ICBM Command and Control – History to Future

Maj Lance K. Adkins, USAF
Command Lead, ICBM Applications Programs
HQ AFSPC

Historical Background: Minuteman I and II

Through years of service, US Intercontinental Ballistic Missiles (ICBMs) have undergone steady and incremental modernization resulting in improved functionality through the incorporation of new technology. However, significant capability improvements generally have required major weapon system upgrades. Nowhere is this more true than in the realm of command and control (C2).

In the earliest ICBM systems (Atlas and Titan), weapon system control was quite direct. Launch control centers were collocated with the launch silos proper. There were no obstacles to running thick bundles of wires and cables through the few hundred feet of tunnel and conduit required.

The development of the Minuteman concept from 1958 to 1962 forced a new look at the control functionality demanded by geographically separated launch facilities (LFs). Whereas collocated missile systems could be guarded and commanded relatively easily within the confines of a secure area, remote LFs required unprecedented innovations in robust digital networking, security perimeter protection, and reliability. With significant modification, these same systems originally emplaced in the early 1960s are still in service today. This first iteration of the Minuteman C2 System was groundbreaking, incorporating a digital network capable of relaying commands from the launch control center (LCC) to individual LFs and returning status messages as needed. This was facilitated by laying tens of thousands of miles of cable that comprised the Hardened Intersite Cable System (HICS) between the launch control centers and launch facilities.

HICS, intended to be protected against acts of man and nature, united the five LCCs and 50 LFs of each missile squadron. It allowed any LCC in a squadron to monitor and command any LF desired within the squadron and was at least nominally survivable against the effects of a nuclear attack. The original Minuteman system did not use encryption or authentication, relying instead on the robustness of the cable's outer casing and maintaining an overpressure of air in the cable for signal protection. An interloper (or more likely a farm implement) cutting into the cable would cause a cable pressure alarm at the owning LCC at which point the duty crew would initiate a security response and investigation of the root cause.

When originally conceived, the concept of an internet-like, packet switched network was still several years in the future, thus the network topology differed significantly from what might be built today.[1] The Minuteman weapon system needed a redundant network that would minimize the average distance between a given point and a set of surrounding points. The result blended features of tree and hub-and-spoke topologies, constructed around the LCC with cables running to multiple LFs and to other LCCs. In practice, it took the form of four radial cables extending from the LCC to a cable ring encircling the LCC at some distance.[2] LFs were connected to branches off this ring and, in some cases, to adjacent rings. This system afforded each LCC the capability to monitor any LF in its squadron of 50. In the Minuteman I system, the missile's own NS10 guidance and control (G&C) computer was integral to the command and control system—receiving, processing, and executing commands transmitted by the LCCs. Additionally, this network (a "strongly connected" network, meaning that it is possible for signals to travel from each node in a squadron to any other node) afforded the system a reasonable measure of redundancy in the event of cables being severed, either by accident or by attack. Finally, commands transmitted from any LCC are repeated by every other node on the network. This "flooding" concept makes the network highly redundant and survivable. As a result, HICS, originally emplaced in the early 1960s, is still in service today, retaining its 1.3 Kbps data rate in the current Minuteman system.

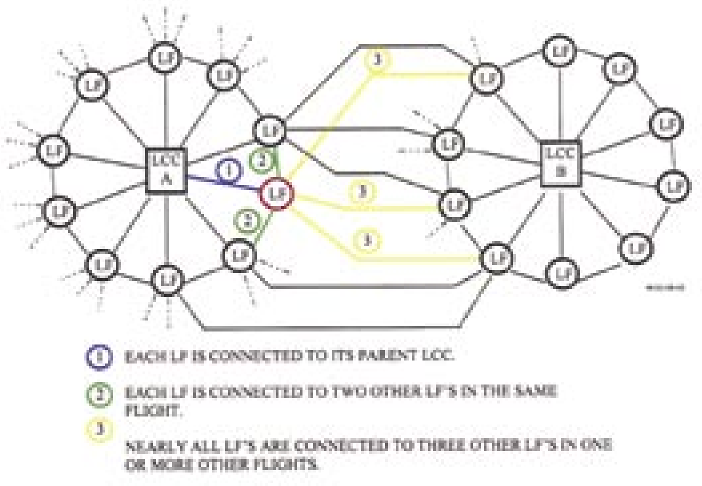
LF
LCC A
LCC B
1
2
3
1 EACH LF IS CONNECTED TO ITS PARENT LCC.
2 EACH LF IS CONNECTED TO TWO OTHER LF'S IN THE SAME FLIGHT.
3 NEARLY ALL LF'S ARE CONNECTED TO THREE OTHER LF'S IN ONE OR MORE OTHER FLIGHTS.

Figure 1. HICS cable runs between LCCs and LFs.

The original Minuteman I guidance system was not capable of being remotely retargeted because of the need to align the missile's internal stabilized platform with a silo-mounted precision North reference. This required that the azimuth of the missile also be aligned to precision North for greatest accuracy. Thus, the missile and its autocollimator (the device used to align the missile guidance to the precision North azimuth) were required to be physically rotated to align to a new target—clearly a challenging process to accomplish under strict time constraints. However, this relatively crude means of aligning missile to target placed very modest requirements on the bandwidth required of the cable system.

In order to achieve the greater levels of versatility required by

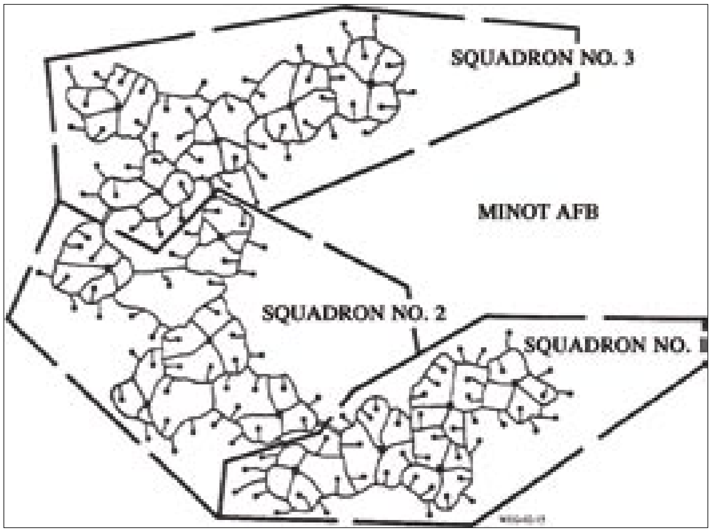

Figure 2. HICS cable layout of Minot AFB, North Dakota, a WS-133A-M system.

Strategic Air Command planners, provisions had to be made for remote retargeting. This upgrade was made in the Minuteman II, which featured the much more sophisticated D37 G&C computer to handle new error correction functions for improved accuracy as well as the faster processing and greater throughput necessitated by the remote retargeting capability. According to the designation system of the time, the original weapon system (designated WS-133A) was redesignated WS-133A-M (or A Modified). Additionally, a new variation on the Minuteman weapon system was developed by Sylvania and designated WS-133B (or the Minuteman II Command Data Buffer). This variant was installed at Grand Forks AFB, North Dakota and in the 564th Missile Squadron at Malmstrom AFB, Montana. Instead of a redundant cable system, the WS-133B used a non-redundant cable system that operated with an independent medium frequency radio that essentially duplicated the command transmission and status monitoring functions of the HICS. A highly survivable architecture in theory, the newer WS-133B was so different from the older WS-133A-M that there was little commonality between the two systems.

A further major change to the Minuteman II C2 system occurred in 1974-1975 when the Software Status Authentication System (SSAS) was incorporated. This change allowed for cryptographic authentication of commands from the LCC and status messages from the LFs. This modification complicated the problems faced by anyone wishing to intercept or spoof traffic moving across the HICS.

Present System: Minuteman III

A desire to improve the accuracy afforded by the Minuteman II led to the Minuteman II Post Boost Control System (PBCS) study, which, in turn, led to the Minuteman III. Minuteman III added a larger third stage motor and a Multiple Independently Targetable Reentry Vehicle capability. Accuracy was greatly improved as a result of the PBCS, which virtually eliminated the downrange error component caused by imprecise Stage III thrust termination. Additionally, a high beta reentry body (one having a finer, more pointed cross-section) was developed that significantly reduced atmospheric dispersion during reentry.[3] Despite these improvements to the missiles themselves, the Minuteman III used the same command and control systems as the older Minuteman I and II. This is not to say, however, that significant changes were not made to the C2 system during this upgrade.

The most sweeping modification to the C2 system since its inception occurred with the Improved Launch Control System (ILCS) upgrade that took place in 1973, starting with Wing V at F. E. Warren AFB, Wyoming. ILCS was needed in order to take advantage of the Minuteman III's remote data change (RDC) capabilities, which were collectively incorporated into the Command Data Buffer (CDB) configuration. Updating to this configuration required significant changes to both the operational flight and operational ground programs as well as to the LCC and LF equipment.[4] In order to prevent unauthorized data change (a potential sabotage method), the RDC protocol employed a second LCC to continually cross-check the information being transmitted by the primary LCC. Any mismatch would result in an abort, which crews would have to cross-check. Significantly, full encryption (as opposed to authentication only in the SSAS upgrade) was now incorporated into the system, and engineers also made significant changes to the G&C system, making the system more capable of handling the kinds of shocks and motion that might result from a nuclear attack. Eventually, five of the six missile wings—regardless of whether they were equipped with Minuteman II or Minuteman III ICBMs—were upgraded to the ILCS standard, with the 44th Missile Wing at Ellsworth AFB, South Dakota, being the sole remaining SSAS Minuteman II wing until it was inactivated in 1994.[5] One disadvantage to CDB was that the encryption scheme slowed the effective data rate of the HICS, making commands and responses somewhat more lethargic from the standpoint of the operator though few today would argue the necessity of strong encryption to nuclear surety.[6]

The most recent and significant upgrade to Minuteman C2 since ILCS has been the Rapid Execution and Combat Targeting (REACT) modification. Essentially computer workstations interfaced with the existing weapon system, REACT was installed at Malmstrom AFB, Minot AFB, and F. E. Warren AFB, during the mid-1990s and allowed for superior integration of communications, weapon system, and retargeting functions at a single two-man console that offered a much improved man-machine interface. Numerous other improvements also came as a result, including data logging, a greater degree of automation in retargeting operations and improved processing of Emergency War Order messages. As sweeping as the changes were to crew operations, the actual changes to the weapon system were less comprehensive. REACT emulates, expedites, and automates the functions performed by the older command consoles but does not otherwise upgrade the C2 network. In order to see dramatically greater performance, the actual C2 infrastructure would have to be upgraded.

In the near future, there will continue to be changes to the Minuteman C2 system, though they will almost certainly remain incremental upgrades rather than wholesale revisions. The first upgrade is known as the ICBM Cryptographic Upgrade (ICU). This involves replacement of the KI-22 cryptovariable used to authenticate and encrypt data moving through the HICS. The KS-60 is an evolved version, designed to be a form, fit, and function replacement for the KI-22, but with a stronger cryptographic scheme and a variety of enhancements, including the ability—following the as-yet unfunded Increment II modification—to have its codes remotely changed, thus saving a considerable number of maintenance hours. The Increment I implementation of KS-60 will reach full operational capability by 2009.

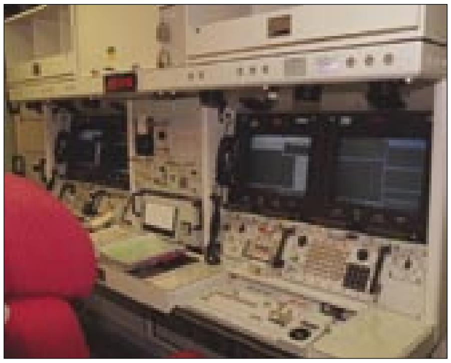

Figure 3. Typical REACT console.

Furthermore, there is a plan afoot to emplace remotely-controlled cameras on LFs to assist in tactical response to security alarms. Designed to address concerns about the lack of updated tactical information available to Alarm Response Team Security Forces, the Remote Visual Assessment (RVA) system (nicknamed "Prairie Hawk") would comprise one or two remotely controlled day/night capable pan-tilt-zoom surveillance cameras on each LF. The concept as currently envisioned uses an 802.11-based wireless internet protocol network, with repeaters mounted on existing structures and purpose-built towers throughout the missile field. Such a system should have fairly significant additional bandwidth and may form the basis of secondary capabilities, such as a means of transmitting data from a variety of portable devices and possibly—following an extensive NSA certification process—form an integral part of the Minuteman C2 architecture. If funded, Prairie Hawk is planned for full operational capability in 2014.

Future Development—the Land-Based Strategic Deterrence Command, Control, Computers, and Communications Study and Minuteman IV

In September of 2005, Air Force Space Command completed the Land Based Strategic Deterrent (LBSD) Analysis of Alternatives. A key part of this study was a Technical Analysis of comand, control, computers, and communications (C4) alternatives conducted by the MITRE Corporation. This analysis examined various technologies from those for enhancing the legacy HICS system to complete replacements for the C4 architecture. These improvements would be integrated into the new Minuteman IV weapon system, planned for deployment in existing Minuteman silos.

One factor that has to be taken into account when Minuteman C4 upgrades are discussed is the expense associated with any sort of HICS replacement. All told, the three remaining Minuteman-equipped space wings have 32,443 miles of buried cable.[7] The cost of replacing this cable with a higher data rate cable is very high (estimated as costing $10.86 per foot or around $2 billion total in 1999 dollars) and would likely represent a significant logistical challenge, as the cables extend largely across privately-owned farms and ranches as well as federally-protected wetlands and other such areas. Naturally, one of the key parts of the LBSD C4 technical analysis involved determining what could be done without incurring the cost of a buried HICS replacement.

Another factor to consider is that the form any C4 system eventually takes will be greatly influenced by the capabilities of the missile guidance set developed for the Minuteman IV. A very fast on-board processor with extensive storage capabilities may well require a high data-rate C4 network to realize the ICBM's full potential, since the new guidance-set computer will likely interface more or less directly with the C4 system. GPS or stellar aiding to augment the accuracy of the inertial guidance system may require regular transmission of almanac data or star catalogs that will place even more demands on bandwidth. Therefore, it appears that some kind of upgrade will be necessary if one of these options is chosen.

Three principal alternatives are described in the study: (1) an Enhanced HICS that as been upgraded to achieve transmission speeds greater than 256 Kbps; (2) a full replacement of the HICS cable with fiber optic cable and; (3) a survivable radio frequency wireless network. Excursions to these alternatives include various hybrids of a fiber-optic and terrestrial radio frequency network. The Extremely High Frequency (EHF) waveform was studied to ensure the alternate launch capability.[8]

The goal of all of these approaches is to produce a net-centric architecture for Air Force ICBMs. This is clearly a big step away from the dedicated, hard-wired infrastructure used in today's Minuteman III system, and it would drive significant increases to speed and flexibility of command. For instance, allowing a missile crew to command any missile in a wing or perhaps even in the entire missile force would become possible. Retargeting could be accomplished in real time to hold more targets at risk, and the possibility exists of using survivable mobile command centers that could deploy in advance of hostilities and perform in a role similar to the current Airborne Launch Control System (ALCS), but more quickly, for longer duration, and at a much reduced operating cost. Next generation ICBM C4 could even be integrated into the Global Information Grid (GIG). This would ensure that the ICBM C4 system remains viable for future network development using common components.

Hardened Intersite Cable System Data Rate Upgrade

According to a 2002 study conducted by General Dynamics, HICS cable is not suitable for extreme upgrades to bandwidth and data rate. Its high capacitance values—due largely to use of Polyvinyl Chloride (PVC) insulation—place a cap on how much frequency bandwidth is available.[9] Modern telephone cables have less than 1/3 the capacitance of HICS cable. This, combined with the extreme length of some stretches of cable between repeaters (in one case 41.7 miles), tends to rule out adding Digital Subscriber Line (DSL) technology to the existing network, at least with commercial, off-the-shelf equipment. Repeaters would have to be added to the network to achieve high data rates, though the study concludes that the existing data rate can probably be improved with DSL, potentially yielding from 64 to 128 Kbps.[10] The aforementioned capacitance issues would also tend to prevent the use of newer Ultra Wide Band (UWB) technology over the existing cable.

The installation of repeaters would alleviate many of the problems but also introduce its own—primarily the need to excavate significant stretches of HICS cable and install nuclear-hardened, radiation-shielded, waterproof amplifiers with some sort of power source, most likely external to the HICS system. Such additional components could introduce new vulnerabilities into an otherwise very robust system.

Fiber Optic Hardened Intersite Cable System Replacement

Another option studied by MITRE Corporation is the outright replacement of the HICS with fiber optic cable. This would provide much faster data signaling rates compared to the HICS. Other advantages include the fact that fiber optic cable runs can easily extend over 100 miles without repeaters, are not susceptible to electromagnetic pulse effects and are lighter and more reliable than copper. However, the cost of replacing the existing HICS, to include obtaining easements, trenching, and laying the cable may be cost-prohibitive in the current fiscal environment. Assuming that fiber optic cable could be installed adjacent to the HICS cable, within the current easements, a wide variety of additional capabilities would be achievable, however, such as transmission of retargeting data to entire wings in fractions of a second, sending and receiving of full-motion video from on-site security systems, and reducing the number of LCCs per squadron from five to one.

A further possibility facilitated by higher bandwidth and fiber optics communication is quantum encryption, which relies upon the quantum physical property of entanglement to protect information from snoopers. Using physical properties of photons which Einstein called "spooky action at a distance," quantum encryption is protected by the laws of physics and would be theoretically unbreakable, regardless of the growth in computer processing power in coming years.[11]

Radio Frequency Terrestrial Replacement of Hardened Intersite Cable System

In an effort to reduce the considerable cost of outright HICS replacement with fiber optic cable runs, the LBSD C4 technical analysis also examined the feasibility of several wireless technologies including free-space optical and several types of radio frequency (RF) technology. There has been a tremendous amount of work and technical innovation in the field of wireless digital communications in the past decade, driven almost entirely by the commercial sector. These innovations, if they could be made acceptable for the ICBM's peculiar needs, have the potential to revolutionize the ICBM's operational art by providing a mixture of low cost, high data rates, flexibility, and potential mobility.

The LBSD study looked at four technological artifices to enable a wireless C4 system. For those familiar with the WS-133B weapon system, wireless ICBM C2 is not a foreign concept. However, the techniques described in the LBSD C4 technical analysis are very distinct from the medium frequency radio incorporated in that system.

The first technology examined involves the use of Free Space Optics, or lasers operating through the air. Such systems exploit very high data rates and low probability of interception, but are also affected by atmospheric conditions, such as rain and snow. Furthermore, the longest sustainable link possible without the use of amplifiers is only around 4 km, requiring numerous amplifier stations.[12] A determined enemy might also attempt to dazzle the laser receivers with other lasers or destroy the amplifier stations to take down the links. Hardening such an architecture would be a considerable challenge.

A second technological possibility examined in the LBSD C4 technical analysis is the new wireless networking technology known as WiMAX, or 802.16. This comparatively recent development incorporates high signal rate line-of-sight (LOS) communications as well as non-line-of-sight (NLOS) communications at a somewhat reduced data rate (nominally 160 Mbps for LOS and 75 Mbps for NLOS). Because it is quite new, WiMAX embodies a variety of technologies to improve the robustness of a wireless C2 system, such as built-in error correcting and adaptive modulation. WiMAX ranges are such that, when within the LOS of other nodes, few amplifiers are required. However, as the NLOS range for WiMAX is less than 10 km, additional amplifiers would be required in occluded terrain.[13]

The greatest weakness of this or any other commercial off-the-shelf (COTS) product will always be nuclear hardness. It is not reasonable to ask hardware designed for business to withstand and operate through the sorts of thermal pulse, blast, and atmospheric scintillation that occur during a nuclear detonation. However, there are improvements that can be made to WiMAX equipment that may make it more tolerant of these conditions and as a waveform and standard, WiMAX seems promising, at least for peacetime operations.[14]

A third type of wireless communications examined by the C4 technical analysis team is known as Ultra Wide Band (UWB). UWB uses extremely short pulses of energy and very accurate timing to produce high data rate signals which are capable of penetrating obstacles, immune to multipath interference, and use very low power levels. Since UWB receivers are only "listening" for a signal at specific and very precisely defined intervals, it is also resistant to jamming or spoofing, since the short receiving intervals act like a range gate on a radar receiver, only accepting signals that fall in a certain time difference of arrival parameters while ignoring all else. A spoofing transmitter would therefore have to be collocated with the spoofed transmitter for its signal not to be rejected.[15] This sort of discrimination, combined with low-probability-of-intercept characteristics makes UWB an alternative with great potential, but its relative novelty means that there are many questions that must be answered before it could begin certification for nuclear C2.[16]

The final possible wireless technology that was explored in the LBSD Analysis of Alternatives (AoA) was based on an advanced EHF satellite communications (SATCOM) equipped with a survivable waveform. While this would be highly dependent upon the funding and development of an appropriate satellite constellation, it would have ample bandwidth for current and future needs as well as providing excellent mobility and survivability, especially in a post-attack scenario, where its EHF signal would be capable of penetrating nuclear scintillation effects.[17] The forthcoming Advanced EHF and Advanced Polar satellite programs will provide a strong combination of survivability and bandwidth that could form the basis of a survivable HICS replacement, assuming that sufficiently hardened EHF terminal can be developed. There would be several drawbacks to such a system, however, including relying on the continued funding, development, and support of the required satellite programs and competing peacetime bandwidth priorities. Additionally, EHF requires exposed antennae, which would be difficult to harden and are susceptible to signal attenuation by precipitation.[18] For this reason, the LBSD AoA recommended consideration of hybrid systems that would use EHF SATCOM as a survivable backup to some other, potentially less survivable system, similar to the role of the ALCS system today, but with greatly enhanced capabilities. The net-centric approach to interlinking the various LFs and LCCs with a packet-switched network could alleviate some of these issues, however, since the SATCOM broadcast would only need to be received at one location in order to be propagated throughout the remainder of the squadron (or wing, or force, depending upon the degree of interconnectivity).[19]

Lockheed Martin Corporation

Figure 4. Advanced EHF satellite.

Conclusion

In the final analysis, Minuteman C2 progress will be dictated by both fiscal reality and the direction of technology. The rapid growth of wireless technology and extremely limited fiscal resources may recommend a wireless or hybrid structure. In any event, the engineers who will lead this effort will be challenged to construct a system that is as robust, long-lived, and sophisticated for its time as the original Minuteman HICS. Even in a very different world than the Cold War Era, the US land-based strategic deterrent has long represented a dagger pointed at the throat of the Nation's would-be adversaries, and as such, commends a high value on the capability to destroy or otherwise marginalize them. A fast, reliable and survivable C2 architecture makes these weapons tougher to counter, more effective, and more defensible—all fundamental to deterrence. A highly accurate, land-based, flexible response option for the President will continue to serve the Nation as a credible deterrent force and the C2 infrastructure must grow along with this option to ensure that this capability is maintained.

Notes:

[1] Albert Wohlstetter and Richard Brody, "Continuing Control as a Requirement for Deterring," *Managing Nuclear Operations*, eds. Ashton Carter, John Steinbruner, Charles Zraket (Washington, DC: The Brookings Institution, 1987), 176.

[2] General Dynamics Communications Systems, *HICS Upgrade Study Technical Report* (Ogden, UT: General Dynamics Communications Systems, 1999), 7-8.

[3] R.F. Nease and Daniel C. Hendrickson, *A Brief History of Minuteman Guidance and Control* (Anaheim, CA: Rockwell Autonetics Defense Electronics, 1995), 3-1.

[4] Ibid., 2-21 – 2-22.

[5] Ibid., 3-34 – 3-35.

[6] Lt Col Erik Hoihjelle, interview by the author, 30 January 2006.

[7] *HICS Upgrade Study*, 91.

[8] Shane Morrison et al., *Land Based Strategic Deterrent (LBSD) Analysis of Alternatives (AoA) – Technical Analysis of Communications Alternatives,* MTR Number 05B0000088 (Bedford, MA: The MITRE Corporation, 2006), 7-1.

[9] Ibid., 2-4.

[10] Ibid., 2-18.

[11] Bob Gourley, *Quantum Encryption vs. Quantum Computing: Will the Defense or Offense Dominate?* (Bethesda, MD: SANS Institute, 2001), http://www.sans.org/rr/whitepapers/vpns/720.php.

[12] Morrison et al., *LBSD AoA* 7-7.

[13] Ibid., 7-5.

[14] Ibid., 7-7.

[15] Ibid., 3-30.

[16] Ibid., 7-7.

[17] Ibid., 4-6.

[18] Ibid., 4-8.

[19] Ibid., 4-8.

Maj Lance K. Adkins (BMusic, University of Tennessee; MS, University of North Dakota; MS, New Mexico Tech) is Command Lead for ICBM Applications Programs in the Directorate of Requirements, Headquarters Air Force Space Command, Peterson AFB, Colorado. He oversees efforts for ensuring the preservation of the ICBM industrial base and development of technologies for future ICBM implementations. He has served as India Flight Commander at Grand Forks AFB, North Dakota; Chief of Flight Test and Chief of Training at the 576th Flight Test Squadron ("TOP HAND"), and Space Superiority Section Chief, Directorate of Transformation, Space and Missile Systems Center. Major Adkins is a graduate of Squadron Officer School and the Sandia Nuclear Weapons Fellowship Program.