MODERNIZING U.S. NUCLEAR COMMAND, CONTROL, AND COMMUNICATIONS

MITCHELL INSTITUTE for Aerospace Studies

MITRE

By Lt Gen David A. Deptula, USAF (Ret.),
and Dr. William A. LaPlante, with Robert Haddick

Note to readers: this electronic edition features an interactive table of contents and endnotes. Click on the page number in the table of contents to be taken to the respective chapter; endnotes in the text are linked to their respective citation at the end of this study. Click on the citation number to go back.

MODERNIZING U.S. NUCLEAR COMMAND, CONTROL, AND COMMUNICATIONS

A Report by
The Mitchell Institute for Aerospace Studies
and The MITRE Corporation

By Lt Gen David A. Deptula, USAF (Ret.),
and Dr. William A. LaPlante,
with Robert Haddick

The Mitchell Institute for Aerospace Studies
Air Force Association
Arlington, VA
February 2019

About the Mitchell Institute for Aerospace Studies

The Mitchell Institute for Aerospace Studies is an independent, nonpartisan policy research institute established to promote understanding of the national security advantages of exploiting the domains of air, space, and cyberspace. The Mitchell Institute's goals are: 1) to educate the public about the advantages of aerospace power in achieving America's global interests; 2) to inform key decision-makers about the policy options created by exploiting the domains of air, space, and cyberspace, and the importance of necessary investment to keep America the world's premier aerospace nation; and 3) to cultivate future policy leaders who understand the advantages of operating in air, space, and cyberspace. Mitchell Institute maintains a policy not to advocate for specific proprietary systems or specific companies in its research and study efforts.

About the Authors

Lt Gen David A. Deptula, USAF (Ret.), is dean of the Mitchell Institute for Aerospace Studies. A decorated Air Force leader, Deptula has planned, flown in, and commanded air operations ranging from humanitarian relief efforts, to contingencies, to major theater war. He served as the principal air attack planner for Operation Desert Storm in 1991, was a joint task force commander in Iraq from April 1998 to October 1999 overseeing Operation Northern Watch, and led the initial air campaign of Operation Enduring Freedom as director of the Combined Air Operations Center from September to November 2001, among other significant operations. Deptula retired after 34 years on active duty in October 2010. In his last assignment, he served as the Air Force's first deputy chief of staff for intelligence, surveillance, and reconnaissance (ISR). He is a prolific author and commentator on modern military strategy and operations, defense, and aerospace power.

Dr. William A. LaPlante is senior vice president and general manager for the MITRE Corporation's national security sector. LaPlante has more than 30 years of experience in defense technology, most recently as the assistant secretary of the Air Force for acquisition from February 2014 to November 2015, and the USAF's principal deputy assistant acquisition secretary from May 2013 to February 2014. Prior to entering public service in 2013, he was MITRE's missile defense portfolio director. During this time, he was appointed to the Defense Science Board (DSB) where he co-chaired a study that looked at enhancing the adaptability of U.S. military forces. Prior to joining MITRE, LaPlante was the department head for global engagement at the Johns Hopkins University Applied Physics Laboratory, where he was responsible for the laboratory's work supporting offensive military capabilities. He holds a bachelor's degree in engineering physics from the University of Illinois, a master's degree in applied physics from Johns Hopkins University, and a doctorate in mechanical engineering from Catholic University of America.

Robert Haddick is a visiting senior fellow at the Mitchell Institute for Aerospace Studies. His previous work for Mitchell includes case study work for the Pentagon's Office of Net Assessment, as well as analysis on NATO defense reform, and strategic deterrence. Haddick has also worked for U.S. Special Operations Command where he wrote studies on security trends in the Asia-Pacific region, and the role of special operations forces in deterrence strategies. He is the author of *Fire on the Water: China, America, and the Future of the Pacific* (Naval Institute Press, 2014), and is a former Marine Corps officer. Haddick has delivered numerous lectures on strategy and force development to audiences inside the U.S. government.

Cover design by Zaur Eylanbekov; photos: Northrop Grumman, U.S. Air Force, U.S. Navy

Contents

Foreword

For over 50 years the forces of America's nuclear triad have prevented the use of nuclear weapons in combat. However, the majority of the aircraft forming one of the triad's legs today have an average age of over 50 years. The land-based Minuteman III intercontinental ballistic missile (ICBM) leg of the triad is approaching 50 years, and the Navy's *Ohio*-class submarines carrying the sea-launched ballistic missile (SLBM) leg of the triad are approaching 40 years. Given the age of these systems that are fundamental to the continued success of the triad, urgency is growing to modernize these nuclear forces. This imperative is exacerbated by the fact that Russia and China have been actively fielding several new nuclear systems, to include new land-based strategic missiles, new strategic missile submarines, new sea-based strategic missiles, improved weapons for their bombers, and multiple ground, sea, and air-launched tactical nuclear weapons. To date, these threats have grown in the absence of any American response in kind.

While the modernization of the systems that make up the nuclear triad are currently planned and now under debate, the fundamental underpinning for their success tends to get little attention. Specifically, the nuclear command, control, and communications (NC3) system that allows positive control of these weapons in peace and, if necessary, in war is a crucial modernization requisite. It is these systems that define an architecture that coalesces in a coherent fashion all the activities, processes, and procedures performed by military commanders and support personnel that, through the chain of command, allow for senior-level decisions on nuclear weapons employment.

As a result of the highly classified nature of these activities, little has been written about the NC3 architecture. The intent of this study is to illustrate, in an unclassified setting, America's NC3 infrastructure in order to convey the absolute criticality of modernizing it. Only with a modernized NC3 system can we ensure that the U.S. retains a resilient and robust command and control architecture that is fundamental to the effectiveness of the nuclear triad. In this regard, the NC3 enterprise is truly the "fifth pillar" of the nation's overall nuclear modernization program—together with modernization of the triad's weapons systems, and the nuclear warhead stockpile itself. Simply put, when it comes to nuclear modernization, NC3 is the least expensive, yet perhaps the most critical.

Lt Gen David A. Deptula, USAF (Ret.)
Dean, The Mitchell Institute for Aerospace Studies
February 4, 2019

Abbreviations

ALCM	Air-Launched Cruise Missile
ALCS	Airborne Launch Control System
AEHF	Advanced Extremely High Frequency
AT&T	American Telephone and Telegraph Company
BMEWS	Ballistic Missile Early Warning System
CJCS	Chairman of the Joint Chiefs of Staff
COG	Continuity of Government
DOD	Department of Defense
DEW	Distant Early Warning
DSP	Defense Support Program
DSCS	Defense Satellite Communication System
EHF	Extremely High Frequency
ELF	Extremely Low Frequency
EMP	Electromagnetic Pulse
FAB-T	Family of Beyond-Line-of-Sight Terminals
GBSD	Ground-Based Strategic Deterrent
Global ASNT	Global Aircrew Strategic Network Terminal
GOC	Global Operations Center
GPS	Global Positioning System
HF	High Frequency
IBM	International Business Machines Corporation
ICBM	Intercontinental Ballistic Missile
IP	Internet Protocol
ITWAA	Integrated Tactical Warning and Attack Assessment
LCC	Launch Control Center
LRSO	Long-Range Standoff munition

MMPU	Minuteman Minimum Essential Emergency Communications Network Program Upgrade
NAOC	National Airborne Operations Center
NCA	National Command Authority
NC3	Nuclear Command, Control, and Communications
NMCC	National Military Command Center
NNSA	National Nuclear Security Administration
NORAD	North American Air Defense Command
NPR	Nuclear Posture Review
PEO	Program Executive Office
PNVC	Presidential and National Voice Conferencing
SAC	Strategic Air Command
SAGE	Semi-Automatic Ground Environment
SAOC	Survivable Airborne Operations Center
SBIRS	Space-Based Infrared System
SHF	Super High Frequency
SOCS	Strategic Operational Control System
SSBN	Fleet Ballistic Missile Submarine (Subsurface Ship, Ballistic-missile, Nuclear-powered)
TACAMO	"Take Charge and Move Out" aircraft
UHF	Ultra High Frequency
USNDS	U.S. Nuclear Detonation Detection System
U.S. STRATCOM	U.S. Strategic Command
VCJCS	Vice-Chairman, Joint Chiefs of Staff
VHF	Very High Frequency
VLF	Very Low Frequency

Executive Summary

The United States Department of Defense is now undertaking a long-overdue recapitalization of its strategic nuclear forces. The development and acquisition of replacement fleets of intercontinental ballistic missiles, ballistic missile submarines, long-range bombers, nuclear-armed air-launched cruise missiles, and the refurbishment of nuclear warheads for these systems receive great attention from Congress, policymakers, analysts, and the media. Yet these new platforms and weapons, as modern and capable as they will be, cannot provide convincing strategic deterrence unless the United States also possesses an effective and robust nuclear command, control, and communications (NC3) infrastructure. Possession of an effective and robust NC3 system, along with the nuclear weapon systems mentioned above, is essential for deterrence since its existence will convince potential adversaries that any attempted surprise nuclear aggression will fail and will be met with a devastating response.

An effective NC3 system performs five functions in support of decision-makers responsible for nuclear forces. The NC3 enterprise:

- Provides policymakers and commanders with current information on the status and readiness of nuclear forces;
- Allows prompt decision-making during a crisis and provides the basis for adjusting war plans as particular crisis situations may require;
- Collects information from a variety of sensors, warning systems, and intelligence sources to provide a comprehensive picture to policymakers and commanders;
- Provides the President and his subordinates with the capability to organize real-time conferences from multiple locations, during which they will assess emerging threats and consider response options;
- Provides for the positive authorized control and, if necessary, employment of nuclear weapons in both peacetime and combat.

A modern NC3 system is comprised of terrestrial and space-based sensors that monitor the globe for threats; a communications architecture that reliably transmits (under any conditions) relevant and accurate data to decision-makers; command and control support systems that provide reliable analyses of threats and response options for decision-makers; and ensures that weapon systems and their operators are always connected to authorized decision-makers. The NC3 system must always reliably transmit the President's orders through the chain of command to properly postured nuclear forces such that those nuclear orders are executed. Yet, the NC3 system must also ensure that nuclear weapons are never employed without proper authorization.

The existing NC3 system was designed in response to a specific threat, namely the Soviet Union's land-based and submarine-based ballistic missiles. The NC3 architecture received its last major upgrade in the 1980s, when the Soviet ballistic missile threat was reaching its peak intensity.

Since then however, the character and dispersion of nuclear threats to the United States have grown, but without commensurate adaptations of the NC3 system. Further, advances in technology, and the will of potential adversaries to employ this technology, have created threats to the NC3 system itself that were not present during the Cold War. These new threats include adversary capabilities to attack NC3 early warning and communication satellites in geosynchronous orbit; offensive cyber threats to systems that provide support to the NC3 architecture; and potential nuclear weapons effects on modern NC3 support systems.

In addition to these threats, the legacy NC3 system suffers from additional problems that in the years ahead could threaten its reliability during a crisis. Since the system has not received a comprehensive upgrade since the 1980s, many of its components could be categorized as "vintage," and are thus difficult to reliably maintain. Finally, the legacy NC3 system will need to reliably connect to the new generation of nuclear weapon platforms (new ballistic-missile submarines, intercontinental ballistic missiles, and long-range bombers) when these systems enter service in the decade ahead. But ensuring reliable communications between these new platforms and an NC3 system nearly a half-century removed from them could be problematic and will likely entail dangerous risks.

...the legacy NC3 system suffers from additional problems that in the years ahead could threaten its reliability during a crisis. Since the system has not received a comprehensive upgrade since the 1980s, many of its components could be categorized as "vintage," and are thus difficult to reliably maintain.

In July 2018, the Secretary of Defense and the Chairman of the Joint Chiefs of Staff designated the commander of U.S. Strategic Command (STRATCOM) as the "NC3 enterprise lead," with the responsibility and authority for the system's operations, modernization, design requirements, engineering, and integration. With this designation, the DOD now has a single four-star flag officer and combatant commander in charge of this much-needed modernization of the overall NC3 system.

Modernizing NC3 is an open-ended process that is likely to intensify over the next decade. Looming challenges for STRATCOM and DOD planners will include refining a modernized NC3 system design that responds to the future threat environment; secures the cooperation of stakeholders inside the government; incorporates into the new architecture best practices, especially, when appropriate, those from the private sector regarding cyber security; and obtains institutional and funding support from Congress.

When successful, a modern NC3 architecture will guarantee connectivity between the President and U.S. nuclear forces in even the direst scenarios. The Congress and officials in DOD can contribute to this outcome by supporting and overseeing STRATCOM as it undertakes this effort.

Introduction

The United States Department of Defense (DOD) is now undertaking a long-overdue recapitalization of its nuclear forces. The development and acquisition of a new long-range bomber (the B-21 Raider), a new air-launched nuclear-armed cruise missile (the long-range standoff munition, known also as the LRSO), a new intercontinental ballistic missile (the ground-based strategic deterrent—GBSD), and a new ballistic missile submarine (the *Columbia*-class) have received the most attention. Updating the nation's arsenal of nuclear warheads, another critical element of the modernization program, is also under way—a responsibility of the Department of Energy's National Nuclear Security Administration (NNSA).

Yet, these new platforms and weapons, as modern and capable as they will be, cannot provide convincing nuclear deterrence unless the United States also possesses an effective and robust nuclear command, control, and communications (NC3) infrastructure. Indeed, as important as the above-mentioned weapon programs are, Air Force Gen John Hyten, the commander of U.S. Strategic Command (STRATCOM), declared in testimony to Congress in March 2017 that the age of the current "ancient" NC3 system was his "biggest concern," and that modernizing NC3 is his "number one priority."[1] Simply put, no weapon, including nuclear forces, is useful unless decision-makers employing the weapon have the capabilities to detect threats, formulate plans, identify targets, issue orders, and assess the results of combat operations.

...new platforms and weapons, as modern and capable as they will be, cannot provide convincing nuclear deterrence unless the United States also possesses an effective and robust nuclear command, control, and communications (NC3) infrastructure.

An effective and robust NC3 system provides those functions, and under the most stressful conditions, namely while under nuclear attack. Possession of an effective and robust NC3 system, along with the weapons mentioned above, is essential for deterrence since its existence will convince potential adversaries that any attempted surprise nuclear aggression will fail and will be met with a devastating response.

This study will examine and explain why modernization of America's NC3 infrastructure is now a critical requirement for the DOD and why modernization should receive the full support of the Congress and the public. It will begin by explaining NC3, its functions, and its major components. Next, it will briefly explore the Cold War origins of the United States' NC3 system and how that legacy has led to today's NC3 architecture. The study will then discuss looming challenges the current NC3 system faces, as new threats to it emerge in the contemporary and future operating environment. A section on NC3 modernization tasks, priorities, and programs will follow, and it will conclude by summarizing findings and offer recommendations for policymakers to consider.

The goal of America's nuclear forces is to preserve peace and freedom by deterring potential adversaries from ever attempting large-scale aggression against the United States and its allies, and to use those

forces to reliably assure allies of protection under the umbrella of extended deterrence. Deterrence has succeeded in preventing nuclear and major-power conflict since 1945. The United States is now pursuing modernization of its nuclear deterrent. NC3 is the least visible and least costly component of the overall modernization program. Even so, NC3 modernization is no less critical than the weapons components of the strategic deterrence architecture, as it serves as the glue of the nuclear triad. This study will strive to explain why Congress and the public should support NC3 modernization and how Congress and DOD should organize that effort.

U.S. Air Force, U.S. Navy, Northrop Grumman

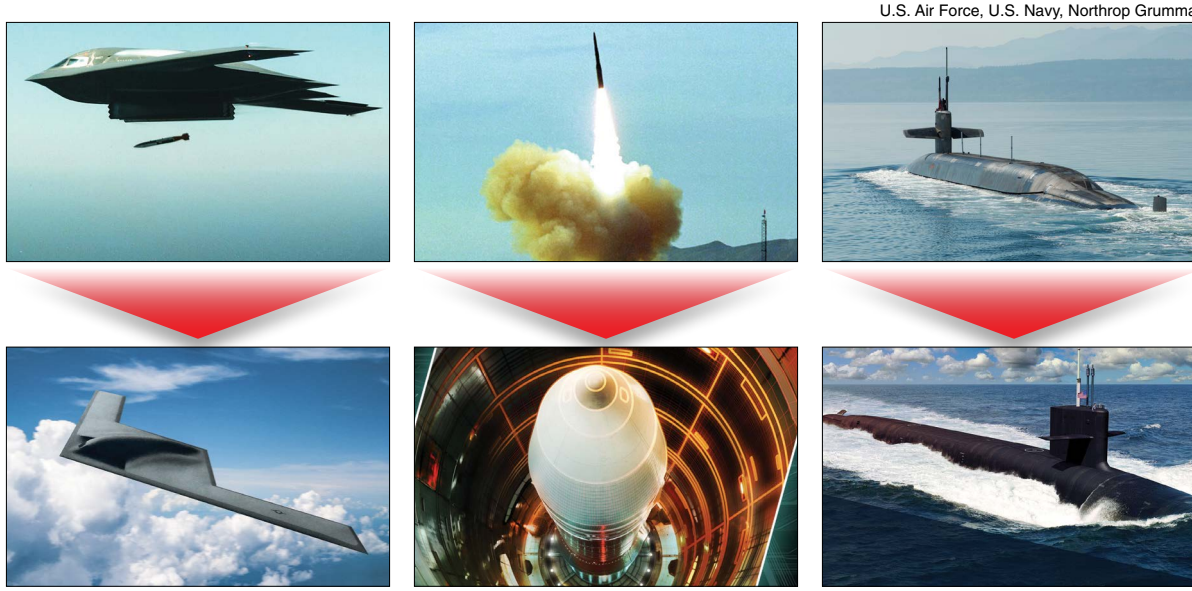


Figure 1: The United States is in the process of recapitalizing the nuclear weapon systems of all three legs of the nuclear triad. From left to right, the Air Force's B-2 stealth bomber will eventually be retired in favor of the B-21 Raider, the Minuteman III ICBM force will be replaced with the ground based strategic deterrent (GBSD), and the Navy's *Ohio*-class submarines will be replaced with a new fleet ballistic missile submarine, the *Columbia*-class. Effective and robust NC3 infrastructure, however, is vital to the success of all three triad legs.

What is NC3?

Definitions

NC3 exists to provide assured command and control of U.S. nuclear forces. The DOD defines nuclear command and control as:

> *"Exercise of authority and direction by the President, as commander in chief through established command lines over nuclear weapon operations of military forces, as chief executive over all government activities that support those operations, and as head of state over required multinational actions that support those operations."*[2]

The NC3 system provides the President and his subordinates (the National Command Authority, or NCA) with the command capabilities they need to exercise this authority. The DOD defines nuclear command, control, and communications as:

> *"Facilities, equipment, communications, procedures, and personnel that enable presidential nuclear direction to be carried out."*[3]

The nuclear command and control system is a multi-agency enterprise with numerous stakeholders across the federal government. The DOD is responsible for the central communications infrastructure within the overall NC3 system.[4]

NC3 Functions

The NC3 system and its operators carry out five functions during the exercise of nuclear command and control. The effective exercise of all five functions is necessary to ensure the unquestioned command and control of nuclear forces.[5]

The nuclear command and control system is a multi-agency enterprise with numerous stakeholders across the federal government.

Force Management includes the assignment, training, deployment, maintenance, and logistics support of nuclear forces and weapons before, during, and after any crisis. NC3 provides policymakers and commanders with current information on the status and readiness of nuclear forces so that these decision-makers can make accurate and timely decisions during a crisis.

Planning involves the development and modification of plans for the employment of nuclear weapons and other operations in support of nuclear employment. Nuclear planning allows prompt decision-making during a crisis and provides the basis for adjusting war plans as particular crisis situations may require.

Situation monitoring comprises the collection, maintenance, assessment, and dissemination of information on friendly forces, adversary forces and possible targets, emerging nuclear powers, and worldwide events of interest. Situation monitoring collects information from a variety of sensors, warning systems, and intelligence sources to provide a comprehensive picture to policymakers and commanders.

Decision-making refers to the assessment, review, and consultations that occur when the employment or movement of nuclear weapons is considered for the execution of nuclear control orders. NC3 must provide the President and his subordinates with the capability to organize conferences during which they will assess emerging threats and consider response options. These conferences may include policymakers and military commanders of U.S. allies around the world.

Force direction entails the transmission and implementation of decisions for the authorized employment of nuclear weapons and the termination of their employment. Force direction also applies to the movement of nuclear weapons and orders for nuclear weapons to be disabled and dismantled. NC3 ensures positive authorized control of nuclear weapons in both peacetime and combat.

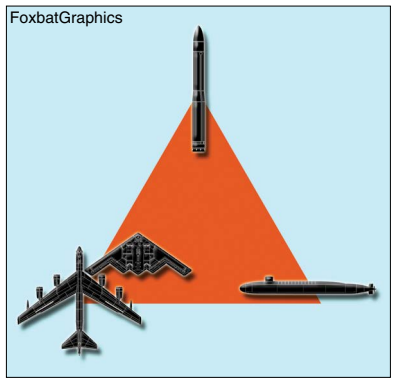


Figure 2: The primary weapon systems of the U.S. nuclear triad (clockwise from bottom left): the B-52 and B-2, the Minuteman II ICBM, and the *Ohio*-class ballistic missile nuclear submarine.

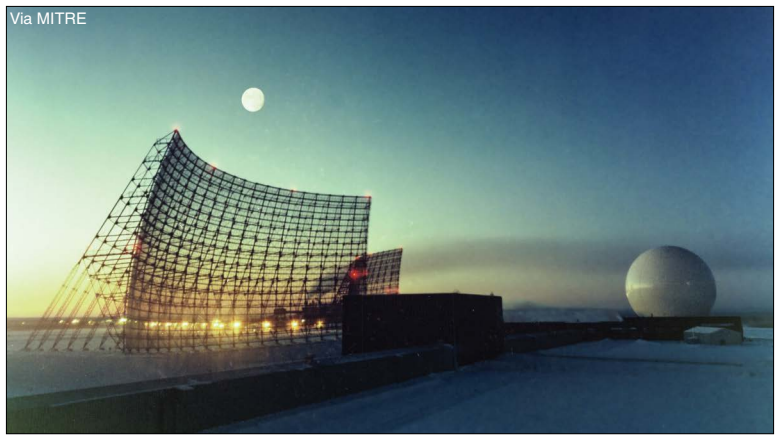
NC3 Subsystems

The NC3 system is a collection of subsystems that together carry out the five NC3 functions described above. Four main subsystems comprise the overall NC3 system.

Sensors, such as infrared detection satellites and ground-based long-range radars, perform the situation-monitoring function. Examples of sensors that support NC3 include the space-based infrared system (SBIRS) satellite constellation that detects ballistic missile launches and the ballistic missile early warning system (BMEWS), three large long-range radars located in Alaska, Greenland, and the United Kingdom, that detect, track, and classify ballistic missile targets.[6]

Transport, NC3's communications backbone, moves data to intelligence processing facilities, to and among decision-makers, transmits orders to nuclear combat forces, and transmits the results of nuclear combat action back to decision-makers. The data transport system encompasses a myriad of terrestrial landlines and relay stations, airborne command posts, and communication satellites. These components range in sophistication from the simple telephone, to radio frequency systems, to government and non-government satellites. Some of these systems are expected to be able to operate through nuclear effects, while others are expected to be subject to nuclear effect disruption for periods ranging from minutes to hours.[7]

Command and control consists of decision-makers such as the President and his various advisers, plus subsystems that integrate and correlate data during a crisis, providing assessments for decision-makers



Via MITRE

Left: The ballistic missile early warning system (BMEWS) radar installation at Thule Air Base, Greenland, pictured here during the early 1960s. The BMEWS was a crucial sensor for the U.S. NC3 network to detect, track, and classify ballistic missiles during the Cold War, and is still in operation today.

to evaluate while they contemplate response orders to military units. The integrated tactical warning and attack assessment system (ITWAA) is an NC3 subsystem that supports both the situation monitoring and decision-making functions of NC3. ITWAA provides decision-makers with unambiguous, reliable, accurate, timely, survivable, and enduring warning information of ballistic missile, space, and air attacks on North America.[8]

Finally, *shooters* receive emergency action messages through the chain of command from the President and, with proper authorization, deliver nuclear effects on adversary targets. Crews operating long-range nuclear-capable bomber aircraft (the B-52 and B-2), the Minuteman III intercontinental ballistic missile (ICBM) force, the *Ohio*-class ballistic missile submarine fleet armed with the Trident II missile, and dual-capable fighter aircraft armed with the B61 nuclear gravity bomb would receive and execute these nuclear emergency action orders. The NC3 system must ensure that these weapons platforms are always connected through the chain of command to the President, regardless of their location, the background conditions, or the location of the President.[9]

SSgt Roidan Carlson/USAF

Above: An unarmed AGM-86B air-launched cruise missile (ALCM) is launched from a B-52H during a nuclear weapons system evaluation sortie over the Utah Test and Training Range, September 22, 2014. The test was part of a system-wide operational nuclear evaluation of 8th Air Force bombers.

Requirements for an Effective NC3 System

An effective NC3 system must detect an incipient surprise attack on the United States or its allies, assess and characterize that attack, immediately transmit that analysis of the attack to the President and his advisers, accurately report to the President and his advisers the status and availability of U.S. nuclear forces, support a decision-making conference of the President and his advisers, and then transmit the President's orders to U.S. nuclear forces through the chain of command to military servicemembers operating nuclear-capable platforms, weapons, and support systems. During a crisis, it may be necessary for the President and U.S. military commanders to communicate with the policy and military leaders of American allies. The NC3 system must securely and reliably support real-time conferencing with certain foreign governments and military forces.

The NC3 system must accomplish all these tasks under the direst circumstances. Accordingly, the U.S. NC3 system must be "reliable, assured, enduring, redundant, unambiguous, survivable, secure, timely, flexible, and accurate," even when the NC3 system itself is under nuclear or other forms of attack.[10] Mission-critical NC3 subsystems must function through nuclear blast effects such as extreme shock, heat, radiation, scintillation of the electromagnetic background, and the damage that electromagnetic pulses (EMP) can cause to electronic components. In addition, some aspects of a modernized NC3 system will have to operate with internet protocol (IP) features, which means that these and connected elements of the NC3 infrastructure will have to be resistant to cyber tampering and interference.[11]

The U.S. NC3 system must assure the achievement of two outcomes that are in opposition to each other, and thus greatly increase demands on the system. The NC3 system must always reliably transmit the President's orders to nuclear forces such that those nuclear orders are executed. Yet, the NC3 system must also ensure that nuclear weapons are never employed, targeted, or postured without proper authorization. Various safeguards such as nuclear weapon safety features, authentication coding, coded firing locks, and the "two-person rule" are examples of procedural and design aspects of nuclear safety and surety. The "always/never" feature of NC3 is a critical and enduring design requirement and must be addressed as the system is modernized.[12]

SrA Jason Wiese/USAF

Left: Air Force 1st Lt Pamela Blanco-Coca, 319th Missile Squadron commander, and her deputy, 2nd Lt John Anderson, simulate key turns for a Minuteman III ICBM in a F.E. Warren AFB, Wyoming launch control center February 9, 2016. The "two-person rule" for an ICBM launch is a key element of U.S. nuclear safety and surety practices, features, and authentication processes.

Finally, NC3 system design requirements must account for times and places where NC3 subsystems rely on civilian infrastructure for necessities such as electrical power, water, transportation nodes and features, civilian communication facilities and pathways, civilian satellites and space-link ground stations, civilian computer server farms and "cloud computing" infrastructure, and other such non-military support to the defense establishment. The NC3 system must be designed to function when supporting civilian infrastructure is impaired or disabled.

Potential adversaries of the United States and its allies also must know that American NC3 will be "reliable, assured, enduring, redundant, unambiguous, survivable, secure, timely, flexible, and accurate" regardless of any action they may take against the system...

NC3's Contribution to Deterrence

These requirements provide assurance to the NCA and nuclear force commanders that U.S. nuclear forces will be responsive to the gravest threats regardless of conditions. But it is not only American policymakers and commanders who need this assurance. Potential adversaries of the United States and its allies also must know that American NC3 will be "reliable, assured, enduring, redundant, unambiguous, survivable, secure, timely, flexible, and accurate" regardless of any action they may take against the system, to include the most severe nuclear or cyber attacks. To prevent enemy tampering or disruption, most technical aspects of U.S. NC3 must remain classified. Yet at the same time, U.S. policymakers and commanders must convince adversaries that any disruption of the overall system will always be beyond their grasp. Modernizing NC3 will contribute to this deterrence function.

History of U.S. NC3

The Soviet Bomber Threat

On August 29, 1949, the Soviet Union successfully tested its first atomic device at a test range in eastern Kazakhstan. Before that test occurred, it had become clear to policymakers in the United States and Western Europe that the West was in a geostrategic competition with the Soviet Union. The Soviet atomic test, combined with a buildup in its long-range bomber force, signaled the potential threat of a widespread surprise nuclear attack on the American homeland and allied targets in Europe.[13] Yet U.S. policymakers and military commanders found that they lacked the critical elements of an NC3 system capable of performing the five NC3 functions discussed earlier in this study.

In 1949, the United States lacked radars capable of detecting Soviet bombers approaching at low altitudes. Early warning of an attack at that time was limited to observers equipped with binoculars.[14] Recognizing the threat posed by Soviet nuclear-armed bombers and the need for early warning of a potential attack, the U.S. and Canadian governments began construction in February 1955 of 57 radar stations stretching from Alaska's Aleutian Islands, across Canada, and then to Greenland. The distant early warning (DEW) Line was completed in about two and half years and was the first example of the "situation monitoring" function of the still-embryonic NC3 system.[15]

TSgt Donald L. Wetterman/USAF

Above: Radar station LIZ-2 at Point Lay, Alaska, one of 30 Air Force stations on the distant early warning (DEW) Line. A Cold War-era network of radars to detect low-flying Soviet bombers, the DEW Line stretched some 3,600 miles from Alaska to Greenland.

Communicating with the Air Force's Strategic Air Command (SAC) bombers in the 1950s was equally embryonic. SAC bombers were the backbone of the Eisenhower Administration's "massive retaliation" nuclear deterrence strategy. Yet the system to communicate with SAC's bomber bases to order a retaliatory strike was primitive and fragile. SAC entered into a contract with the American Telephone and Telegraph Company (AT&T) to develop the strategic operational control system (SOCS) that aimed to link SAC headquarters with its far-flung bomber bases. AT&T provided connectivity to SAC on an "on call" basis, which required up to 30 minutes to establish a connection from headquarters to the bases. SAC messages were limited to 100 words per minute and could not be encrypted. Although state-of-the-art at the time, SOCS did not meet SAC operational requirements.[16]

The Soviet Missile Threat

Before the concrete had cured on the last DEW Line radar station, the Soviet Union again stunned the U.S. and its allies. In August 1957, the Soviets launched *Sputnik I*, the first man-made satellite placed into orbit. *Sputnik II* followed on November 3, 1957, and weighed about a half a ton, as large or larger than a nuclear weapon. Soviet possession of an intercontinental-range ballistic missile (ICBM) added a new threat to the United States homeland, capable of far greater speeds than a bomber. Soviet ICBMs could reach targets in the United States in about 30 minutes. Worse, the DEW Line radars were not suited to detect Soviet missiles. Work soon began on the three ballistic missile early warning radars (BMEWS) mentioned in the previous section. But until these were operational, the U.S. would have no warning of a potential Soviet missile attack.[17]

To enhance the growing NC3 system's situation monitoring capacity and to provide redundancy, the U.S. government looked to space as a domain for early warning. In November 1970, the DOD launched the first defense support program (DSP) ballistic missile early warning satellite. DSP satellites use infrared detectors to identify and track the launch of ballistic missiles.[18] Data from DSP and, later, SBIRS satellites, combined with data from BMEWS radar and other intelligence monitoring to provide the overall NC3 system with comprehensive situation monitoring.

Right: An artist's rendering of a defense support program (DSP) ballistic missile early warning satellite. By the 1970s, the U.S. looked to space for extra monitoring capacity and redundancy for NC3 system.

Computers Join NC3

As the DOD built the DEW Line radars and organized fighter-interceptor squadrons to respond to possible raids of Soviet bombers, planners realized that they did not have an adequate system for organizing the incoming data from the radars and aircraft that would be needed to mount a coordinated and effective response to a large Soviet attack. Through an agreement with the Canadian government, the DOD stood up the North American Air Defense Command (NORAD) in 1957, and placed its headquarters in Colorado Springs, Colorado.[19]

NORAD needed a command and control system capable of tracking potentially hundreds of Soviet bombers and organizing a response with fighter-interceptors and surface-to-air missiles. An early NORAD project was the semi-automatic ground environment (SAGE), a state-of-the-art centralized command and control system developed by the MITRE Corporation that linked early warning radars such as the DEW Line directly to anti-aircraft missiles and fighter-interceptors based around the United States and Canada. SAGE consisted of 24 direction centers that would receive data from the sensors and coordinate the responses of U.S. and Canadian missiles and aircraft.[20] Each direction center housed a pair of AN/FSQ-7 computers, the first mainframes produced by the International Business Machines Corporation (IBM). They were the fastest and most expensive computers at the time, with each containing about 25,000 vacuum tubes and resting on a half-acre of floor space.[21]

The groundbreaking SAGE system relied on AT&T's telephone lines to transmit sensor data from the radars to the SAGE command centers, and from those centers to the air defense missile and aircraft bases. Officers in the military chain of command would decide whether to fire the system's weapons. But those decisions would be framed by the data and analyses produced by SAGE.[22]

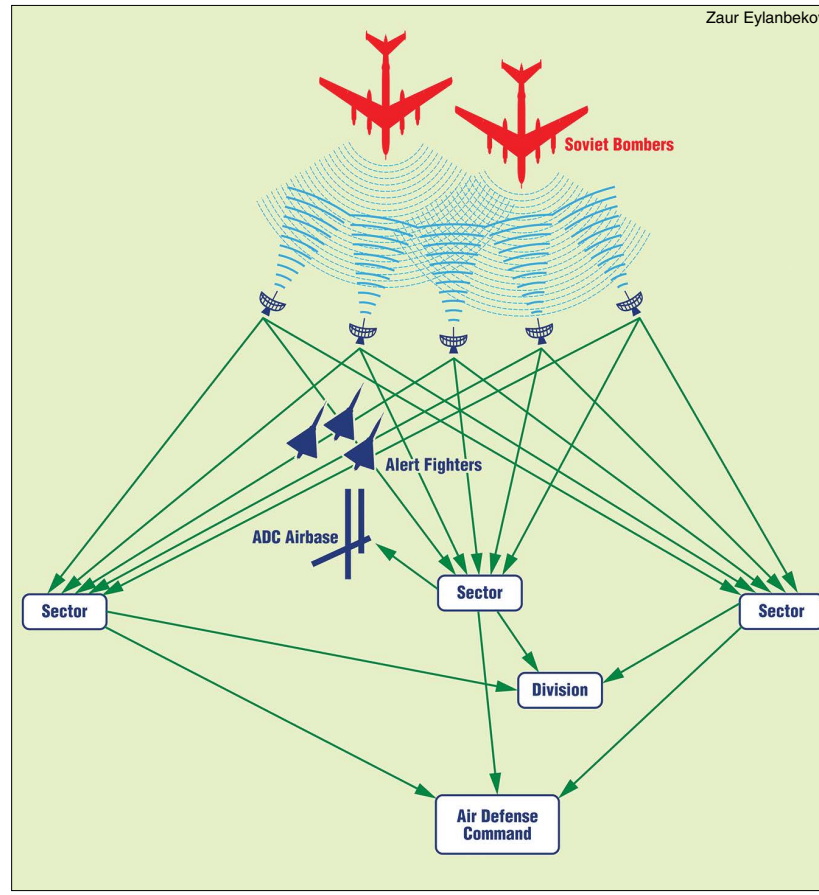


Figure 3: A diagram of the semi-automatic ground environment (SAGE) air defense command and control system, constructed during the Cold War to help organize and track the large volumes of radar data required to effectively respond to a Soviet bomber attack.

SAC was soon linked to NORAD and received its data and analyses. SAC planners also decided that they needed their own computerized command and control system, along with a much more speedy and reliable data transmission system for distributing attack orders to subordinate bomber and missile units dispersed around the world. In the 1960s, SAC built a massive underground command post at its Offutt Air Force Base headquarters near Omaha, Nebraska, consisting of three underground levels and housing for 800 people. The command center hosted state-of-the-art computers, communications equipment, and displays that projected the near-real-time status of SAC operations on a wall 20 feet high and nearly 50 yards wide.[23]

USAF

Above: Strategic Air Command's Cold War-era underground command post at Offutt AFB, Nebraska. The facility consisted of three underground levels, and housing for around 800 people.

Coping With "Decapitation"

In January 1961, in his first week as Secretary of Defense, Robert McNamara received a briefing from the DOD's weapon systems evaluation group on the status and vulnerabilities of the country's NC3 system. The briefing, from the group's *Report No. 50*, revealed how easy it would be for a Soviet surprise attack to destroy top leadership targets in the United States, potentially disrupting an effective response against Soviet targets. The report estimated that just 35 Soviet missiles could, with 90 percent probability, kill the U.S. government's top leaders and destroy the American nuclear command and control system.[24] McNamara and other government officials soon concluded that the need for an improved nuclear command and control system was beyond dispute, and "a matter of transcendent priority."[25]

American defense planners turned to coping with a potential "decapitating" strike that could potentially kill the President and top leaders before they could organize a response to an attack. In response to the sobering DOD assessment, planners began work on "continuity of government" (COG) preparations. Examples of COG facilities and plans included an alternate underground National Military Command Center (NMCC) located in the mountains of western Maryland; airborne command posts for use by the President, his advisers, and the commanders of SAC and Navy fleets operating missile submarines; an underground command bunker for other government functions located in rural Virginia; procedures for identifying and swearing in a new President should top officials die in a surprise decapitation attack; the buildout of redundant communication networks to ensure connectivity with surviving U.S. nuclear forces after an enemy nuclear attack; and elaborate procedures and exercises to implement COG plans.[26]

In the early 1960s, the Air Force implemented two critical, yet controversial, programs aimed to dissuade Soviet leaders who thought they could win a nuclear war with a surprise attack. Operation Looking Glass consisted of an EC-135 airborne command post manned by a general officer and his battle staff, that would operate aloft continuously. In case of a successful decapitation strike, the Looking Glass staff and aircraft was equipped to transmit war orders to U.S. nuclear forces. After three decades of continuous operations, Looking Glass flew for the last time in 1991. The second program was Operation Chrome Dome, which featured a force of nuclear-armed B-52 bombers constantly in the air, ready for orders to attack the Soviet Union. Five crashes of nuclear-armed Chrome Dome aircraft forced McNamara to cancel the program in 1968.[27]

Preparing NC3 for a Long War

By 1980, the DOD had added two long-range PAVE PAWS radars to an early warning network that then consisted of the three north-facing BMEWS radars and the constellation of DSP infrared ballistic missile launch detection satellites. The PAVE PAWS radars, located in California and Massachusetts, pointed out to sea to detect the launch of Soviet submarine-launched ballistic missiles. A third radar located in Florida,

Below: An Air Force EC-135C Looking Glass aircraft, at Offutt AFB, Nebraska. In the 1960s, the EC-135 Looking Glass served as a dedicated airborne command post operating continuously, able to transmit orders to U.S. nuclear forces in the event of a "decapitation strike" on the President.

Library of Congress

FPS-85, would detect possible missile launches from the Caribbean and other points south.[28] Analysts at that time concluded that the U.S. NC3 system was vulnerable to disruption, which reduced the credibility of the country's overall nuclear deterrent. NC3 vulnerabilities in 1980 included:

1. Excessive concentration of NC3 facilities such as radars and command centers in too few fixed locations, which were known to adversaries and were vulnerable to missile attack or sabotage.

2. The emergence of a Soviet anti-satellite capability that could threaten certain reconnaissance and communication relay satellites in low-earth orbit.

3. The limited time available for the President, his advisers, and nuclear force commanders to make decisions, especially in the case of a surprise attack. For example, when Soviet ballistic missile submarines began operating in the Atlantic Ocean, Washington, DC, became vulnerable to destruction with less than 15 minutes of warning.

4. A nuclear weapons detonation in the atmosphere above the United States could potentially threaten the American power grid and cause widespread damage to some electronic components due to EMP effects. In addition, atmospheric nuclear explosions can disrupt radio transmissions to command posts and nuclear forces in the field by creating scintillating interference to the electromagnetic spectrum.

5. Potential Soviet jamming of U.S. radio communication networks.[29]

These vulnerabilities, created in part by the arrival of Soviet ballistic missile submarines and by the increasing accuracy of ballistic missiles, compounded the concerns officials had about the United States' NC3 system. Indeed, in Congressional testimony delivered in early 1979, William Perry, then-undersecretary of defense for research and engineering, stated that NC3 was "perhaps the weakest link in our strategic forces today."[30] Policymakers and analysts during the Carter and Reagan-era nuclear reform period considered two objectives for modernizing the NC3 system of the time. The first objective called for improving the capability and redundancy of NC3 to survive a surprise attack, and to provide a more thorough and detailed assessment to policymakers on the size, targets, and characteristics of a potential large Soviet surprise attack. Achieving this objective for NC3 called for additional ground and spaced-based sensors and new radios that would provide redundant communication channels to nuclear forces.[31]

Left: The PAVE PAWS radar installation at Beale AFB, California. These radars, located in the continental U.S. at Beale and at Cape Cod Air Force Station, Massachusetts, were developed to detect and characterize a sea-launched ballistic missile attack.

The second objective of NC3 modernization in the late 1970s and early 1980s was to improve the endurance and survivability of the NC3 system, such that the United States would be capable of fighting a less intense but potentially long-lasting nuclear conflict that could stretch over weeks, months, or even years. Beginning in 1961, U.S. policymakers and war planners sought to add limited war options to the massive one-time nuclear retaliatory response in place since the Eisenhower Administration. But in spite of the desire for more flexible and limited response options, planners and commanders were not confident the U.S. NC3 system could survive an initial Soviet strike and function through a drawn-out, limited nuclear war.[32] Work on this second objective sought to solve this problem. It placed less emphasis on investment in more sensors and more emphasis on mobile ground command posts, more mobile and hidden facilities for supporting dispersed command and control, and capabilities to reconstitute global communications networks.[33]

Beginning in 1961, U.S. policymakers and war planners sought to add limited war options to the massive one-time nuclear retaliatory response in place since the Eisenhower Administration.

Alarmed by a fragile NC3 system it concluded was inflexible and vulnerable, the Reagan Administration aggressively modernized NC3 infrastructure in pursuit of both objectives described above. The Reagan-era defense program added redundancy to early warning sensors and communication networks. But the program also included capabilities that would allow the NC3 system to survive an attack and that would allow decision-makers to maintain command and control of nuclear forces for a possible nuclear war lasting weeks and months.[34]

NC3 equipment and capabilities added during this period included greater protection against EMP, deployment of the global positioning system (GPS) satellite constellation, upgrades of the command centers at SAC headquarters and the alternate NMCC, new terrestrial antennas for communicating with submerged submarines, new mobile command posts housed in tractor-trailer trucks to provide additional redundancy to the airborne command posts, and a greatly expanded role for the Vice President in nuclear and continuity-of-government planning.[35]

NC3 Today

Using open sources, the following is an overall unclassified description of the current U.S. NC3 system for the purposes of this study. Classified elements and descriptions of the system are not included here.

Sensors

Radars, such as BMEWS, and satellite constellations, such as SBIRS and DSP, continue as the basic tactical warning systems of the NC3 enterprise. Compared to the 1970s-vintage DSP infrared missile launch detection technology, SBIRS provides much greater clarity, position refinement, and tracking capabilities. In addition, newer models of GPS satellites include the U.S. nuclear detonation detection system (USNDS), a network of sensors that detects and precisely locates nuclear explosions that would occur on the earth's surface or in the atmosphere.[36] The confirmation and location of nuclear detonations, both those on the United States and those occurring elsewhere, including against adversaries, is critical information for policymakers and military commanders responsible for making decisions during a hypothetical nuclear campaign. The satellite communication networks discussed in the next section are also a key channel for transmitting nuclear battle damage information—both friendly and adversary—to key decision-makers.

Investments since the 1970s in additional airborne and satellite-based communications capabilities and waveforms have provided redundant links to nuclear forces that could be critical in an emergency.

Transport

Investments since the 1970s in additional airborne and satellite-based communications capabilities and waveforms have provided redundant links to nuclear forces that could be critical in an emergency. In addition, the employment of new waveforms to communicate with nuclear forces provide radio pathways that are less susceptible to interference during a nuclear warfare environment. These radio waveform links supplement the NC3 system's extensive landline and undersea data cables and transmission nodes.[37]

For example, radio transmissions in the extremely high frequency (EHF) and super high frequency (SHF) bands of the electromagnetic spectrum are less susceptible to electromagnetic blackout caused by atmospheric nuclear detonations. In addition, transmissions in the EHF and SHF bands are more difficult for adversaries to jam and can have higher data rates compared to transmissions in the very high frequency (VHF) and ultra-high frequency (UHF) bands traditionally used by commercial and military radios.[38] Two U.S. Air Force satellite constellations exploit these characteristics. The defense satellite communications system (DSCS) operates in the SHF band and provides nuclear-hardened, jam-resistant links to the NC3 system. The advanced extremely high frequency satellite system (AEHF) provides NC3 with the same capability in the EHF band.[39] The President and nuclear force commanders can use the satellite-based EHF and SHF bands to communicate attack orders to bomber and ICBM crews.[40]

Left: An artist's rendition of a satellite in the advanced extremely high frequency (AEHF) system, which provides survivable, global, secure, protected, and jam-resistant communications for U.S. leadership, such as nuclear emergency action messages.

Communicating nuclear emergency action messages to submerged ballistic missile submarines requires transmissions on the opposite end of the radio spectrum, namely the very low frequency (VLF) band. Underground ICBM launch control centers (LCCs) also have secure receive capability in this area, in both emergency network message processing mode and high data rate mode. The U.S. NC3 system's airborne command posts (discussed next) have the capability to communicate to submerged submarines over these bands, providing redundancy to terrestrial VLF transmission facilities that are highly vulnerable to disruption during a nuclear attack. Submerged submarines can also extend a tethered radio buoy to the surface. Antennas on these buoys can receive attack orders over the SHF and EHF bands from the DSCS and AEHF satellites.[41]

Command and Control

Current NC3 command and control facilities consist of a redundant combination of terrestrial and airborne command posts, each fitted with equipment to access the data and message transport systems described above.

The primary terrestrial NC3 command facility is the National Military Command Center (NMCC), located in the Pentagon. The NMCC is staffed continuously and provides intelligence and communication support to the President, Secretary of Defense, and the Chairman of the Joint Chiefs of Staff (CJCS).[42] An alternate NMCC is located underground in western Maryland.[43] STRATCOM, located at Offutt Air Force Base, Nebraska, operates the global operations center (GOC), which continuously monitors the global strategic situation and maintains communication links with all U.S. nuclear forces.[44]

Should the major terrestrial NC3 command facilities come under attack, decision-makers would employ airborne command posts to disperse, while maintaining contact with each other and with deployed nuclear forces.

Right: An Air Force Global Strike Command E4-B is refueled by a KC-10 during a sortie June 12, 2017. The E-4B fleet provides a highly survivable emergency backup NC3 command center to direct U.S. forces from and coordinate actions with civil authorities.

Above: A U.S. Navy E-6B Mercury command and control aircraft photographed during a testing sortie at Edwards AFB, California in early 2017. The airborne command post aircraft is equipped with satellite communication equipment to link the aircraft with the President and the other operational legs of the nuclear triad.

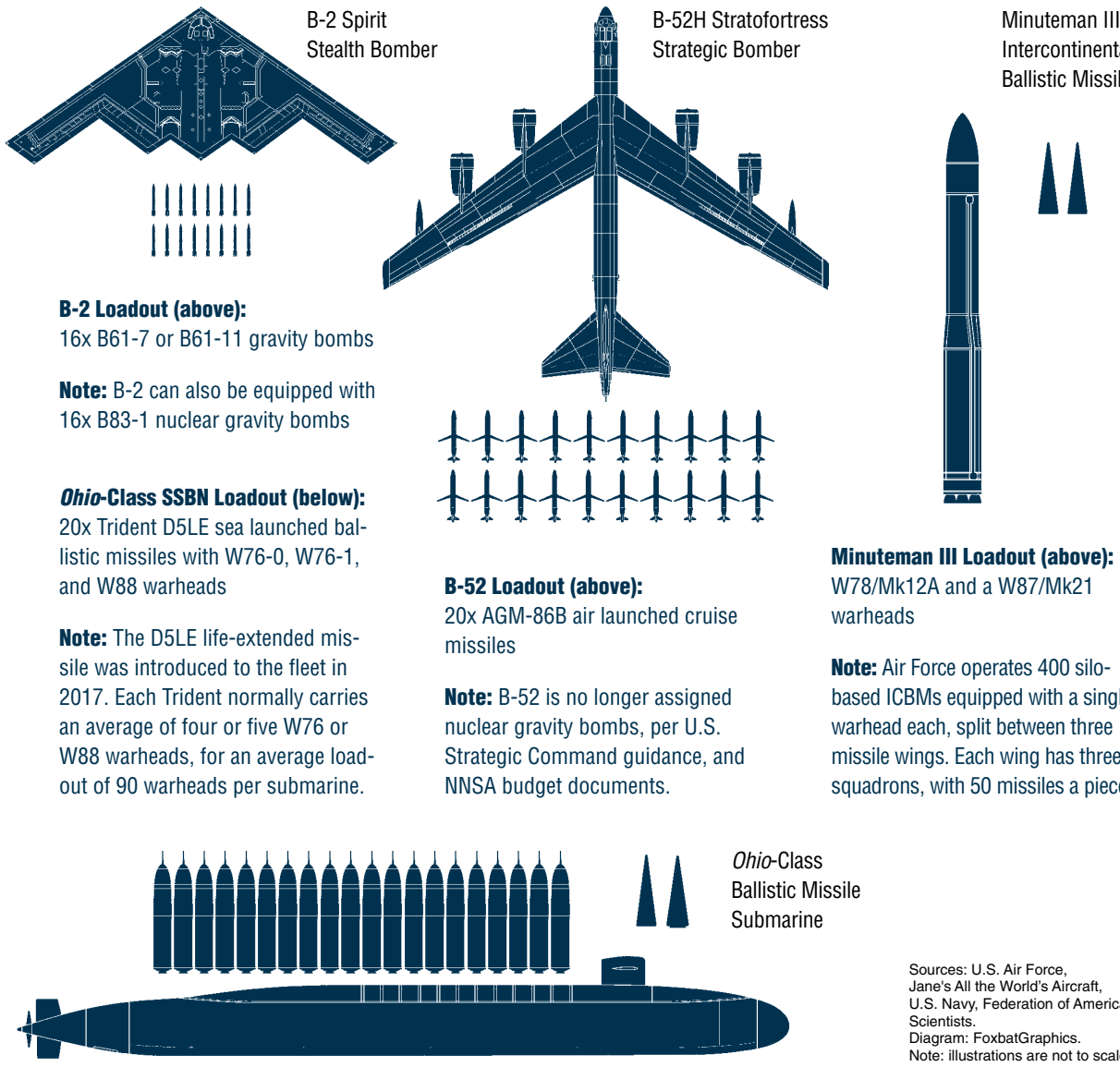
The U.S. Air Force maintains a fleet of E-4B national airborne operations center (NAOC) aircraft, at least one of which is ready from random locations to launch within minutes. NAOC is a heavily modified Boeing 747 aircraft that is hardened against EMP, can communicate to nuclear forces on all NC3 radio bands, and can carry a mission and flight crew of up to 112 persons.[45] The NAOC functions as a backup to the NMCC, supporting the President, the Secretary of Defense, CJCS, and their advisers during an emergency.[46]

The U.S. Navy operates a fleet of E-6B Mercury command and communication aircraft. The E-6, a modified Boeing 707, was originally configured for the TACAMO or "take charge and move out" mission, providing airborne connectivity to the Navy's ballistic missile submarine fleet. By 2003, all E-6s were upgraded to the B model, which provided the aircraft with workspaces for the STRATCOM battle staff, plus equipment to connect to all U.S. nuclear forces. The E-6B is equipped with the airborne launch control system (ALCS), which permits commanders onboard the aircraft to directly launch U.S. ICBMs. The E-6B is also equipped with a suite of satellite communication equipment to communicate with the President and with U.S. Air Force bombers. The E-6B can extend an antenna up to five miles behind the aircraft to communicate on the VLF and ELF bands with submerged ballistic missile submarines, and ICBM LCCs in unencrypted and secure modes.[47] Thus, the E-6B functions as an airborne backup to STRATCOM's global operations center. Should the underground GOC in Nebraska be threatened, the commander of STRATCOM and his staff can quickly launch in a waiting E-6B and maintain communications with the President, as well as with deployed nuclear forces.[48]

Shooters

The "shooters" of the U.S. nuclear deterrent consist of missile-carrying submarines, land-based intercontinental-range missiles, and bomber aircraft armed with either gravity bombs or cruise missiles. The U.S. Navy operates 14 *Ohio*-class fleet ballistic missile submarines (SSBNs). Based at Bangor, Washington, and King's Bay, Georgia, each SSBN carries 20 Trident II D5 ballistic missiles. On average, the *Ohio*-class submarines spend 77 days at sea, followed by 35 days in port. Each SSBN has two crews, which alternate manning the submarine and taking it on patrol.[49] Each Trident II D5 missile carries multiple independently targeted W76 or W88 nuclear warheads.[50] As mentioned above, the President and nuclear force commanders communicate with submerged SSBNs through VLF and ELF radio transmissions, or to an SSBN on the surface (or its radio buoy) on satellite-based UHF, EHF, or SHF bands.

Figure 4: Notional weapon loadouts for all three of the nuclear triad's primary "shooters."



Sources: U.S. Air Force, Jane's All the World's Aircraft, U.S. Navy, Federation of American Scientists.
Diagram: FoxbatGraphics.
Note: illustrations are not to scale.

The U.S. Air Force operates 400 Minuteman III ICBMs and maintains 450 protected underground launch silos for these missiles. Each Minuteman III carries a single W78 warhead, although the missile was armed with three warheads during the Cold War.[51] The President and commanders can transmit attack orders to launch crews over rapid, secure landline systems, MILSTAR (military strategic and tactical relay) satellites in the UHF, EHF, and AEHF spectrum, and survivable, secure radio communications in the VLF spectrum. Launch crews aboard E-6B aircraft can also initiate launches of Minuteman ICBMs by radio transmissions directly from the aircraft or relayed by satellite.

The U.S. Air Force also operates 46 nuclear-capable B-52H bombers and 20 nuclear-capable B-2 bombers. Nuclear armament for the B-52H consists of up to 20 air-launched cruise missiles (ALCMs).[52] Nuclear armament for the B-2 consists of up to 16 B61 or B83 nuclear gravity bombs.[53] The U.S. Air Force also operates F-15E aircraft that can deliver the B61 bomb from forward theater locations.[54] The President and nuclear force commanders would transmit attack orders to these aircraft over a long-range over-the-horizon high frequency (HF) band, from other aircraft or terrestrial relay points over the UHF band, or via satellite using the UHF or EHF bands.[55]

STRATCOM's current commander, Air Force Gen John Hyten, has described the existing NC3 system as "resilient, robust, and ancient."

STRATCOM's current commander, Air Force Gen John Hyten, has described the existing NC3 system as "resilient, robust, and ancient."[56] Looking out 10 years, Hyten has expressed his concern that the current NC3 system will become increasingly fragile.[57] According to Hyten, current NC3 technology is vastly outdated and is becoming ever more difficult to maintain.[58] It has now been three decades since the U.S. government comprehensively modernized its NC3 system.[59] As the next section of this study will explore, the NC3 system faces increasing challenges. Modernization is crucial if U.S. NC3 is to remain robust and reliable in the security environment of the future, and it must keep pace with all weapon system modernization efforts.

Legacy NC3 Faces the Future Operating Environment

As highlighted earlier, it has been three decades since the U.S. government has comprehensively modernized its NC3 system. Since then, changes in technology, new threats, and looming changes in the operating environment are exerting stresses on the reliability and security of the legacy NC3 system. The current NC3 architecture was designed to face the threat posed by the Soviet Union's ballistic missiles forces. By contrast, current and future threats come from a much longer list of potential adversaries and attack vectors, each providing unique challenges to effective command and control.[60]

In addition, the DOD is undertaking urgently required modernization of all nuclear "shooter" platforms—ballistic missile submarines, ICBMs, long-range bombers, and dual-capable theater-range strike aircraft. The NC3 system will require modernization to support the command and control of the next generation of nuclear weapon systems.

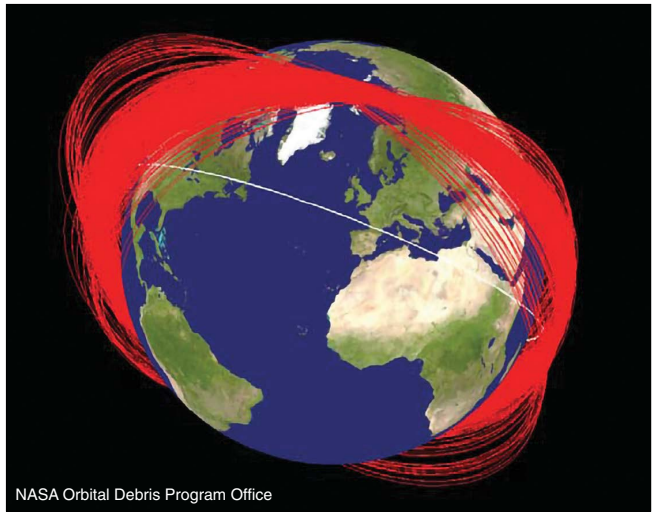
This section describes the challenges the future operating environment poses to U.S. NC3. It will also summarize the U.S. nuclear platform modernization program and the implication of that modernization for the NC3 system.

Threats to Space-Based NC3 Assets

During the Cold War both the United States and the Soviet Union developed capabilities to attack satellites in low-earth orbit. Attacking satellites in much higher geosynchronous orbits was at that time very technically challenging. In addition, policymakers on both sides tacitly recognized that designating the geosynchronous realm, where both sides maintained the most critical elements of their space-based NC3 assets as off limits to attack, would enhance mutual deterrence.

The number of state and non-state actors capable of space operations continues to grow, and the number of objects launched into all orbital regimes continues to expand. The addition of new players in space complicates decision-making for U.S. national security policymakers responsible for space operations.

Today, however, space, even in the geosynchronous realm, is no longer a sanctuary. Since 2011, the DOD has recognized space as increasingly congested, contested, and competitive.[61] The number of state and non-state actors capable of space operations continues to grow, and the number of objects launched into all orbital regimes continues to expand. The addition of new players in space complicates decision-making for U.S. national security policymakers responsible for space operations. Space congestion increasingly puts U.S. national security space assets at risk and has the potential to create radio interference for data transmitted to and from these assets. But most disturbing and profound is the end of space as a sanctuary domain—space is likely to be a battleground, with space assets vulnerable to attack.[62]



Left: Known orbit planes of *Fengyun-1C* debris, a Chinese weather satellite destroyed by an anti-satellite (ASAT) interceptor weapon in 2007. The white orbit signifies the International Space Station. China's development of ASAT weapons increasingly threatens space-based assets connected to the NC3 enterprise.

China has been a particularly aggressive developer of counterspace capabilities. In January 2007, China demonstrated a direct-ascent anti-satellite missile. That test destroyed a defunct Chinese weather satellite and created hundreds of pieces of space debris that will continue to orbit the earth and threaten other satellites for many years. On July 23, 2014, China performed another anti-satellite test, with a missile that repeated the 2007 trajectory without deliberately striking an orbiting object.[63]

Perhaps most disturbing was a Chinese missile test on May 13, 2013, that reached above 30,000 kilometers, or to geosynchronous height. The missile was not on a trajectory appropriate for deploying satellites into geosynchronous orbit and its payload did not attempt to do so. Nor was the trajectory useful for any scientific purpose. The U.S. DOD concluded that the most likely purpose for the launch was to test a counterspace capability against satellites in geosynchronous orbit.[64] Chinese geosynchronous counterspace capabilities place the major space-based components of the U.S. NC3 architecture at risk, such as the DSP and SBIRS early warning satellites, as well as NC3-related communication satellites such as MILSTAR, AEHF, and DSCS.

Cyber Security

Much of the U.S. NC3 infrastructure dates to the pre-internet era, before internet-protocol (IP) packet transmission became the dominant method of data communication. Thus, ironically, the NC3 system's age provides it with some protection against cyber intrusion and disruption. Hyten remarked in a 2018 interview that the U.S. NC3 system is "an old system. But it is very secure. If you want a cyber-secure system, build it in the 1960s."[65] Hyten also noted that U.S. NC3 is a closed network, specifically designed to be disconnected from outside networks.

Right: A SAGE control center during the Cold War. The U.S. NC3 system's age and "closed network" provides it with some protection against cyber attack, but as new equipment built on internet protocol (IP)-based subsystems is attached to the existing network, the introduction of cyber risk is inevitable.

That said, the U.S. NC3 system is not completely immune to cyber risks. As the U.S. government acquires new equipment, built on IP-based subsystems, and attaches this equipment to its command and control networks, the NC3 system will have to accommodate this equipment and its characteristics.[66] This process has inevitably introduced cyber risks to a system that was built before the modern cyber era. In addition, there are elements of the overall NC3 infrastructure that, although not connected to the outside environment, may still rely on support services, such as electrical power, water, fuel, and human support, any of which an adversary might attempt to disrupt through cyber attacks, thereby affecting NC3 performance.[67] Thus, cyber security is a potential vulnerability for the U.S. NC3 system—a risk that is likely to grow.[68]

Nuclear Effects on NC3 Operations

As discussed previously, U.S. NC3 was originally designed to function through all phases of a nuclear attack (before, during, and after) and was upgraded in the 1980s to sustain operations through a prolonged nuclear war lasting weeks or months. The focus of these design features was the NC3 infrastructure inside the United States supporting American strategic nuclear forces.

However, current nuclear threats have taken on a different character compared to the Cold War era. For example, Russia threatens and conducts training exercises displaying the limited use of theater nuclear weapons as a means of achieving decisive leverage during potential regional crises. Western analysts have termed this Russian doctrine "escalate to de-escalate," with Russian leaders presuming that their opponents will capitulate after a Russian limited theater nuclear attack.[69]

The NC3 systems of both the United States and its allies protected by extended deterrence may come under stress from a limited theater employment of nuclear weapons by either Russia or other nuclear-capable adversaries.[70] In these scenarios, nuclear weapon effects could potentially impair the theater elements of U.S. and allied NC3 systems, inhibiting early warning, sensors, multinational leadership conferencing, and prospective orders to theater-based nuclear forces.

Nuclear Platform Modernization

As mentioned previously, Congress has authorized replacements for all the "shooter" components of U.S. strategic nuclear forces. These weapon programs include:

1. The *Columbia*-class fleet ballistic missile submarine, which will replace the current *Ohio*-class SSBN fleet.

2. The ground-based strategic deterrent (GBSD), a new ICBM to replace the current Minuteman III missile.

3. The B-21 Raider long-range bomber, that will replace the B-2, and later the B-52 in their nuclear roles.

4. The long-range standoff munition (LRSO), a nuclear-armed cruise missile that will replace the AGM-86B ALCM.[71]

Left: Airmen with the 5th Aircraft Maintenance Squadron load unarmed AGM-86B air-launched cruise missiles (ALCMs) on the wing pylon of a B-52 at Minot AFB, North Dakota November 3, 2015 as part of Exercise Global Thunder 16—an annual U.S. Strategic Command readiness and command and control exercise. Congress has authorized the eventual replacement of the AGM-86B with the long-range standoff munition (LRSO).

These programs are still in development, and details remain classified. Little is publicly known about their technical specifications, especially regarding their communication features. It is reasonable to assume that these platforms will have the same communication capabilities as the platforms they will replace. However, it is also possible that the new platforms may be equipped with new communication technologies that the current NC3 system is not equipped to support. In that case, the NC3 system would require upgrades to communicate with a new generation of strategic nuclear platforms.

In sum, the changing security environment, propelled by adversaries equipped with new technologies and operational doctrines, is placing the legacy NC3 system under increasing strain. Counterspace threats to satellite constellations in geosynchronous orbits, offensive cyber capabilities, and adversary nuclear doctrines focused on theater operations are new stresses on the U.S. NC3 system. The U.S. government last comprehensively overhauled the system over three decades ago. As a result, those responsible for maintaining the system are experiencing increasing difficulty acquiring replacement parts for aged components. Finally, the legacy NC3 system will have to communicate with a new generation of platforms, which will be equipped with the latest communication technologies.

The U.S. NC3 system requires modernization to cope with these trends. The next section will discuss and articulate requirements and priorities for NC3 modernization, and include recommendations for how the U.S. government should organize this effort.

Designing and Organizing the NC3 Modernization Effort

It is imperative that the U.S. government modernize its three-decade-old NC3 system in a manner that accounts for current and future threats to its functionality and vulnerabilities.[72] Looming challenges to assured NC3 connectivity include all those that existed during the Cold War (Russia remains a nuclear peer to the U.S.) in addition to new challenges that have resulted from both emerging technologies and changes in the geostrategic environment. NC3 remains an existential mission for the U.S. government and its NC3 system must adapt to the new operating environment. This section describes how NC3 planners and program managers should establish requirements and priorities when fashioning a next-generation NC3 system.

It is imperative that the U.S. government modernize its three-decade-old NC3 system in a manner that accounts for current and future threats to its functionality and vulnerabilities.

The *2018 Nuclear Posture Review* (NPR) listed initiatives the U.S. government will pursue to modernize the NC3 system. These initiatives include:

1. Strengthen protection against space-based threats by increasing the agility and resilience of U.S. NC3-related space-based assets.

2. Strengthen protection against cyber threats.

3. Enhance integrated tactical warning and attack assessment by upgrading the SBIRS satellite constellation, ground-based missile warning radars, the U.S. nuclear detonation system sensors, and improving the integration of data from these systems.

4. Improve command posts and communication links by upgrading mobile command posts such as NAOC and E-6B, terrestrial command posts and data links, and transmitters and terminals across the NC3 system.

5. Advance decision support technology such as data analysis and information display tools to assist Presidential and commander decision-making.

6. Integrate planning and operations at the regional command level to allow commanders at that level to better coordinate prospective nuclear and non-nuclear military operations, thus enhancing overall deterrence.

7. Reform governance of the overall NC3 system to ensure effectiveness and efficiency during the modernization process.[73]

Due to the classified nature of the NC3 system and its modernization plans, the NPR declined to include many details about these initiatives. The remainder of this section will discuss additional aspects of NC3 modernization policymakers should consider, in addition to the NPR initiatives.

Countering Counterspace Threats to NC3

The previous section discussed how potential adversaries such as China have developed counterspace capabilities that threaten critical U.S. NC3 assets operating in geosynchronous orbit. This is a new threat to NC3 that did not exist during the Cold War, and that the legacy NC3 system did not account for in its design. The next-generation NC3 system will have to mitigate, either with countermeasures or replacements, the threats to NC3-related satellite constellations such as SBIRS, AEHF, and DSCS.

Possible lines of effort to mitigate adversary counterspace capabilities include:

1. Diplomacy. The U.S. government can use dialogue with China, Russia, and other potential counterspace actors to communicate expected norms of behavior and to reinforce the U.S. view declared in the 2018 NPR that the United States reserves the right to retaliate with nuclear weapons if an adversary were to launch a "significant non-nuclear strategic attack," examples of which include "attacks on U.S. or allied nuclear forces, their command and control, or warning and attack assessment capabilities."[74] The U.S. government can also use diplomacy with its allies and the wider international community to establish norms of behavior for space operations. Adversaries violating these accepted norms would then pay a higher price for doing so.

2. Dispersion of space assets. Succeeding generations of NC3-related satellite constellations should have their communication and earth-observation functionality distributed over a much greater number of platforms. Increasing the number of targets an adversary must attack will increase the cost of attacking U.S. NC3 space capabilities. Ideally, the marginal cost of units in these constellations will be lower than the cost of adversary satellite-killing weapons. Expanding U.S. NC3 space operations to commercial and multinational space platforms would add redundancy and increase the target set for adversaries.

3. Rapid space reconstitution capabilities. The U.S. government should develop systems to rapidly replace NC3 space assets that become disabled. These systems would include ready inventories of replacement satellites and launchers to place them into orbit. These reconstitution systems should themselves be redundant, geographically dispersed, including on mobile airborne and seaborne launch platforms.[75]

4. Suppression of adversary counterspace capabilities. The DOD should formulate operational concepts to attack adversary counterspace assets such as launch facilities, space command and control nodes, ground-based anti-satellite laser facilities, and other related infrastructure. U.S. long-range strike aircraft, such as its bomber forces, will be critical for such capabilities. U.S. forces will likely be required to track and attack mobile adversary forces in order to execute this mission.

Left: A United Launch Alliance Atlas V rocket launches on January 19, 2018, from Cape Canaveral Air Force Station, Florida, carrying the space-based infrared system (SBIRS) GEO flight four satellite onto orbit. The U.S. has to develop new systems and operational concepts to rapidly replace space-based NC3 assets that become disabled, as a way to mitigate counterspace capabilities.

Should the United States convincingly develop these counters to counterspace capabilities, it could convince potential adversaries to not waste their resources on the counterspace mission. Preserving the reliability of space-based NC3 will enhance deterrence and security.

Cyber Vulnerabilities

In its original state, the legacy NC3 system had minimal vulnerability to cyber effects because it was installed before the advent of widespread internet use, and because NC3 is a closed system, segregated from other networks. Even so, the attachment of more modern equipment has inevitably introduced cyber vulnerabilities.

This trend will only accelerate as strategic nuclear modernization proceeds. The new generation of nuclear "shooters"—the *Columbia*-class SSBNs, the GBSD ICBM, the B-21 Raider, the LRSO cruise missile, and the F-35, which will take on the dual-capable tactical aircraft mission carrying the B61 nuclear bomb—will be designed to modern technology standards, not to those of the pre-internet era. The future NC3 system will have to communicate with these modern platforms.[76] In addition, the President and senior leaders already use, and will continue to use, the NC3 system to manage non-nuclear crises and for other non-nuclear-related command and control purposes.[77] These uses will inevitably require the NC3 system to interface outside its previous closed, segregated environment, thus introducing cyber vulnerabilities.

It will not be possible to protect the NC3 system from cyber effects by turning the clock back to the pre-internet age. It will therefore be critical for designers of the future NC3 system to adopt cyber defense best practices to mitigate threats from adversary offensive cyber action against the system. According to Hyten, these cyber-defense best practices do not currently exist inside the DOD. In his view, ensuring cyber security for the future NC3 system will require the expertise of commercial entities and federal-funded research and development companies.[78]

U.S. Air Force NC3 Modernization Priorities

The U.S. Air Force owns and operates about 75 percent of the DOD's NC3 system, and spends about $4 billion annually operating, maintaining, and upgrading it.[79]

Air Force NC3 modernization priorities focus on upgrades and replacements for airborne command posts and communication terminals and receivers. Examples of these programs include:

1. Survivable airborne operations center (SAOC). The NC3 system's airborne command post aircraft are very old and need to be replaced.[80] A new aircraft, still in an early design phase, would replace the E-4B Boeing 747-model national airborne operations center (NAOC). The Air Force and Navy have even expressed interest in possibly working together on a common aircraft to replace both the NAOC and the Boeing 707-model E-6B Mercury airborne command post and command link to the Navy's SSBN fleet and the Air Force's ICBM wings.[81] In late 2018, the Air Force announced it had aligned the effort to recapitalize Air Force and Navy airborne command post aircraft under a new office at Air Force Materiel Command's Air Force Life Cycle Management Center. The new hub for these efforts is now the "presidential and executive airlift directorate" at the center, which is responsible for sustaining the existing VC-25A ("Air Force One") fleet and building the new VC-25B presidential aircraft. The office will also lead efforts to replace the E-4B NAOC, the Navy's E-6B, and the Air Force's C-32A executive aircraft. Many of these aircraft have similar challenges and a shared mission set, Maj Gen Duke Richardson, the program's executive officer, said in the announcement. The office will work to ensure the communications systems on these aircraft are modular so the President or any other senior leader flying on them will have a "predictable and reliable" experience.[82]

The U.S. Air Force owns and operates about 75 percent of the DOD's NC3 system, and spends about $4 billion annually operating, maintaining, and upgrading it.

2. Satellite terminals. Air Force programs to replace satellite receive-transmit terminals include the family of beyond line-of-sight terminals (FAB-T), global aircrew strategic network terminal (Global ASNT), the Minuteman minimum essential emergency communications network program upgrade (MMPU), and presidential and national voice conferencing (PNVC). These terminals connect to the AEHF satellite constellation and are designed to function through EMP, nuclear scintillation, and jamming.[83]

3. Very low frequency receivers. The common VLF receiver program, now in early development, will provide new terminals to command and control aircraft, bombers, tankers, ICBM LCCs, and other command posts. These receivers will allow the reliable and secure transmission of emergency action messages on the VLF band over very long distances and through nuclear detonation interference.[84]

As is evident from some of the descriptions, many of these Air Force NC3 modernization programs are either in their embryonic stages (such as replacement command and control aircraft and the strategic automated command and control system replacement) or are replacing very old equipment and thus may be late to need. Both of these observations are evidence of the lagging attention in recent years to NC3 modernization.

Reforming the Governance of U.S. NC3 Modernization

In July 2018, then-Secretary of Defense James Mattis and Marine Corps Gen Joseph Dunford, Chairman of the Joint Chiefs of Staff, formally appointed STRATCOM's Gen Hyten to be "the NC3 enterprise lead, with increased responsibilities for operations, requirements, and systems engineering and integration."[85] According to reporting from the Pentagon, Mattis was uncomfortable with the committee-like structure that had previously governed DOD's management of NC3 operations and modernization, and instead insisted that the STRATCOM commander be assigned responsibility and authority over the NC3 portfolio.

In July 2018, then-Secretary of Defense James Mattis and Marine Corps Gen Joseph Dunford, Chairman of the Joint Chiefs of Staff, formally appointed STRATCOM's Gen Hyten to be "the NC3 enterprise lead, with increased responsibilities for operations, requirements, and systems engineering and integration."

According to Hyten, the new authorities his office received from this directive are sufficient to achieve control over the NC3 modernization effort, although he cautioned that he and his successors may require additional authorities as NC3 modernization matures.[86]

Modernizing NC3 is an open-ended process that is likely to intensify over the next decade. Looming modernization challenges for STRATCOM and DOD planners will include refining a modernized NC3 system design that responds to the future threat environment; secures the cooperation of stakeholders inside the government; incorporates into the new architecture best practices, especially (when appropriate) those from the private sector regarding cyber security; and obtains institutional and funding support from Congress.

Conclusion

Policymakers should view the modernization of America's NC3 system as the "fifth pillar" of the nation's overall nuclear modernization program. The large and expensive programs to build new generations of ballistic missile submarines, ICBMs, and nuclear-capable long-range bombers, along with critical life-extension programs for the nuclear weapons themselves, receive the most attention. But even when these platforms and weapons are fielded, the United States will lack a credible nuclear deterrent if it does not also possess a nuclear command and control system that provides "no fail" communications to nuclear forces in a future environment that will include unique threats and challenges. Of the five pillars of nuclear modernization, NC3 is the least expensive, yet perhaps the most critical. Regardless of whether one supports individual elements of triad modernization, NC3 upgrades are critical to maintaining the communication structure for the current nuclear deterrent.

...the United States will lack a credible nuclear deterrent if it does not also possess a nuclear command and control system that provides "no fail" communications to nuclear forces in a future environment that will include unique threats and challenges.

Senior leaders in DOD understand the importance of NC3 modernization acutely. The 2018 *Nuclear Posture Review* discussed the aging legacy NC3 system, the challenges posed by the emerging threat environment, and the need for modernization. STRATCOM's Hyten has termed the NC3 system his greatest concern and highest priority. The U.S. Air Force, which is responsible for about 75 percent of the NC3 architecture, is now executing a modernization program.

But in spite of this needed attention, the U.S. government can and should do more to ensure the effective modernization of the NC3 system. The commander of STRATCOM now has the mission and the initial authority for organizing, planning, and leading the modernization of the NC3 system. When successful, this modernization program will result in a future architecture that will guarantee connectivity between the President and U.S. nuclear forces in even the direst scenarios. The Congress and DOD officials can contribute to this outcome by supporting and overseeing STRATCOM as it undertakes this effort in the years ahead, and ensure it can complete it successfully. ✪

Endnotes

1 *Military Assessment of Nuclear Deterrence Requirements*, *Hearing of the U.S. House of Representatives, House Armed Services Committee*, 115th Congress (March 8, 2017) (statement of USAF Gen John Hyten in response to question, video 43:35), https://armedservices.house.gov/legislation/hearings/military-assessment-nuclear-deterrence-requirements (All links accessed December, 2018).

2 Department of Defense, *Glossary Section - Nuclear Matters Handbook 2016* (Washington, DC: Office of the Deputy Assistant Secretary of Defense for Nuclear Matters, 2016) https://www.acq.osd.mil/ncbdp/nm/NMHB/index.htm.

3 Ibid.

4 Department of Defense, *Chapter Six: Nuclear Command and Control System - Nuclear Matters Handbook 2016* (Washington, DC: Office of the Deputy Assistant Secretary of Defense for Nuclear Matters, 2016), https://www.acq.osd.mil/ncbdp/nm/NMHB/chapters/chapter_6.htm.

5 Ibid.

6 Authors' note: See "Gallery of Weapons," *Air Force Magazine*, June 2018, 118, and "Fact Sheet: Ballistic Missile Early Warning System," U.S. Air Force Space Command, updated March 22, 2017, http://www.afspc.af.mil/About-Us/Fact-Sheets/Display/Article/1126401/ballistic-missile-early-warning-system/.

7 Department of Defense, *Chapter Six: Nuclear Command and Control System - Nuclear Matters Handbook 2016.*

8 Ibid.

9 Ibid.

10 Ibid.

11 Ibid. See also: *Appendix C: Basic Nuclear Physics and Weapons Effects – Nuclear Matters Handbook 2016,* and *Appendix E; Nuclear Suvivability*.

12 Eric Schlosser, *Command and Control: Nuclear Weapons, the Damascus Incident, and the Illusion of Safety*, (New York: The Penguin Press, 2013), 170-4. See also: Department of Defense, *Chapter Seven: Nuclear Surety - Nuclear Matters Handbook 2016*.

13 Schlosser, *Command and Control*, 85-6.

14 Ibid, 86.

15 Ibid, 151.

16 Authors' note: This information was gathered from an unclassified PowerPoint presentation shared with the authors detailing the history and evolution of U.S. NC3, titled "The Evolution of NC3 Systems," (Lesson Two: NC3 Systems), The MITRE Corporation, 2017.

17 Schlosser, *Command and Control*, 175-8.

18 "Gallery of Weapons," *Air Force Magazine*, June 2018, 117.

19 Schlosser, *Command and Control*, 151-2.

20 Ibid., 152-3.

21 Ibid, 153.

22 Ibid.

23 Ibid, 154.

24 Ibid, 251-2.

25 Ibid, 271.

26 Authors' note: For more on U.S. COG planning, see Garrett Graff, *Raven Rock: The Story of the U.S. Government's Secret Plan to Save Itself – While the Rest of Us Die*, (New York: Simon & Schuster, 2017).

27 "The Evolution of NC3 Systems," The MITRE Corporation.

28 John Hamre, Richard Davison, and Peter Tharpgaard, *Strategic Command, Control, and Communications: Alternative Approaches for Modernization* (Washington, DC: Congressional Budget Office, 1981), 8-10.

29 Ibid, 13-7.

30 Ibid, 3-4.

31 Ibid, 19-31.

32 Schlosser, *Command and Control*, 181-2.

33 Hamre, Davison, and Tharpgaard, *Strategic Command, Control, and Communications*, 31-8.

34 Schlosser, *Command and Control*, 442-3.

35 Ibid.

36 "Gallery of Weapons," Air Force Magazine, June 2018, 117. See also: Ashton Carter, "The Command and Control of Nuclear War," *Scientific American*, Vol. 252, No. 1, January 1985, 35.

37 Department of Defense, *Chapter Six: Nuclear Command and Control System - Nuclear Matters Handbook 2016.*

38 Carter, "The Command and Control of Nuclear War," 37.

39 "Gallery of Weapons," *Air Force Magazine*, June 2018, 116-7.

40 Carter, "The Command and Control of Nuclear War," 34.

41 Ibid, 36-7.

42 Department of Defense, *Chapter Six: Nuclear Command and Control System - Nuclear Matters Handbook 2016.*

43 Graff, *Raven Rock.*

44 Department of Defense, *Chapter Six: Nuclear Command and Control System - Nuclear Matters Handbook 2016.*

45 "Gallery of Weapons," *Air Force Magazine*, June 2018, 94-5.

46 "Nuclear Matters Handbook 2016," Chapter 6: Nuclear Command and Control System.

47 U.S. Navy, "E-6B Mercury Airborne Command Post," Fact File, last updated February 17, 2009, http://www.navy.mil/navydata/fact_display.asp?cid=1100&tid=800&ct=1.

48 Department of Defense, *Chapter Six: Nuclear Command and Control System - Nuclear Matters Handbook 2016.*

49 U.S. Navy, "Fleet Ballistic Missile Submarine – SSBN," Fact File, last updated October 24, 2017, http://www.navy.mil/navydata/fact_display.asp?cid=4100&tid=200&ct=4.

50 U.S. Navy, "Trident II (D5) Missile," Fact File, dated May 11, 2017, accessed May 21, 2018, http://www.navy.mil/navydata/fact_display.asp?cid=2200&tid=1400&ct=2.

51 Department of Defense, *Nuclear Posture Review 2018* (Washington, DC: Office of the Secretary of Defense, February 2018), https://media.defense.gov/2018/Feb/02/2001872886/-1/-1/1/2018-NUCLEAR-POSTURE-REVIEW-FINAL-REPORT.PDF, 45-6.

52 U.S. Air Force, "B-52 Stratofortress," fact sheet, updated December 16, 2015, http://www.af.mil/About-Us/Fact-Sheets/Display/Article/104465/b-52-stratofortress/.

53 U.S. Air Force, "B-2 Spirit," fact sheet, updated December 16, 2015, http://www.af.mil/About-Us/Fact-Sheets/Display/Article/104482/b-2-spirit/.

54 *Nuclear Posture Review,* 48.

55 Carter, "The Command and Control of Nuclear War," 34.

56 *Military Assessment of Nuclear Deterrence Requirements*, House Armed Services Committee (March 8, 2017), video 44:00, https://armedservices.house.gov/legislation/hearings/military-assessment-nuclear-deterrence-requirements.

57 Ibid.

58 Author interview with Gen John Hyten, USAF (commander, U.S. Strategic Command), via email, November 5, 2018.

59 *Nuclear Posture Review,* 56.

60 Hyten interview, November 5, 2018.

61 Department of Defense and Office of the Director of National Intelligence, *National Security Space Strategy – Unclassified Summary* (Washington, DC: DOD and ODNI), http://archive.defense.gov/home/features/2011/0111_nsss/docs/NationalSecuritySpaceStrategyUnclassifiedSummary_Jan2011.pdf.

62 Hyten interview, November 5, 2018.

63 Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2015* (Washington, DC: OSD, 2015), 14.

64 Ibid.

65 Sandra Erwin, "Q&A: Air Force Gen John Hyten Says U.S. Space Strategy, Budget, Moving 'Down the Right Path,'" *Space News*, April 3, 2018, http://spacenews.com/qa-air-force-gen-john-hyten-says-u-s-space-strategy-budget-moving-down-the-right-path/.

66 Ibid.

67 Author interview with Gen Kevin Chilton, USAF (Ret.), (former commander, U.S. Strategic Command), May 1, 2018.

68 *Nuclear Posture Review*, 57.

69 Ibid, 30.

70 Ibid, 57.

71 Department of Defense, *Defense Budget Overview: United States Department of Defense Fiscal Year 2019 Budget Request* (Washington, DC: Office of the Under Secretary of Defense (Comptroller), Chief Financial Officer, February 2018), https://www.defense.gov/Portals/1/Documents/pubs/FY2019-Budget-Request-Overview-Book.pdf, 3-7,3-8.

72 Hyten interview, November 5, 2018.

73 *Nuclear Posture Review*, 57-8.

74 Ibid, 21.

75 Authors' note: For more on countering adversary counterspace capabilities, see James Vedda and Peter Hays, *Major Policy Issues in Evolving Global Space Operations* (Arlington, VA: Mitchell Institute for Aerospace Studies, February 2018), 49-55.

76 Erwin, "Q&A: Air Force Gen. John Hyten."

77 Department of Defense, *Chapter Six: Nuclear Command and Control System - Nuclear Matters Handbook 2016.*

78 Hyten interview, November 5, 2018.

79 Authors' note: This figure on nuclear expenditures was quoted to the authors by Col Todd Sriver, USAF, chief of the nuclear command, control, and communications division in the Air Staff's directorate for strategic deterrence and nuclear integration. This data point comes from a talking points memo Sriver prepared in advance of a presentation to the Air Force Association's Gabriel Chapter, in McLean, VA, on May 9, 2018, titled "Nuclear Command, Control, and Communication (NC3) Modernization."

80 Hyten interview, November 5, 2018.

81 Aaron Mehta, "U.S. Navy To Work With Air Force On E-6B Replacement," *Defense News*, March 8, 2017, https://www.defensenews.com/naval/2017/03/08/us-navy-to-work-with-air-force-on-e-6b-replacement/.

82 Brian Brackens, "Air Force Consolidates Life Cycle Management of Presidential and Executive Aircraft Fleet," U.S. Air Force Life Cycle Management Center Public Affairs, updated November 26, 2018, https://www.afmc.af.mil/News/Article-Display/Article/1697959/air-force-consolidates-life-cycle-management-of-presidential-and-executive-airc/.

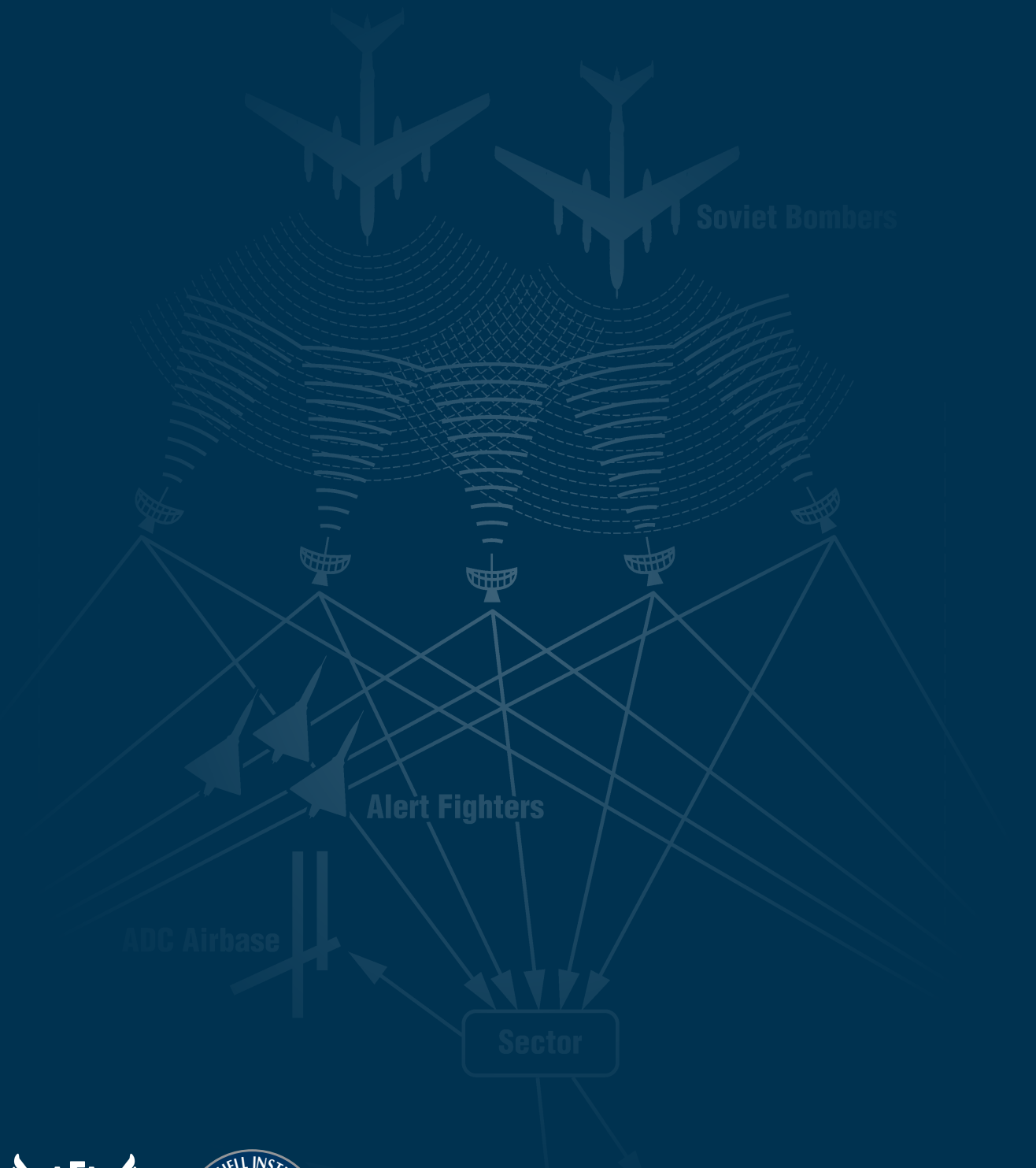
83 Sriver, talking points memo for presentation, "Nuclear Command, Control, and Communication (NC3) Modernization."

84 Ibid.

85 Sandra Erwin, "U.S. STRATCOM To Take Over Responsibility For Nuclear Command, Control And Communications," *Space News*, July 23, 2018, https://spacenews.com/u-s-stratcom-to-take-over-responsibility-for-nuclear-command-control-and-communications/.

86 Hyten interview, November 5, 2018.

www.mitchellaerospacepower.org



An Affiliate of the Air Force Association | www.mitchellaerospacepower.org