Even if Moscow and Washington were to survive a general nuclear exchange, the hot line probably would not be available for war termination communications. It uses communications satellites (Molniya or Statsionar [i.e. Gorizont] and Intelsat), which are unlikely to withstand the nuclear environment and may not be excluded by both sides from antisatellite attacks. And, neither system is dedicated to hot line use, so either or both may carry military related traffic. This could cause either side to target them.
>
> The hot line is the only direct, government-to-government communications link between the National Command Authorities of the United States and the Soviet Union. It is not a survivable link and will not be available for general nuclear war termination communications (Leahy, 1988, pp. 42, 44).

3.4 *The Direct Communications Link (DCL)*

The present DCL is essentially that which was agreed by the USA and the USSR in September 1971 and which became operational in January 1978, with three significant modifications: first, the Soviet communications satellite (COMSAT) component, which initially consisted of transponders on particular Molniya II and III highly elliptically orbiting satellites, now consists of a Gorizont geostationary COMSAT stationed at 14°W longitude (Johnson, 1987, p. 24); second, the US satellite ground station at Fort Detrick in Maryland has recently been modernized (WP, 1990, p. B-3); and, third, as agreed on 17 July 1984, a facsimile transmission capability has been added to the system to enable the parties not only 'to exchange messages faster' but also 'to send graphic material such as maps or pictures which would play a crucial role in helping to resolve certain types of crises or misunderstandings' (*Signal*, 1984, p. 110; US ACDA, 1986, p. 523).

The current architecture of the DCL is as follows:

1. Two independent satellite communications circuits between Washington and Moscow, with each circuit using a completely separate satellite system. These circuits are capable of simultaneously transmitting and receiving 4800 bits per second. The US contribution to the satellite link is provided by an Intelsat COMSAT stationed at 24.5°W longitude. The Soviet contribution is currently provided by Gorizont 15 (1988–28A), launched on 31 March 1988 and stationed at 14°W.
2. Four satellite ground stations, one each in the USA and the USSR for the Intelsat circuit and one each for the Gorizont circuit. The Intelsat ground stations are at Etam in West Virginia, some 225 km west of Washington, DC; and in Moscow. (There is also an Intelsat ground station at Dubna, some 110 km north of Moscow, which also accesses the Intelsat satellite at 24.5°W.) The Gorizont ground stations are at Vladimir, some 180 km northeast of Moscow; and at Fort Detrick in Maryland, some 68 km northwest of Washington, DC.
3. Cable and terrestrial microwave links from the satellite ground stations to the DCL terminals. In the US case, there are cable and microwave links from Etam and Fort Detrick to the National Military Command Center (NMCC) in the Pentagon, and thence to the Situation Room in the White House basement. In the Soviet case, there are cable and microwave links from the Vladimir and Moscow satellite ground stations to the Soviet Defence Ministry at 19 Frunze Embankment and thence to the Kremlin and CPSU headquarters.
4. A third circuit is provided by the original cable telegraph link established in 1963, which remains as a backup link. (The radio circuit via Tangier was taken out of service in 1978 when the satellite circuits became operational. Cf. Riberia, 1985, pp. 95–96.)
5. The terminals in Moscow and Washington, which are equipped with teletype and facsimile machines, information security devices (which 'consist of microprocessors that . . . combine the digital facsimile output with buffered random data read from standard 5¼ inch floppy disks'), cathode ray tube displays, and printers (US ACDA, 1984, pp. 520–522).

3.5 *Vulnerabilities and Deficiencies of the DCL*

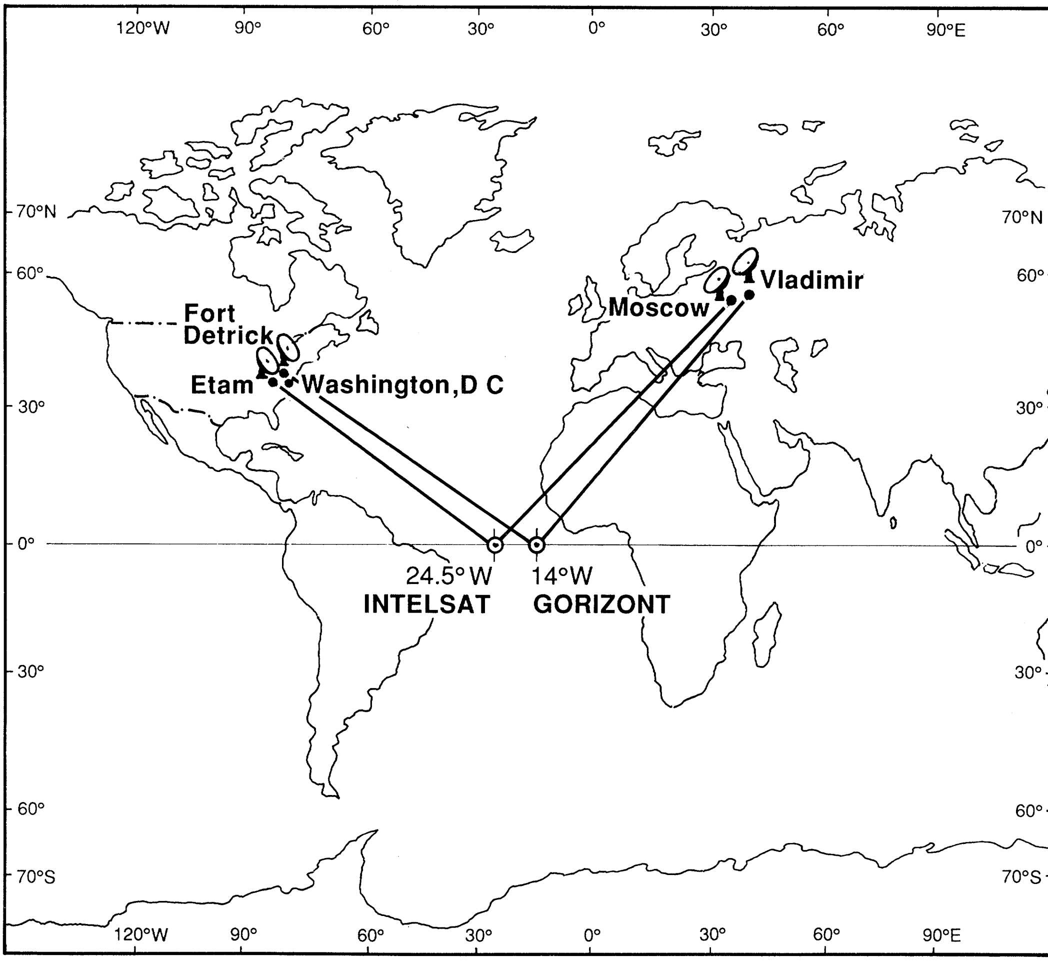
The Intelsat and Gorizont COMSATs provide an extremely reliable communications link between Moscow and Washington in peacetime circumstances. As Secretary Weinberger reported to Congress in April 1983:

> In 1971, the two governments agreed to establish two satellite communication circuits for the DCL, with a system of multiple terminals in each country. When those became operational in 1978, the DCL achieved *almost 100 percent technical reliability* (Weinberger, 1983, p. S4364) [Emphasis added].

However, the Intelsat and Gorizont satellites are quite deficient with respect to the security of their transmissions. These can be intercepted fairly easily by interested third parties – either other governments or large media organizations. Access to the DCL communications provides the potential for emerging agreement to be subverted through disruptive action or other mischief. The disclosures and commentaries of the media on the use of the DCL would not be conducive to careful crisis management or frank and considered intra-war communications.

Both the Intelsat and Gorizont satellites have 'spot' or 'zone' beam capabilities as well as hemispheric and global beam capabilities. The global beams provide footprints which cover more than 40% of the Earth's surface, while the hemispheric beams cover some 20%. The footprints of the spot beams are also quite large – covering more than a million square kilometres of the Earth's surface.[1]

Fig. 1. Present DCL Satellite Communications Circuits



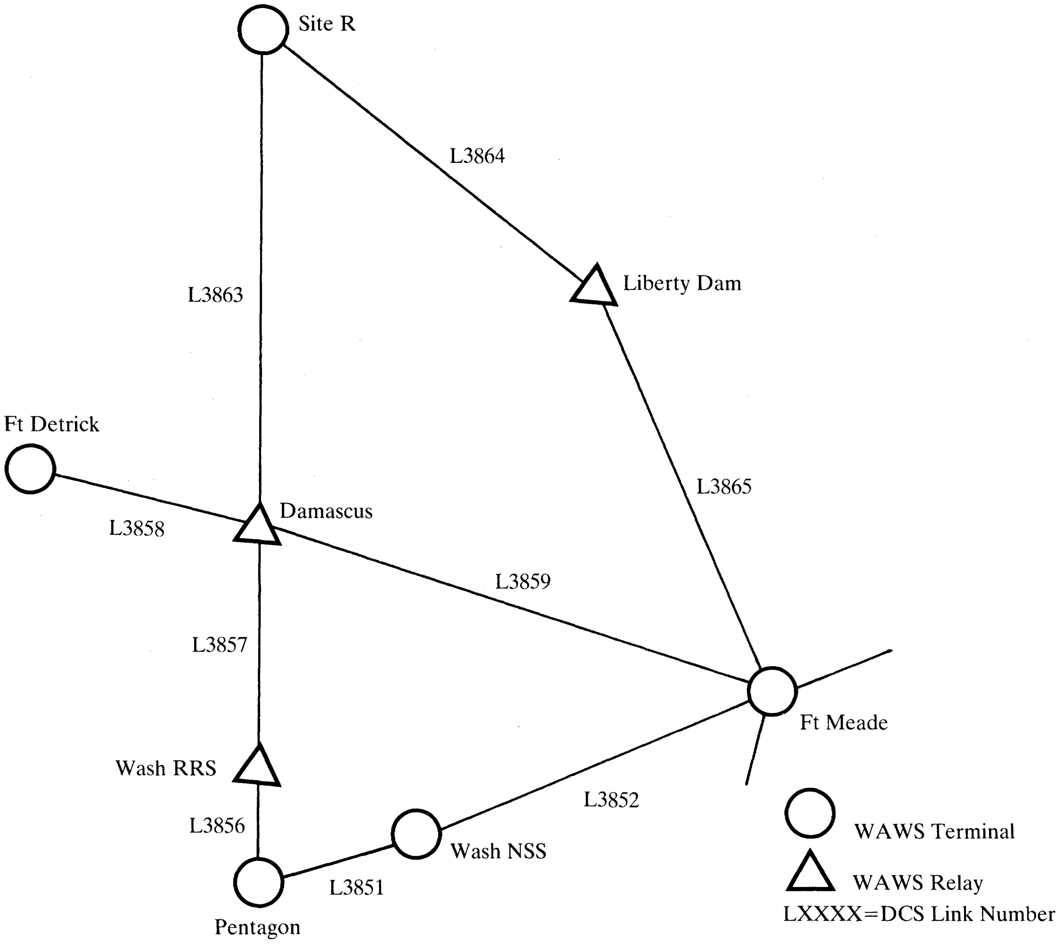
These COMSAT transmissions are very vulnerable to interception. According to a study by the MITRE Corporation, Intelsat or other comparable ground stations operated by other interested parties could easily be used to intercept COMSAT traffic of interest:

> An INTELSAT earth station in one country could be employed to receive and demodulate r-f [radio frequency] carriers intended for INTELSAT subscribers of other countries. This capability is available since the low-noise parametric amplifiers employed for most subscriber earth stations are nearly always broad-band (500 MHz) and therefore are capable of receiving the entire frequency band allocated to space communications. Following amplification by the parametric amplifiers, the r-f carriers can be separated by filtering and the signals targeted for interception passed to a conventional microwave receiver for demodulation. Since the frequency assignments of subscribers are changed only infrequently, a crystal-controlled, fixed frequency microwave receiver would appear acceptable . . . A selective level meter is employed to select and demodulate the single FDM telephone channel of interest (Sanders et al., 1977, pp. 90–93).

Moreover, the intercept equipment is also relatively easy to conceal:

> The intercept equipment (including the antenna) could . . . be 'hidden' by adding the intercept receiving equipment to legitimate antenna installations such as a subscriber-owned earth station for use with domestic satellites, a radio astronomy station or manufacturing plants which build and test radar

Fig. 2. Washington Area Wideband System (WAWS) Fort Detrick–Pentagon



Radio system/maintenance is leased Western Union Microwave. Transition Interface Point (TIP) is digital coax patch between GFE KG81 (bulk encryption) and each 12.928 MBS DMX-A3 digital MUX channel (TDM). Radio is Collins MDR-6 SD.

Source: DCA, 1985, p. 7.

and/or radio antennas. INTELSAT earth station equipment in one country could also be used to intercept traffic between two other countries (Sanders et al., 1977, p. 17).

Monitoring the transmissions is a very different exercise from reading the messages themselves. As noted above, the agreement of 17 July 1984 to expand the DCL included provisions for information security devices to encode the signals (US ACDA, 1984, p. 521). However, it would be dangerous to be complacent about the security of the link. The encoding devices and algorithms are not the most sophisticated available. Moreover, it could be possible for interested third parties to discern much about the communications even without decoding the signals.

4. *The DCL in a War Environment*

The DCL is not designed to survive or function in a war environment. Its principal component subsystems are essentially unprotected against blast or other nuclear effects or electronic countermeasures (such as jamming). There would be no strategic rationale for attacks against the DCL as such by either the USA or the USSR – if either wished for some unimaginable reason to render the link inoperable it need only disconnect the teletype and facsimile machines or simply refuse to respond to the other's communications. However, some of the principal component subsystems are located with or near some high-value targets. Other subsystems are also used for C^3I missions which are important to the successful conduct of strategic nuclear strikes. And there may be third parties involved in the conflict which might wish to interfere with these subsystems, either to prevent their use for other strategic purposes or even to frustrate intra-war negotiations between Moscow and Washington.

Moscow and Washington themselves are likely to be attacked at some point in a nuclear exchange. Both cities contain numerous governmental and economic targets. In the case of Soviet target planning, strategic C^3I facilities (such as the Pentagon and the White House) rank in the primary category of targets, and in accordance with Soviet strategic nuclear policy and doctrine would likely be attacked at the very outset of a strategic nuclear exchange (Ball, 1986b, ch. 3). In the case of US strategic nuclear target planning, numerous warheads have been allocated to targets within the Moscow city limits (Ball, 1981, p. 30). Although US target plans from the early 1960s through to the late 1970s defined Moscow as a 'withhold', to be exempted from attack in the initial stages of any nuclear exchange,[2] the most recent version of the SIOP includes an option for a 'decapitation' strike against Moscow at the outset of an exchange (Ball & Toth, 1990, pp. 65–92).

In any event, it should be assumed for planning purposes that both Moscow and Washington will be attacked at some point in any large-scale strategic nuclear exchange – and that the DCL terminals in these cities will be destroyed. The statement by Dr Dinneen in March 1979, cited in Section 2 above, indicates that US authorities assume that the hot-line would not be available after the first impact on Washington. Yet the objectives of and circumstances attending attacks on the national capitals would be among the most important subjects for direct discussion and clarification during any nuclear exchange.

It is possible that the NCAs would have evacuated the national capitals before they are attacked. In the USA the NCA has available a variety of alternative command posts and relocation centres, including the E-4B National Emergency Airborne Command Post (NEACP), the underground Alternate National Military Command Center (ANMCC) at Fort Richie in Maryland (about 75 miles from Washington), several other underground command posts in the Washington area, and at least two mobile command posts based near Washington. In the events that Washington is destroyed and/or the NCA has evacuated the city, it would be important that hot-line terminals were available in these various alternate command posts. As Dr Dinneen testified, it is critical to the continuing operation of the hot-line that there be a connection to the NEACP (US Congress, 1979, p. 105) – which serves not only as a potential route of evacuation and an emergency alternate command post for the NCA, but also as an alternate emergency national strategic communications link for the NCA should it decide to remain on or under the ground in the Washington area. However, no means of connecting the NEACP into the DCL have yet been developed. Indeed, according to one report, 'none of the survivable US command centers has an independent hot line capability' (Leahy, 1985, pp. 165–167).[3]

The Soviet NCA has established a much more extensive array of alternate command centres – including airborne systems, numerous deep underground relocation centres (such as the alternate national command centre at Sharapovo, some 50 miles south of Moscow), trains and other vehicles (Department of Defense, 1988, pp. 17, 59–62). Again, however, notwithstanding the acceptance that Moscow would be attacked and the evident plans for relocation of the leadership, 'there is no indication that the

Soviets have installed a hot line terminal in any of their survivable command centers' (Leahy, 1985, p. 42).

The satellite ground stations at Fort Detrick, Etam, Moscow and Vladimir are neither hardened nor in any other way protected against nuclear attack. The dish antennas are extremely vulnerable. They could probably resist no more than about 5 psi blast overpressure and, indeed, perhaps only 1 or 2 psi of dynamic overpressure – meaning that they could be destroyed by a 1-megaton weapon detonating as far as 10 miles away. These stations are all either collocated with important targets or are themselves associated with other C^3I missions which could cause them to be targeted. The Moscow Intelsat ground station is located within the city limits. Vladimir is also an important ground control station for other Soviet communication satellites – including the Gorizont 10 and 16 geostationary COMSATs stationed at 80°E and the Molniya highly elliptically orbiting COMSATs, which are used extensively by the Soviets for government and military communications.

The US Army's East Coast Telecommunications Center (ECTC) at Fort Detrick is one of the largest communications facilities in the USA. In addition to hosting the DCL Gorizont ground station, it also serves as the 'primary hub for satellite communications support to Washington' (Arkin & Fieldhouse, 1985, p. 192). It is a Net Control Facility (NCF) for the Defense Satellite Communications System (DSCS), controlling DSCS satellites stationed over the Atlantic Ocean and providing direct connections with such other important DSCS stations as Rosman and Northwest in Virginia, Shemya and Elmendorf in Alaska, Oakhanger in England, Landstuhl in [West] Germany, Diyarbakir in Turkey and Howard Air Force Base in the Panama Canal Zone. It is also an AUTODIN switching centre, providing teletype connections with other AUTODIN centres such as Coltano in Italy, Pirmasens in [West] Germany and Croughton in England (DCA, 1985). Fort Detrick must rank among the top 50 US C^3I targets in Soviet strategic nuclear war plans.

The ground station at Etam could well be targeted because of the communications support which the Intelsat system provides for a range of important defence and intelligence programs. Intelsat circuits are used by the Department of Defense for operational communications as well as administrative and logistic communications.

Until 1983, for example, the critical US missile early warning system was dependent upon commercial COMSAT links, including Intelsat circuits, for communications between the major early warning stations – such as the Ballistic Missile Early Warning System (BMEWs) station at Fylingdales in England, the Pave Paws submarine-launched ballistic missile (SLBM) early warning station at Otis Air National Guard Base in Massachusetts, and the Defense Support Program (DSP) satellite early warning system ground stations at Nurrungar in South Australia and Buckley Aerospace Data Facility outside Denver in Colorado – and the US Air Force Space Command/Peterson Air Force Base and North American Aerospace Defense Command (NORAD) complex at Colorado Springs, Colorado. Since 1983, with the installation of DSCS terminals at Buckley, Peterson and the various missile early warning stations, the use of Intelsat for missile early warning communications has been effectively relegated to a backup service (Ball, 1989, pp. 11–15). However, any Soviet effort to destroy or incapacitate the US missile early warning communications system could not afford to neglect this Intelsat service.

The Intelsat system is also used for intelligence communications. For example, some ocean surveillance information collected by US and Allied high frequency direction finding (HF DF) stations around the world is transmitted back to the US on leased Intelsat circuits (Ball, 1989, p. 15). It could be important to the Soviets to destroy or impair this intelligence communications link in some contingencies.

The Etam Intelsat ground station itself provides leased-circuit connections, via Intelsat satellites stationed over the Atlantic Ocean, with numerous important US over-seas defence bases and facilities, including some in Iceland, Ascension Island, Barbados, Panama, Puerto Rico and Western Europe (DCA, 1985).

The Intelsat and Gorizont satellites are completely vulnerable to nuclear effects, electronic interference and other anti-satellite (ASAT) operations.

Both the United States and the Soviet Union currently possess several means of destroying or incapacitating the other's satellites, although these means remain quite limited in their technical sophistication and operational utility. The Soviet Union maintains a handful of ASAT vehicles at Tyuratam, but these are only able to threaten satellites in low earth orbit (LEO) – i.e. satellites at altitudes of below around 2000 km. However, boosters are available which are capable of lifting ASAT packages to geostationary altitudes. Nuclear weapons could also be detonated in space and disable satellites hundreds of kilometres away. Directed energy weapons such as lasers already have a limited capability against geostationary satellites.

The present DCL host-satellites are not well positioned from the point of view of avoiding the effects of ASAT activities against other more critical geostationary satellites. For example, Gorizont 15 (1988–28A) is stationed immediately adjacent to a DSCS III satellite (DSCS LANT) and a US Navy LEASAT, and only 2° from a proposed MILSTAR station at 16°W. Similarly, the Intelsat satellite at 24.5°W is immediately adjacent to a US Navy FLTSATCOM satellite (Ball, 1989, pp. 65–71).

The Intelsat and Gorizont satellites also lack any protection against either the electromagnetic pulses (EMP) or the transient radiation effects on electronics (TREE) caused by nuclear explosions. In a situation where there are multiple detonations in space, it is possible that unprotected satellites could be disabled by EMP, TREE or other nuclear radiation even if detonations do not take place in the vicinity of the satellites.

Further, the frequencies used for Intelsat and Gorizont transmissions are not optimal for propagation in a nuclear environment. Explosions of nuclear weapons in the atmosphere will increase dramatically the ionization of the upper levels of the atmosphere and ionosphere. The attenuation that a radio wave experiences in traversing these ionized layers depends exponentially on the square of the wave length. Hence, the SHF frequencies employed by these satellites are somewhat less susceptible to blackouts than UHF frequencies, but are more vulnerable than frequencies in the EHF band (Wheelon et al., 1982, p. 4).

Finally, the Intelsat and Gorizont satellites are relatively vulnerable to jamming – whether unintentional or intentional. Assuming that sufficient power is used, a satellite antenna will receive radiation from any source operating in its frequency band emanating in its direction if the source is visible to the satellite's antenna pattern. In the case of the antennas on the Intelsat and Gorizont satellites, the area from which interfering signals can emanate is very large indeed. In a wartime environment, with numerous signal sources (including high-powered jammers) activated, there is a high probability of unintentional interference. As compared to EHF frequencies, the SHF transmissions have larger sidelobes and smaller bandwidths, which also make jamming easier. And the satellites lack any capability for frequency-hopping or steering the transmission beams away from sources of interference.

5. *Other Moscow–Washington Communications Links*

In addition to the DCL for communications between the US and Soviet NCAs, a variety of other communications links have also been installed which can support crisis communications. However, these links do not provide connections which can be utilized by the NCAs for direct communications between them; they generally involve governmental and military authorities who lack responsibility for negotiation or agreement at the levels required; they are designed for purposes other than crisis management and intra-war negotiations; and they use many of the same communications circuits as the DCL itself, and share many of the vulnerabilities and deficiencies of the DCL system. In terms of the strategic rationales of the DCL, these communications links would be of little value in either crisis or strategic nuclear war.

5.1 *The Warm Line: The Nuclear Risk Reduction Centers (NRRCs)*

On 15 September 1987, Soviet Foreign Minister Eduard Shevardnadze and the US Secretary of State George Shultz signed the US–Soviet Agreement on the Establishment of Nuclear Risk Reduction Centers. These Centers, which are located in Moscow and Washington, are intended to reduce 'the risk of outbreak of nuclear war, in particular, as a result of misinterpretation, miscalculation, or accident' (ACT, 1987, pp. 28–29). The Washington NRRC, which was formally opened on 22 March 1988, is located in Room 7518 on the seventh floor of the State Department building. The Moscow NRRC, which was opened on 1 April 1988, is in the Kremlin.

The NRRC system is supposed to serve a variety of purposes. Most generally, it is a confidence-building measure, serving as a transmission channel for information exchanges and notifications of certain military activities. According to Article 1 of Protocol 1 of the Agreement, for example, notification of strategic ballistic missile launches (including launch area and area of impact) should be provided to the NRRCs no less than 24 hours in advance of the planned date. It also serves as an instrument of arms control verification, providing for the exchange of information on missile tests and other activities which might be thought to be in violation of arms control agreements. However, although it is intended to reduce the risk of nuclear war through 'misinterpretation, miscalculation, or accident', it is not designed for crisis management.

Like the DCL terminals, the NRRCs are located in the capital cities and hence are likely to be destroyed in any strategic nuclear exchange. They also use the same Intelsat and Gorizont satellite systems as the DCL, as well as the same local communications links and information security devices. In a war situation, they would function no longer than the DCL itself.

5.2 *Joint Military Communications Links*

On 12 June 1989, the Chairman of the US Joint Chiefs of Staff and the Chief of the Soviet General Staff signed the Agreement on the Prevention of Dangerous Military Activities, which is designed to prevent and resolve peacetime incidents involving US and Soviet armed forces. 'Dangerous military activities' include entering the national territory of the other party unintentionally; using lasers in a manner that 'could cause harm' to the personnel or equipment of the other party; and interfering with command and control networks in a manner that 'could cause harm' to the personnel and equipment of the other party (Carnahan, 1989, pp. 13–17).

Annex 1 to the Agreement contains detailed provisions with respect to communications between the parties' armed forces, including specified radio frequencies, visual signals, and English phrases for use in particular contingencies (Carnahan, 1989, pp. 13–17). In December 1989, tests were conducted of the newly established joint military communications channels (including tests of air-to-ship links in the Mediterranean and air-to-air and air-to-surface links in the Bering Sea) (CN, 1989, p. 6), and the Agreement entered into force on 1 January 1990.

The June 1989 agreement was 'obviously inspired by the success' of the agreement of May 1972 on the Prevention of Incidents at Sea (Carnahan, 1989, p. 13), which has led to a marked reduction in collisions and other incidents at sea as well as in the severity or degree of danger implicit in these incidents (Ball, 1985–86, pp. 7–8). However, the new agreement goes beyond that of 1972 in that it covers all the armed forces of the USA and the USSR (rather than only their naval forces), and in that it applies worldwide and not merely on or over the high seas (Carnahan, 1989, p. 13).

On the other hand, the new agreement falls far short, in terms of both purpose and capabilities, of proposals for a Joint Military Communications Link (JMCL) that have been advanced by Secretary of Defense Weinberger (Weinberger, 1983, pp. S4364–S4365), President Reagan (Nelson & Skelton, 1985, p. 1) and various strategic analysts. As described by Secretary Weinberger, for example, a JMCL would provide a direct facsimile transmission capability between the National Military Command Center (NMCC) in the Pentagon and the Soviet national crisis control centre.

> [The JMCL] would supplement, but not supplant, existing diplomatic channels . . .
>
> It would allow rapid exchange of highly technical information that could be essential to understanding and therefore resolving a nuclear or other military crisis. No existing communication channel between the United States and the USSR has a similar capability.
>
> A JMCL could . . . have a crisis control function. It could be used in the event of any military incident that required urgent communication between the United States and the USSR, but did not warrant direct contact between the two heads of government (Weinberger, 1983, p. S4364).

The design and development of a secure, highly capable and reasonably survivable JMCL is quite feasible. However, its particular features, purposes and capabilities should be addressed in the context of a significantly improved hot-line. The two systems could share some of the technical features (e.g. anti-jamming and nuclear radiation protection features). Their strategic purposes and operations could be closely complementary. In an intra-war situation, for example, it might not always be possible to communicate with all the strategic nuclear forces (e.g. submarines preparing to launch their missiles in the face of enemy ASW activity, or bombers flying at low altitude within enemy air space) in order to countermand orders or to disengage these forces. Direct and rapid communications between the two military commands would be helpful in ensuring that an intra-war pause or armistice was not nullified by such failure.

6. *Improving the DCL*

There are a wide range of improvements which could be made to the DCL. Many of these involve the utilization of current communications systems and technologies under development. One possibility, which received some consideration in the late 1970s, involved the provision of a dedicated hot-line transponder on a DSCS satellite. This would have provided enhanced communications security as well as several other superior operational features, but it would have made for a more lucrative target and the system as a whole would be no more survivable. There was also a security concern – that the Soviets might be able to learn valuable intelligence about US defence communication satellite transmission capabilities and techniques – although this is in practice a trifling concern. One possibility would be to acquire an advanced defence communications satellite with modified transponders to alleviate the security concern. However, these provide far more capability than is necessary for a DCL circuit and are far too expensive. (The MILSTAR satellites, for example, are likely to cost as much as USD 2 billion each.)

It is important that an improved DCL consist of a dedicated system, designed solely and wholly for the DCL mission. Only if it operates completely independently of other communications programs can it claim sanctuary from direct attack in a war situation. Moreover, sharing of facilities would be false economy, since the system would be encumbered with unnecessary and expensive capabilities.

A dedicated DCL system can be designed and deployed which would provide a sufficiently capable, reliable, survivable and reasonably endurable communications link and which would cost around three-quarters of a billion dollars for the complete program (see Table I).

The system would consist of two dedicated geostationary satellites with dedicated mission control facilities, a high frequency (HF) radio network as a backup, and multiple terminals installed at the full range of national command posts in both the USA and the USSR (Gottfried & Blair, 1988, pp. 111, 318–319).

Table I. Summary of Costs of an Improved DCL

Associated Hardware and Operating Systems	USD million
Satellites (2 × USD 200 m)	400
Satellite Launches (2 × USD 60 m)	120
Fixed satellite ground control stations (4 × USD 20–25 m)	90
Mobile satellite ground control stations (4 × USD 10–15 m)	50
Optical fibre cable (4000 km)	30
Multiple EHF terminals (20 × USD 1 m)	20
HF system	40
Total	750

6.1 *The Geostationary Satellites*

Two geostationary satellites, one each produced by the USA and the USSR, would provide essential redundancy. The satellites would utilize the most advanced and sophisticated (but proven) technologies where necessary, but in other respects would be quite simple and unadorned.

The satellites should have a dual frequency capability, operating in both the SHF and EHF bands. EHF transmissions, which have been tested on various US military communications satellites, offer several advantages over lower frequency bands. EHF transmissions are largely unaffected by nuclear blackout phenomena. The transmissions are highly directional, making interception difficult and allowing the use of relatively small ground terminals. The signal can also be spread over a 1-GHz bandwidth, which is too great to permit effective broadband jamming.

On the other hand, EHF transmissions are relatively vulnerable to attenuation due to rain (Flock, 1987; Ippolito et al., 1983) and perhaps even to dust and smoke particles injected into the atmosphere by large-scale multiple detonations during the course of a nuclear exchange.[4] It would therefore be wise to also have an SHF capability, which suffers less attenuation due to precipitation, can propagate almost as well in a nuclear environment, and can be accommodated with various anti-jamming capabilities (such as steerable waveguide antennae).

With respect to nuclear effects, the improved hot-line satellites should have some hardening and other forms of protection against both transient radiation electronic effects (TREE) and EMP (such as fully redundant power subsystems which are able to isolate load faults and to rapidly respond to load changes caused by EMP). However, since the principal threat to the survivability of these satellites would be the incidental effects of attacks directed at other satellites rather than of direct attack, it should not be necessary to acquire a full suite of extremely expensive protective measures against laser, nuclear, kinetic/conventional and electronic threats.

Some protection against damage caused by attacks on nearby satellites would be gained by ensuring that the hot-line satellites are 'parked' as far away as possible from defence and intelligence satellites. The present Gorizont 10°W and Intelsat 24.5°W stations were determined through a process of application by the Soviet Ministry of Communications and Intelsat respectively to the International Telecommunications Union (ITU) in Geneva, which is responsible for the allocation of geostationary 'slots' – a process in which avoidance of signal interference is the primary concern and in which the interests of the 'hot-line' transponders have never been considered. There are no satellites which are likely to be directly attacked either currently operational or proposed between 16°W and 23°W, which suggests 19.5°W as one possible station.

The tracking telemetry and control (TT&C) on the satellites should be very sophisticated. A dual frequency TT&C system would enable the satellites to be controlled and operated in various jamming and nuclear effect environments. While being accessible to two or more dispersed ground control stations, it must have sufficient intelligence, security, and operational autonomy to prevent 'spoofing' by other ground stations. Although a narrow spot beam capability is essential, there should be backup hemispheric and global coverage beams in the event that the TT&C/stationkeeping capability is degraded.

These satellites – quite austere in many respects when compared to the Intelsat VI

COMSATs, yet as advanced and sophisticated as DSCS III or MILSTAR satellites in others – should cost around USD 200 million each (compared to USD 120–150 million for an Intelsat VI satellite). It would be reasonable to expect a design life of 8–12 years. The launch costs would be about USD 60 million per satellite.

6.2 *The Ground Segment*

The ground segment of the improved hot-line satellite communications system would consist of the satellite control stations, multiple terminals located at the primary and alternate national command centres, and the connections between these stations and terminals.

The minimum ground control capability should consist of four stations – one for each satellite in both the USA and the USSR, as with the present Intelsat/Gorizont system. These stations should be located in low risk areas, some distance (e.g. 100 km) from the national capitals and as far as possible from potential military and industrial target areas. In the US, there are numerous suitable expanses in both Virginia and West Virginia (DCPA, 1975, pp. 18–21). Analysis of the US National Strategic Target List (NSTL) would suggest comparable low risk areas in the Moscow area. (Geographic separation of the stations would also increase the probability that EHF transmissions could be received in all weather conditions, since locations could be selected which rarely experience heavy rainfall at the same time.)

Several antenna systems are available which have some blast protection (at least against detonations more than a few kilometres away); which can operate and maintain traffic in an EMP environment;[5] which have a dual frequency and spread-spectrum multiple access (SSMA) capability to provide jam resistance and ensure a continued ability to transmit and receive critical mission traffic through a variety of threat scenarios; and which have redundant equipment in all critical areas and built-in fault isolation capabilities to ensure traffic availability approaching 100%. These terminals can be procured for some USD 20–25 million each.

These fixed ground control stations might be supplemented with backup mobile ground terminals. Several mobile command posts have been developed which have both blast and EMP protection, as well as the requisite operational features, and which cost around USD 10–15 million each (DE, 1985, p. 25; Munro, 1989, pp. 3, 26).

These ground control stations should have secure and survivable connections with a multiplicity of primary and alternate command posts. In the US case, this should include not just the NMCC in the Pentagon and the White House, but also the NEACP, the ANMCC at Fort Richie, and several other underground and mobile alternate command posts within a 200 km radius of Washington, DC. Underground optical fibre links should be used to connect the ground control stations to the fixed national command posts. Low probability of intercept (LPI) radio transmissions, using low power and high directionality, could provide connectivity to the mobile command posts (May & Harvey, 1987, p. 715). A secure SHF/EHF data link for facsimile transmission should be designed for linking the ground control stations to the NEACP. And small 6–8-foot EHF terminals could be installed at each of the underground and mobile alternate command posts, as well as abroad the NEACP, to permit direct reception of hot-line transmissions from the satellites.

6.3 *The High Frequency (HF) Radio System*

The high frequency (HF) radio system proposed as a backup to the satellite system would be very different to the HF radio circuit that operated as part of the DCL from 1963 to 1978.

In a nuclear environment, many HF channels are likely to be blocked, but many others should remain open. The problem in using the HF band to communicate is that the usable channels will not be known in advance. However, several recent developments in HF propagation techniques (known collectively as 'adaptive HF') allow this problem to be avoided while still retaining sufficient bandwidths for high-speed teletype communications. One approach is to use ionospheric sounders and other devices for measuring channel noise and interference content to select and continually change frequencies and other signal parameters in order to maintain optimum communication in spite of ionospheric disturbances and electronic countermeasures. Another approach involves spectrum-wide communication where data are transmitted throughout the entire HF band without any special regard for the limited band in which successful communication occurs, but with the expectation that at least one channel would effectively propagate. Protocols concerning frequency management and propagation information would need to be exchanged between Washington and Moscow (Di Julio, 1980, pp. 16–17; Gottfried & Blair, 1988, p. 111; Higgins, 1981, pp. 56–57; McLaughlin, 1981, pp. 53–56).

Modern HF antennas can be buried or otherwise protected against both blast and EMP damage, and can be deployed in low-profile configurations (Lee, 1986, pp. 27–35). The terminals can be quite small and dispersed easily over many platforms, providing a similar architecture to that of the improved satellite ground segment outlined above.

6.4 *Operations and Maintenance Personnel*

The present DCL is operated and maintained by a relatively small number of personnel. In the case of the United States, the dedicated personnel include engineers from the US Army Satellite Communications Agency (USASATCOMA) responsible for the operation and maintenance of the DCL satellite ground station at Fort Detrick, and a handful of Army communications technicians and Russian language specialists who staff the MOLINK room in the NMCC in the Pentagon and the terminal in the White House Situation Room.

An improved DCL should have a somewhat larger personnel strength, organized as a special unit, specifically responsible for the operation and maintenance of the DCL in a nuclear war environment. The unit should have the capability to maintain connectivity with and to operate the multiple dispersed terminals in the underground and mobile command posts in the event that Washington is destroyed and/or the NCA evacuated from the capital, and rapidly to reconstitute the system in the event that unforeseen nuclear effects destroy or impair critical links. The unit should have its own repair and maintenance equipment as well as spare antennas, cables and terminals in the event that improvised connections are required.

7. *Targeting Issues*

The technical issues involved in constructing and maintaining a survivable and secure DCL are well within the bounds of feasibility and reasonable cost. There are, however, other considerations of strategic nuclear policy, including arms control and targeting issues, which are at least as important and perhaps more difficult to resolve. Some of the more interesting technical, targeting and arms control issues are in fact quite interrelated.

An essential feature of a survivable and endurable DCL is the ability to provide dedicated and continuous communications connections between the satellites and/or the satellite ground control stations, and the HF network on the one hand, and the terminals in the mobile and underground alternate command posts on the other hand. It is also essential, however, that the features of dedicated and continuous operation of the communication links do not compromise the location of these alternate command posts and, more especially, that of the NCA itself. As May & Harvey have stated: 'A dedicated communications link . . . must not serve . . . as a mechanism that could assist targeting of command and control nodes' (1987, p. 715).

The design and operation of the terminal connections should therefore be accorded the closest attention from a targeting perspective. The laying of underground optical fibre cables (including trench excavation) can be monitored from where the trenches/cables connect with the satellite ground control stations. In the Soviet case, however, the deep underground facilities are so extensive and interconnected that the point where a cable entered an underground bunker could be so far (tens of miles) from the underground command post itself as to raise no particular concern. The existence of EHF SATCOM terminals could also be monitored, but these are sufficiently small to be camouflaged; the underground connections between the terminals and the actual command posts can also be tens of miles long; and EHF SATCOM terminals will soon be widely deployed for a variety of purposes, including many not related to strategic command and control. Even low probability of intercept (LPI) transmissions could provide intelligence on the general directional relationships and likely distances between the dispersed terminals.

The issue warrants high-level policy consideration because of the attention which both the USA and the Soviet Union accord to the respective leaderships in their strategic nuclear targeting policies and plans.

The destruction of the US leadership is central to Soviet strategic nuclear doctrine and plans. Soviet strategic planners believe that the best approach to limiting damage to the Soviet Union is the rapid and wholesale destruction of the ability of the USA and its allies to wage nuclear war. Soviet planners evince no willingness whatsoever to seriously consider the possibility of limited or controlled strategic nuclear operations. Rather, Soviet strategic policy and targeting doctrine, together with some quite explicit pronouncements, is to the effect that any nuclear exchange would involve simultaneous and unconstrained attacks on a wide range of targets, which would certainly include the US NCA and its national C^3I systems, and other administrative and governmental facilities (Ball, 1986b, ch. 3).

There is no evidence that the Soviet strategic planners believe that the damage the Soviet Union would suffer from the resultant US response would be anything less than horrendous. On the other hand, they evidently reckon that it would be significantly less than that which would pertain in the event that the USA was allowed to control the escalation process and to engage the Soviet Union with its strategic forces fully coordinated and its planners fully informed by timely and accurate intelligence with respect to the deployments and movements of the Soviet's own strategic nuclear forces. By attacking the US national command system together with the strategic nuclear forces and associated C^3I system, and thus causing any US response to be less coordinated, more ragged and much more degraded than it otherwise would be, the casualties which the Soviet Union would be likely to suffer could well be less than half what they otherwise might be – perhaps 30–50 million fatalities rather than 50 to 100 million! Indeed, if the US NCA and the other critical elements of the US C^3I system were to be successfully destroyed at the outset of any exchange, Soviet planners could well believe that it might be possible to limit fatalities and damage to much lower levels.

The Soviet Union maintains the most extensive and comprehensive signals intelligence (SIGINT) capabilities in the world (Ball, 1989), and one of its principal purposes is to monitor the communications of US national command authorities and their command posts. The GRU Technical Service (TS) Group in the Soviet Embassy on 16th Street in Washington has been extremely successful in monitoring US crisis communications, both within the capital and between the capital and other important command authorities and facilities. According to one account, for example:

> After the Cuban missile crisis of 1962, Krushchev complimented the GRU for having provided him with information from telephone intercepts in Washington clarifying the events and discussions in official circles that led to the final resolution of the crisis (Parham, 1985, p. 8; Rositzke, 1981, p. 197).

US command frequencies and circuits which have been identified by the Soviet SIGINT agencies are continuously monitored – including frequencies used for communications with the NEACP, SAC Emergency Action Message (EAM) transmissions, and for communications between the NMCC in Washington and SAC and NORAD headquarters in Nebraska and Colorado respectively. In June 1980, for example, following one of the two false alarms of Soviet ballistic missile launches which occurred at the NORAD Cheyenne Mountain Complex that month, the NEACP at Andrews Air Force Base in Maryland was moved to the end of the runway and readied for take-off. The communications between the NMCC, SAC headquarters and NORAD headquarters were monitored and transmitted to Moscow in real-time (NBC Nightly News, 1986). Given the Soviet interest in destroying the US NCA in a nuclear exchange, it is only prudent to assume that Soviet SIGINT derived from monitoring communications between the NCA and the subordinate and alternate command facilities would be used, together with other intelligence on leadership movements, to target the NCA together with the subordinate and alternate command facilities.

US nuclear war planning also includes attacks on the Soviet leadership, although there has been significant evolution with respect to the strategic rationale of such attacks. Since the late 1940s, US plans have included leadership and command centres as part of the broad goals of negating Soviet war-fighting capability and inflicting maximum political and societal punishment for Soviet aggression. SIOP-63, which came into effect on 1 August 1962, included a Major Attack Option (MAO) dedicated to leadership targets, and through the 1960s a variety of decoys and other 'penetration aids' ('penaids') were devised to counter the anti-ballistic missile (ABM) system deployed around Moscow. However, most Soviet leadership posts proved very difficult to locate precisely. Moreover, since SIOP-63 the leadership target category had been regarded as a 'withhold', i.e. an option to be reserved until the later phases of an exchange, when all-out war was inevitable. (As noted above, Moscow was separated out from other targets in the SIOP in November 1961.) This approach was intended to enhance escalation control by allowing the Soviets the ability to order discriminate and controlled nuclear strikes short of all-out war and by preserving the possibility of negotiating war termination between the US and Soviet leadership.

In 1974, new targeting guidance was issued which retained the Soviet leadership as a specific target category, although the 'centres of political leadership and control' remained exempted from attack in the initial phases of a strategic nuclear exchange to promote intra-war deterrence and intra-war bargaining. The newly created Strategic Reserve Force was designed primarily to destroy the Soviet leadership in the latter phases of an exchange if necessary.

In 1979 the Nuclear Targeting Policy Review (NTPR) identified the targeting of the Soviet leadership and political control system as an essential issue (US Congress, 1979, p. 116). The argument made at the time was that deterrence was most enhanced by targeting 'what the Soviet Union fears most', which was loss of its own physical (territorial) integrity and political (Communist Party) control (Gray, 1986, pp. 181–186). Guidance issued in 1980 gave a qualitatively greater thrust to targeting the Soviet leadership. Secretary of Defense Harold Brown, in his final Annual Report to Congress on 19 January 1981, stated that 'the Soviet leadership clearly places a high value on preservation of the regime and on the survival and continued effectiveness of the instruments of state power and control', and that 'a clear US ability to destroy them [i.e. Soviet leadership and control centers] poses a marked challenge to the essence of the Soviet system and thus contributes to deterrence' (Brown, 1981, pp. 38, 41). The Soviet leadership was defined to consist of 'some 100,000 people', for which hardened underground shelters had been constructed near their places of work, and at relocation sites outside Moscow and other cities (Brown, 1980, p. 78).

Since 1987, plans have been developed to enable the destruction of the Soviet political and military command and control system at any point in a strategic nuclear exchange (Ball & Toth, 1990, pp. 72–77). For the first time, a prompt counter-leadership option has been incorporated in the SIOP and weapons allocated to this mission. 'Prompt counter-C^3' weapons which have been allocated to the Soviet leadership facilities include highly accurate Peacekeeper MX

ICBMs, which are capable of destroying 'very hard leadership bunkers' (Chain, 1987, p. 67; Sjordal, 1988, p. 22; US Congress, 1982, p. 4173). Trident II D-5 SLBMs with comparable accuracy will also be targeted, at least in part, on hardened Soviet leadership facilities (Chain, 1987, p. 67).

On the other hand, US officials have argued that the accuracy/yield combinations of both the MX and Trident II are inadequate for high kill probabilities against 'deeper buried' leadership and C^3 centres, and that earth-penetrating warheads are therefore required (Canan, 1988, p. 74). In September 1988, Secretary of Defense Frank Carlucci authorized the Department of Defense to proceed (in cooperation with the Department of Energy) to develop an earth-penetration capability (Strobel, 1988, p. 1). Several earth-penetration concepts have been studied in recent years, including both 'rigid' and 'shallow' types (Silber, 1987, p. 1; Ulsamer, 1987, p. 70). The former includes a high-strength metal 'bullet' carrying the nuclear device that could burrow hundreds of feet into the earth using the force of the impact.[6] Manoeuvrable Reentry Vehicles (MARVs) carrying rigid penetrating warheads are under development, with an operational target date of the mid-1990s (DE, 1987, p. 13). Warheads with vastly higher yields and specially enhanced effects are under development. Weapons of truly gigantic yields are back in vogue, apparently as short-term solutions using bombers as the delivery system. For example, two-decade-old B-53 bombs with yields of 9 megatons (some six times greater than anything else in the US inventory) are being reactivated (Carlson, 1987, p. 1; WT, 1987, p. 5); and, according to one official source, consideration is being given to the development of a mammoth 22-megaton weapon.

New penetration aids are also under development to ensure that US ICBMs would be able to penetrate any foreseeable enhancement of the ABM system around Moscow and destroy the national leadership facilities (AWST, 1987a, p. 13; AWST, 1987b, p. 17; Ulsamer, 1987, p. 70).

Finally, a variety of new airborne and satellite sensor systems have been developed to provide a capability to locate Soviet underground and mobile command posts during a strategic nuclear exchange. One of the first airborne systems to be tasked with intra-war strategic intelligence collection was RC-135 strategic reconnaissance aircraft. According to General Robert Rosenberg, then Policy Assistant to the President for National Security Affairs, 12 RC-135s equipped with SIGINT capabilities have been set aside for intra-war C^3I monitoring purposes: 'The aircraft have certain capabilities essential to being able to tell what is alive and what is not alive in Soviet command and control capability after a raid' (Rosenberg, 1980, p. 63). A new Mach 5 Stealth reconnaissance aircraft has also been developed to provide SAC with intelligence concerning the location and operation of Soviet alternate command posts (Halloran, 1988, pp. 1, 5; Happenheimer, 1988, pp. 70–73, 114, 116). With respect to new satellite sensor systems, one of the purposes of the *Lacrosse* radar-imaging satellites, which can 'see' through clouds, darkness, and even some foliage, is to monitor the movement of Soviet mobile command posts. Similarly, the latest US photographic intelligence (PHOTINT) satellites – variously referred to as the Advanced KH-11, the KH-12 *Ikon*, or the Strategic Response Satellite – are also designed to track Soviet mobile command posts. In addition, these satellites are equipped with SIGINT capabilities designed to monitor Soviet 'secure' communications (AWST, 1990, p. 26; Kolcum, 1990, p. 25). Finally, a new series of geostationary SIGINT satellites – variously referred to as *Magnum*, *Mentor* or *Orion* – are able to monitor a plethora of relatively weak signals and other electronic emissions throughout the Soviet Union. A primary wartime mission of these geostationary SIGINT satellites is to locate and monitor the Soviet alternate national C^3 system.

The existence of these various targeting plans, weapons programmes and sensor systems must impact on the willingness of the US and the Soviet NCAs to make contact with each other in an intra-war situation. At the very least, they are not conducive to expeditious or responsive communication exchanges. In a situation where much of the respective US and Soviet national C^3 systems had been destroyed and each side was actively searching for signs of leadership reconstitution in the other country, there would be grave concern that use of the hot-line could be tantamount to suicide.

8. *Conclusion*

For more than a decade now, both the United States and the Soviet Union have devoted increasing resources to enhancing the capabilities, survivability and endurance of their respective strategic C^3I systems. The particular directions of these investments and the strategic rationales for these efforts have, however, been significantly different. In the United States, the principal concern has been to provide the NCA with the ability to conduct strategic nuclear operations in some responsive and informed fashion for some 24–48 hours following the initiation of a strategic nuclear exchange, although throughout the 1980s attempts were also made to support the more problematic goal of controlling a nuclear exchange for a more protracted period of several weeks or even months. In the case of the Soviet Union, the emphasis has been less on escalation control than on ensuring the survivability of the leadership itself. In both cases, some programmes have been pursued more because of the opportunities provided by technological promise than by the demands of national strategic policies.

However, despite the high-level policy attention accorded strategic C^3I programmes and the magnitudes of both the Soviet and US investments in these programmes, the requirements of the direct communications link between Moscow and Washington have been essentially ignored. Very few improvements have been made to the DCL since the satellite communications link became operational in 1978. In 1984, a facsimile transmission capability was added, and the Soviet COMSAT circuit was transferred from the highly elliptically orbiting Molniya satellites to the geostationary Gorizont COMSAT system. The US satellite ground station at Fort Detrick in Maryland has recently also been modernized. However, these improvements have done little to enhance the strategic utility of the DCL.

The DCL remains quite deficient with respect to its strategic rationales. Three principal strategic rationales have been delineated: crisis management; escalation control; and war termination. The DCL has 'proved invaluable' with respect to crisis management, as Secretary Weinberger reported to Congress in April 1983 (Weinberger, 1983, p. S4364), but even in this respect there are important deficiencies in communications security (COMSEC) which need to be addressed. The present DCL system is quite incapable of satisfying the other two strategic rationales. It simply lacks sufficient survivability and endurance to provide connectivity between Moscow and Washington throughout a strategic nuclear exchange. Indeed, it is only likely to remain operational during the period in a nuclear exchange when restraint is being exercised for other reasons. Once restraint is abandoned, and an exchange progresses to any large-scale level, the availability of the hot-line could not be relied upon, yet it is during this period that direct communication between the respective US and Soviet national command authorities is likely to be most critical. The deficiencies of the present DCL with respect to war termination are especially disturbing since the DCL is the principal mechanism which has been identified with facilitating war termination.

An improved DCL, which would provide a sufficiently capable, reliable, survivable and reasonably endurable communications link, can be designed and deployed for around three-quarters of a billion dollars for the complete programme. This cost would be shared between the two parties – i.e. some USD 375 million each (or around half the cost of a single B-2 bomber!). The improved system would be dedicated solely to the purpose of direct Moscow–Washington communications and would have redundancy in all its critical components – satellite and HF circuits; dual satellites and ground control stations; dual transmission frequencies; and multiple, dispersed terminals installed in various alternate mobile and underground national command posts. It would be capable of surviving all the threats likely to be encountered in a nuclear war environment, apart from concerted attacks specifically directed against it – for which there is no imaginable strategic rationale.

In order to ensure that neither the US nor Soviet national command authorities have any inhibitions against using the hot-line in an intra-war situation, there should be a reconsideration of those weapons programmes and strategic targeting plans which are designed specifically to locate and destroy these national command authorities. Finally, consideration should be given to arms control and confidence-building measures designed to further enhance the survivability of the DCL and encourage confidence in its strategic utility. An agreement to specifically eschew actions which might impair its operations is worth consideration. An anti-satellite (ASAT) agreement would also be very helpful.

There is simply no excuse for not proceeding to develop and deploy an improved hot-line. The costs are virtually insignificant; its utility in the event of a nuclear exchange is incalculable. The fact that current political developments in the Soviet Union and in the US–Soviet strategic relationship are dramatically reducing the likelihood of strategic confrontation is not a reason for inaction. Rather, these developments provide an unprecedented opportunity for cooperative efforts to dramatically improve communications links between the superpowers. Posterity will not be forgiving if the opportunity is forsaken.

NOTES

1. The coverage of the Gorizont satellite stationed at 14°W is shown in Long (1987, pp. 187–190), and the Intelsat satellite stationed at 24.5°W in Long (1987, pp. 225–226).
2. Moscow was specifically separated out from other targets in the first US SIOP, SIOP-62, in November 1961. In the second SIOP, SIOP-63, which was prepared in 1961–62 and which officially came into effect on 1 August 1962, Soviet national command and control facilities were exempted from early attack in order to provide the Soviet NCA with the option of conducting a controlled, 'no-cities' counterforce exchange. Through SIOP-5 (1976–83) and into SIOP-6, Soviet command and control facilities were explicitly defined as one of the critical 'withhold' target sets (Ball, 1986a, pp. 63–64, 82).
3. The lack of a DCL connection in the case of the Strategic Air Command (SAC) Post-Attack Command and Control System (PACCS) or *Looking Glass* aircraft is discussed in Ford (1985, pp. 165–167).
4. There is a strong argument that dust clouds raised by detonations should not be considered a particular threat to EHF communications (see Fasuse, 1981).
5. For example, the AN/GSC-52 state-of-the-art medium terminal (SAMT), produced by Ford Aerospace and Communications Corporation and Harris Corporation Government Systems Sector, has a concentric three-zone shielding design which together with the use of fibre optics provides protection against EMP.
6. The W-86 earth penetration warhead designed for the Pershing II missile was intended 'to dive about nine stories underground before exploding' (Cochran et al., 1984, p. 311).

REFERENCES

ACT, 1987. 'US, Soviet Union Sign Pact to Reduce Risk of Nuclear War: Text of the Agreement', *Arms Control Today*, vol. 17, no. 8, October, pp. 28–29.

Arkin, William M. & Richard W. Fieldhouse, 1985. *Nuclear Battlefields: Global Links in the Arms Race*. Cambridge, MA: Ballinger.

AWST, 1987a. *Aviation Week and Space Technology*, vol. 127, no. 11, 21 September, p. 13.

AWST, 1987b. *Aviation Week and Space Technology*, vol. 127, no. 13, 28 September, p. 17.

AWST, 1990. 'NASA Prepares Shuttle Atlantis for Next Mission', *Aviation Week and Space Technology*, vol. 132, no. 8, 19 February, p. 26.

Ball, Desmond, 1981. *Can Nuclear War Be Controlled? Adelphi Paper* no. 169. London: International Institute for Strategic Studies.

Ball, Desmond, 1985–86. 'Nuclear War at Sea', *International Security*, vol. 10, no. 3, Winter, pp. 3–31.

Ball, Desmond, 1986a. 'The Development of the SIOP, 1960–1983', pp. 57–83 in Desmond Ball & Jeffrey Richelson, eds, *Strategic Nuclear Targeting*. Ithaca, NY: Cornell University Press.

Ball, Desmond, 1986b. 'Soviet Strategic Planning and the Control of Nuclear War', pp. 49–67 in Roman Kolkowicz & Ellen Propper Mickiewicz, eds, *The Soviet Calculus of Nuclear War*. Lexington, MA: Heath.

Ball, Desmond, 1989. *Soviet Signals Intelligence (SIGINT): Intercepting Satellite Communications*. Canberra Papers on Strategy and Defence no. 53, Canberra. Strategic and Defence Studies Centre, Australian National University.

Ball, Desmond & Robert C. Toth, 1990. 'Revising the SIOP: Taking War-fighting to Dangerous Extremes', *International Security*, vol. 14, no. 4, Spring, pp. 65–92.

ANNEX 1: REPORTED USES OF THE DCL

There is no publicly available list of the occasions when the hot-line has been used. As Secretary of Defense Caspar Weinberger reported to Congress in April 1983:

> In keeping with the Hotline mission, the precise number of times that the two heads of state have used it has not been disclosed. It is known that it has been used sparingly during its twenty-year existence, but it has proved invaluable in major crises. US Presidents have cited its use during the 1967 Arab–Israeli War to prevent possible Soviet misunderstanding of US fleet movements in the Mediterranean and during the 1973 Arab–Israeli War (Weinberger, 1983, p. S4364).

The following is a summary compendium derived from memoirs of former US Presidents and other senior US national security officials as well as unconfirmed media accounts.

Date	Comments
1. 5 June 1967	First use of the hot-line. Initiated by Soviet Premier Kosygin within hours of the outbreak of the Arab–Israeli War. According to President Johnson's account: [Kosygin] expressed Soviet concern over the fighting. Kosygin said that the Russians intended to work for a ceasefire and that they hoped we would exert influence on Israel. I replied, in part, that we would use all our influence to bring hostilities to an end, and that we were pleased the Soviets planned to do the same thing (Johnson, 1971, pp. 287–303).
2. 8 June 1967	Following the Israeli attack on the USS *Liberty*, President Johnson used the hot-line to inform Premier Kosygin that the US was aware that Israel was responsible and that US aircraft were scrambling from carriers in the area only to aid the stricken ship (Johnson, 1971, p. 301).
3. 10 June 1967	Initiated by Premier Kosygin, who informed President Johnson that the Soviet Union would take 'independent action' if Israel did not cease military operations in accordance with UN Security Council resolutions (Johnson, 1971, p. 302). Additional exchanges over the hot-line continued throughout the morning of 10 June 1967 (Johnson, 1971, p. 303).
4. 'Late December 1968'	Reportedly used by President Johnson to send Moscow progress reports on the Apollo 8 mission that circumnavigated the moon (Hudson, 1973, p. 24).
5. 12 December 1971	Indo-Pakistani War. First use of hot-line by the Nixon Administration. Used by President Nixon to inform Moscow that unless pressure was put on India to accept a standstill ceasefire and immediate negotiations, the US would proceed unilaterally, which might produce 'consequences neither of us want' (Kissinger, 1979, p. 909).
6. 13 December 1971	Response to above from General Secretary Brezhnev to the effect that Moscow was conducting a 'clarification' of the circumstances in India and would inform the US of the results 'without delay' (Nixon, 1978, p. 529).
7. 24 October 1973	Yom Kippur War in the Middle East. Used by General Secretary Brezhnev to inform Washington that Moscow believed Israel was continuing to fight despite a UN Security Council resolution and that unless the US and the Soviet Union immediately dispatched military forces to the region, Moscow would consider unilateral action. President Nixon has described this message as 'perhaps the most serious threat to US–Soviet relations since the Cuban missile crisis eleven years before'. Rather than respond with 'words' over the hot-line, the US decided to increase the alert levels of all US forces (to DEFCON 3) (Nixon, 1978, pp. 938–939).
8. 26 October 1973	'Another hot-line exchange', initiated by General Secretary Brezhnev, who (according to President Nixon's account) 'made a formal complaint about what he called Israeli hostilities', and also complained that the US alert 'had surprised him . . . and had not promoted a relaxation of tension' (Nixon, 1978, p. 942. See also Kissinger, 1982, pp. 607–608).

Date	Comments
9. 27 October 1973	President Nixon responded that the Brezhnev message of 24 October had represented a serious threat and was 'taken seriously here in Washington' (Nixon, 1982, p. 609).
10. July 1974	Turkish invasion of Cyprus (Stone, 1988, p. 60).
11. October 1978	Conflict in Lebanon. As recounted by President Jimmy Carter. Late at night I sent Brezhnev a rare message on the hot line urging him to help us by using his influence with the Syrians to obtain a cease-fire in Lebanon . . . Quite early in the morning . . . I had Brezhnev's reply, pledging to give us maximum assistance (Carter, 1982, p. 233).
12. 1979	SALT II negotiations. According to an account in the *New York Times Magazine*: During SALT II negotiations, when President Jimmy Carter's personal letters to General Secretary Brezhnev were repeatedly answered in a style one United States security adviser suggested 'had been written by the 14th sub-secretary of the Foreign Ministry', Zbigniew Brzezinski, the national security adviser, recommended that the President send his communications over the hot line. It got Brezhnev's attention, all right, but one White House participant recalls that the Russians, who take use of the hot line very seriously, replied with something akin to: 'Please don't ever do that again!' (Stone, 1988, p. 60).
13. 28 December 1979	Initiated by President Jimmy Carter following the Soviet invasion of Afghanistan. According to President Carter's account: I sent Brezhnev on the hot line the sharpest message of my Presidency, telling him that the invasion of Afghanistan was 'a clear threat to the peace' and 'could mark a fundamental and long-lasting turning point in our relations'. I added, 'Unless you draw back from your present course of action, this will inevitably jeopardize the course of United States–Soviet relations throughout the world. I urge you to take prompt constructive action to withdraw your forces and cease interference in Afghanistan's internal affairs' (Carter, 1982, p. 472; see also Brzezinski, 1983, p. 429; and IHT, 1979, p. 1).
14. 30 December 1979	General Secretary Brezhnev responded to President Carter's message of 28 December 1979. According to Carter's account: Brezhnev came back with a devious message, repeating his false claim that the Soviets had gone in at the request of Afghan leaders because of 'armed incursions from without into Afghanistan territory' – which, in fact, were nonexistent. He repeated an earlier promise: 'As soon as the reasons which prompted the Afghan request to the Soviet Union disappear, we fully intend to withdraw the Soviet military contingents from Afghan territory' (Carter, 1982, p. 472).
15. 3 December 1980	Polish crisis. President Jimmy Carter 'sent Brezhnev a direct message warning of the serious consequences of a Soviet move into Poland' (Carter, 1982, p. 584). Carter recorded in his diary on 8 December 1980 that 'Brezhnev has not answered my hot-line message. This is the first time that has occurred' (Carter, 1982, p. 585).
16. 1981	The hot-line was reportedly used by President Reagan to express concern about the situation in Poland (Stone, 1988, p. 60).
17.	It was reportedly also used by Moscow to clarify events in Lebanon (Stone, 1988, p. 60).
18. 28 December 1984	Moscow reportedly activated the hot-line to inform Washington of an aberrant missile launched from the Barents Sea on a course to Hamburg (but which crashed in Finland) (Evans, 1985, p. 1).

Brown, Harold, 1980. *Department of Defense Annual Report Fiscal Year 1981*. Washington, DC: US Government Printing Office.

Brown, Harold, 1981. *Department of Defense Annual Report Fiscal Year 1982*. Washington, DC: US Government Printing Office.

Brzezinski, Zbigniew, 1983. *Power and Principle: Memoirs of the National Security Adviser, 1977–1981*. New York: Farrer, Straus & Giroux.

Canan, James W., 1988. 'The Dangerous Lull in Strategic Modernization', *Air Force Magazine*, vol. 71, no. 10, October, pp. 70–75.

Carlson, John, 1987. 'US Ready to Reactivate Colossal Iowa-made Bomb', *Des Moines Register*, 28 September, p. 1.

Carnahan, Burrus M., 1989. 'Decreasing the Danger in Military Activities: The Meaning of the New US–Soviet Agreement', *Arms Control Today*, vol. 19, no. 6, August, pp. 13–17.

Carter, Ashton B.; John D. Steinbruner & Charles A. Zraket, eds, 1987. *Managing Nuclear Operations*. Washington, DC: Brookings.

Carter, Jimmy, 1982. *Keeping Faith: Memoirs of a President*. New York: Bantam.

Chain, General John T. (CINCSAC), 1987. 'Strategic Fundamentals', *Air Force Magazine*, vol. 70, no. 7, July, pp. 64–67.

CN, 1989. 'Soviet/US Joint Test', *Current News* (American Forces Information Service), Washington, DC: Office of the Assistant Secretary of Defense for Public Affairs, 5 December, p. 6.

Cochran, Thomas B.; William M. Arkin & Milton M. Hoening, 1984. *Nuclear Weapons Databook, Volume 1: US Nuclear Forces and Capabilities*. Cambridge, MA: Ballinger.

DCA, 1985. Defense Communications Agency (DCA), *Facilities Handbook (Areas 1, 2, and 9)*, Scott Air Force Base, IL: Defense Communications Agency Operations Center, January.

DCPA, 1975. Defense Civil Preparedness Agency (DCPA), *High Risk Areas*, Washington, DC: Defense Civil Preparedness Agency, TR-82, April, pp. 18–21.

DE, 1985. 'Ford Developing Mobile Satellite Station', *Defense Electronics*, vol. 17, no. 5, May, p. 25.

DE, 1987. 'Manoeuvrable, Penetrating Nuclear Warhead Expected', *Defense Electronics*, vol. 19, no. 9, September, p. 13.

Department of Defense, 1988. *Soviet Military Power 1988: An Assessment of the Threat*. Washington, DC: US Government Printing Office.

Di Julio, Michael J., 1980. 'HF Radio Program for the Future', *Signal*, vol. 35, no. 3, November, pp. 16–17.

Evans, Michael, 1985. 'Rogue Missile Was on Course for Hamburg', *Daily Express* (London), 31 January, p. 1.

Fasuse, R. P., 1981. *Effects of Sandstorms and Explosion-Generated Atmospheric Dust on Radio Propagation*. Project Report DCA-16, Lexington, MA: Lincoln Laboratory, Massachusetts Institute of Technology, 10 November.

Flock, Warren L., 1987. *Propagation Effects on Satellite Systems at Frequencies Below 10 GHz: A Handbook for Satellite Systems Design*. Washington, DC: National Aeronautics and Space Administration, NASA RP-1108(02), December.

Ford, Daniel, 1985. *The Button: The Pentagon's Strategic Command and Control System*. New York: Simon & Schuster.

Gottfried, Kurt & Bruce Blair, eds, 1988. *Crisis Stability and Nuclear War*. Oxford & New York: Oxford University Press.

Gray, Colin S., 1986. 'Targeting Problems for Central War', pp. 171–193 in Desmond Ball & Jeffrey Richelson, eds, *Strategic Nuclear Targeting*. Ithaca, NY: Cornell University Press.

Halloran, Richard, 1988. 'US To Build Spy Plane That Radar Can't Spot', *International Herald Tribune*, 11 January, pp. 1, 5.

Happenheimer, T. A., 1988. 'Revealed! Mach 5 Spy Plane', *Popular Science*, vol. 233, no. 5, November, pp. 70–73, 114, 116.

Higgins, Commander Harley, 1981. 'The Rediscovery of HF for Command and Control', *Signal*, vol. 35, no. 7, March, pp. 56–57.

Hudson, Richard, 1973. 'MOLINK is Always Ready', *New York Times Magazine*, 26 August, pp. 14, 18, 20, 24, 26 and 29.

IHT, 1979. 'US Warns Soviet Union on Afghanistan Invasion', *International Herald Tribune*, 31 December, p. 1.

Ippolito, L. J.; R. D. Kaul & R. G. Wallace, 1983. *A Propagation Effects Handbook for Satellite Systems Design: A Summary of Propagation Impairments on 10–100 GHz Satellite Links, With Techniques for System Design*, NASA RP-1082(03), Washington, DC: National Aeronautics and Space Administration, June.

Johnson, Lyndon Baines, 1971. *The Vantage Point: Perspectives on the Presidency 1963–1969*. London: Weidenfeld & Nicolson.

Johnson, Nicholas, L., 1987. *The Soviet Year in Space 1986*. Colorado Springs, CO: Teledyne Brown Engineering.

Kissinger, Henry, 1979. *The White House Years*. London: Weidenfeld & Nicolson.

Kissinger, Henry, 1982. *Years of Upheaval*. London: Weidenfeld & Nicolson/Michael Joseph.

Kolcum, Edward H., 1990. 'NASA Delays Launch of Hubble Telescope', *Aviation Week and Space Technology*, vol. 132, no. 5, 29 January, p. 25.

Kolkowicz, Roman & Ellen Propper Mickiewicz, eds, 1986. *The Soviet Calculus of Nuclear War*. Lexington, MA: Heath.

Leahy, Robert G., 1985. 'C^3 for Strategic Nuclear War Termination', *Signal*, vol. 42, no. 12, August, pp. 42, 44.

Lee, Freeman G., 1986. 'High Frequency Tactical Antennas Go Low Profile', *Signal*, vol. 41, no. 3, November, pp. 27–35.

Long, Mark, 1987. *World Satellite Almanac: The Complete Guide to Satellite Transmission and Technology*, Second Edition. Indianapolis, IN: Sams.

May, Michael M. & John R. Harvey, 1987. 'Nuclear Operations and Arms Control', pp. 704–735 in Carter et al., 1987.

McLaughlin, John E., 1981. 'Toward Achieving Adaptive HF', *Signal*, vol. 36, no. 3, November, pp. 53–56.
Munro, Neil, 1989. 'Mobile Posts Could Serve as Wartime Nerve Centers', *Defense News*, 24 April, pp. 3, 26.
NBC Nightly News, 1986. 'Soviet Eavesdropping Techniques'. New York, 19 August, transcript.
Nelson, Jack & George Skelton, 1985. 'Reagan Will Offer Military Hot Line Plan', *Los Angeles Times*, 7 May, p. 1.
Nixon, President Richard, 1974. 'Policy for Planning the Employment of Nuclear Weapons', National Security Decision Memorandum (NSDM)-242, 17 January.
Nixon, Richard, 1978. *The Memoirs of Richard Nixon*. New York: Grosset & Dunlap.
Parham, William, 1985. 'GRU Outspends KGB Seeking Military Data', *Washington Times*, 24 May, p. 8.
Riberia, Robert C., 1985. 'The Evolution of the Direct Communications Link', *Signal*, vol. 40, no. 4, December, pp. 95–96.
Rosenberg, General Robert, Spring 1980. 'The Influence of Policy Making on C^3I'. Cambridge, MA: Seminar on Command, Control, Communications and Intelligence, Center for Information Policy Research, Harvard University.
Rositzke, Harry, 1981. *The KGB: The Eyes of Russia*. Garden City, NY: Doubleday.
Rumsfeld, Donald H., 1977. *Annual Defense Department Report FY 1978*. Washington, DC: US Government Printing Office.
Sanders, C. W.; G. F. Sandy, J. F. Sawyer & A. Schneider, 1977. *Study of Vulnerability of Electronic Communication Systems to Electronic Interception*. MITRE Technical Report MTR-7439, The MITRE Corporation, Metrek Division, vol. 1, January.
Signal, 1984. 'US–Soviet Hotline', *Signal*, vol. 39, no. 4, December, p. 110.
Silber, Howard, 1987. US Working on Warheads To Hit Soviets Underground', *Omaha World-Herald*, 27 September, p. 1.
Sjordal, Lt. Col. Paul E. (Director of Public Affairs, Midwest Region, Department of the Air Force), 1988. 'Peacekeeper Just That: A Peacekeeper', *Chicago Tribune*, 21 April, p. 22.
Stone, Webster, 1988. 'Moscow's Still Holding: Twenty-five Years on the Hot Line', *New York Times Magazine*, 18 September, pp. 58, 60, 67.
Strobel, Warren, 1988. 'US To Make Nuclear Bomb That Burrows', *Washington Times*, 12 September, p. 1.
Ulsamer, Edgar, 1987. 'Missiles and Targets', *Air Force Magazine*, vol. 7, no. 7, July, p. 70.
US ACDA, 1982. US Arms Control and Disarmament Agency (ACDA), 'US submission to the Eighteen-Nation Disarmament Committee (ENDC), Geneva, 12 December 1962', *Arms Control and Disarmament Agreements: Texts and Histories of Negotiations*. Washington, DC: Arms Control and Disarmament Agency.
US ACDA, 1984. US Arms Control and Disarmament Agency (ACDA), 'Agreement Between the United States of America and the Union of the Soviet Socialist Republics to Expand the US–USSR Direct Communications Link, July 17, 1984', in *Documents on Disarmament 1984*. ACDA Publication 126, Washington, DC: US Government Printing Office.
US ACDA, 1986. US Arms Control and Disarmament Agency (ACDA), 'Statement by President Reagan: Agreement to Expand the Direct Communications Link With the Soviet Union, July 17, 1984', *Documents on Disarmament 1984*. ACDA Publication 126, Washington, DC: US Government Printing Office.
US Congress, House of Representatives, Committee on Appropriations, 1979. *Department of Defense Appropriations for 1980*, Part 3, Washington, DC: US Government Printing Office.
US Congress, Senate Armed Services Committee, 1982. *Department of Defense Authorization for Appropriations for Fiscal Year 1983*. Washington, DC: US Government Printing Office.
US Congress, Senate Foreign Relations Committee, 1974. *US–USSR Strategic Policies*. Washington, DC: US Government Printing Office.
USN&WR, 1980. *US News & World Report*, 6 October, p. 22.
Weinberger, Caspar W., 1983. 'Report to the Congress Direct Communications Link and Other Measures to Enhance Stability', *Congressional Record – Senate*, 12 April, pp. S4362–4372.
Wheelon, Albert D.; Roger W. Clapp & Barnet Krinsky, 1982. *EHF Satellite Communications*. Monterey, California: Paper prepared for US Navy Space Symposium, 15 October, p. 4.
Whitman, John G. & William W. Davison, 1974. 'The New Hotline – Via Satellite Direct Communications Link', *Signal*, vol. 28, no. 6, March, p. 52.
WP, 1990. 'Hot Line to Moscow', *Washington Post*, 13 February, p. B-3.
WT, 1987. 'Powerful B-53 Bomb Comes Out of Mothballs', *Washington Times*, 5 August, p. 5.

DESMOND BALL, b. 1947, PhD in International Relations (Australian National University, 1972); Special Professor, Institute of Advanced Studies, Australian National University, and Head, Strategic & Defence Studies Centre, Australian National University. Most recent books: *Pine Gap: Australia and the US Geostationary Signals Intelligence Satellite Program* (1988); *Soviet Signals Intelligence (SIGINT)* (1989); *Security and Defence: Pacific and Global Perspectives* (1990).