TECHNOLOGY FOR GLOBAL SECURITY

U.S. NUCLEAR COMMAND AND CONTROL FOR THE 21ST CENTURY

TECHNOLOGY FOR GLOBAL SECURITY SPECIAL REPORT

DR. JOHN HARVEY

FORMER PRINCIPAL DEPUTY ASSISTANT SECRETARY OF DEFENSE FOR NUCLEAR, CHEMICAL, AND BIOLOGICAL DEFENSE PROGRAMS

May,23rd, 2019

JOHN R. HARVEY

MAY 23, 2019

I. INTRODUCTION

In this essay, John Harvey asserts that the US NC3 system "must seek vastly improved senior leader conferencing capabilities to support decisions that go beyond what some of us call the Cold War's "multiple choice test"—that is, which major attack option to execute. To support consultations among allies, partners and potentially adversaries, in addition to senior military and advisors in complex conflict scenarios involving, say, combined offense and defense, nuclear and conventional operations—that is, the "essay test"—will require global, secure, high-quality voice, video and data transmissions that are resilient in stressed nuclear environments and go well beyond what was required for the Cold War mission."

Acknowledgments: The workshop was funded by the John D. and Catherine T. MacArthur Foundation.

This report is published simultaneously here by Nautilus Institute and here by Technology for Global Security and is published under a 4.0 International Creative Commons License the terms of which are found here.

It will be published in May 2019 by the journal *Comparative Strategy* here

The views expressed in this report do not necessarily reflect the official policy or position of the Nautilus Institute. Readers should note that Nautilus seeks a diversity of views and opinions on significant topics in order to identify common ground.

A podcast with John Harvey, Peter Hayes, and Philip Reiner on NC3 in a multipolar world is found here.

The views expressed in this report do not necessarily reflect the official policy or position of the Nautilus Institute. Readers should note that Nautilus seeks a diversity of views and opinions on significant topics in order to identify common ground.

Banner image is by Lauren Hostetter of Heyhoss Design.

CITATION

John Harvey, "U.S. Nuclear Command and Control for the 21st Century," *Tech4GS Special Reports*, May 23, 2019, https://www.tech4gs.org/nc3-systems-and-strategic-stability-a-global-overview.html

II. TECH4GS SPECIAL REPORT BY JOHN R. HARVEY

U.S. NUCLEAR COMMAND AND CONTROL FOR THE 21ST CENTURY

MAY 23, 2019

Introduction

The nuclear command and control system (NC2) of the United States is the critical link between U.S. nuclear forces and the sole authority of the President to execute those forces. It must support nuclear crisis decision making by the President, wherever located, by the discovery, integration, and provision of accurate, tailored information, by ensuring means for the President to consult with key advisors and others as necessary, and by providing means to communicate decisions to U.S. forces and, when appropriate, to the American people to inform them about those decisions. The NC2 system must function in pre-, trans-, and post-conflict phases and under all conditions of warning and force alert postures. It must allow for graceful degradation of capabilities in plausible threat environments. The understood resilience of the NC2 system is a critical component of deterrence and strategic stability.

This paper addresses the sustainment and modernization of the NC2 system. It identifies the key functions of the system and the specific system elements that enable those functions. It describes how the system that was developed and fielded during the Cold War, and designed to meet Cold War security needs, must change to address new thinking about how conventional conflict in the 21st century, and escalation to nuclear use, will evolve. A specific focus is the information and decision support needs of the President in responding to 21st century conflict scenarios and how those needs are much more varied and extensive then during the Cold War. In light of this discussion, two priorities are advanced for NC2 modernization:

- Fix the legacy NC2 system, including the so-called "thin line" architecture, to address the nuclear scenarios we focused on during the Cold War and which have not yet gone away;
- Develop an NC2 concept and associated architecture to address "modern" nuclear conflict, and generate a plan to field it over the next 10-15 years.

The paper addresses specific recommendations for NC2 modernization as well as challenges in carrying it out and concludes with a discussion of funding needs for modernization.

Nuclear Command and Control Today

The 2018 Nuclear Posture Review (NPR) concluded that the U.S. will retain a strategic nuclear triad composed of ICBMs, SLBMs, nuclear-capable heavy bombers, and a small but important component of non-strategic nuclear forces consisting of dual capable fighter aircraft. Based on its assessment of the current international security environment, the NPR also directed two supplemental capabilities: a lower-yield warhead option for the Trident SLBM and the initiation of a nuclear sea-launched cruise missile program to provide additional non-strategic nuclear capabilities. Critical to nuclear deterrence is the command and control system that links U.S. nuclear forces with Presidential authority. The system provides the President with means to

convey deterrence messages by re-deploying forces or adjusting force posture, as well as assured capabilities, when necessary, to execute nuclear forces or terminate nuclear operations.

Today's NC2 system is a legacy of the Cold War. It is fundamentally the same system that we had in place since the 1970s and described by former Secretary of Defense Ash Carter almost 35 years ago in his seminal article in Scientific American.[1] There has been some upgrading and modernization of components but the fundamental systems' architecture remains in essence as it was back then and is characterized by information technologies and electronics that range from modern-day to 1960's vintage. Portions of the system are dedicated to the nuclear mission. Other portions are multiple-use and employed during general purpose military operations.

Acquisition oversight for the sustainment and modernization of major pieces of the architecture is split between the individual services (Air Force, Navy, Army) and the Defense Information Systems Agency (DISA). Their integration into a complex system of systems, supported with adequate funding, has been a challenge for decades. Both the Obama and Trump NPRs called attention to shortfalls in NC2 funding and governance and significant progress has been made in redressing them. Just this past year, then Defense Secretary Mattis placed the Commander, Strategic Command, in charge as the "go to" person for overseeing the health of the NC2 enterprise. It is still too soon to assess the long-term impact of this change.

NC2 Functions and Basic Elements of the NC2 Architecture

The *functions* of the NC2 system are to: (1) provide clear, unambiguous, and timely detection and characterization of an attack; (2) establish a conference among the President and his senior advisors to convey critical information needed to assess the attack and determine a timely response; (3) communicate an authenticated Presidential decision in the form of an emergency action message (EAM) to nuclear forces taking into account force survivability; and (4) provide enduring control of surviving forces. In support of these activities, the Strategic Command, in coordination with the Secretary of Defense and the Joint Staff, develops pre-planned strike options and provides, as well, capabilities for rapid, adaptive planning to address unforeseen contingencies. Finally, the system must assure positive and negative control of nuclear forces even under the enormous stress of a nuclear crisis.

The specific functions of nuclear crisis management are summarized in Figure 1. The National Leadership Command Capability (the box labelled NLCC in Fig 1) comprises the capabilities within the office of the President for crisis management generally. Whether it be a nuclear strike, a catastrophic weather event, a flu epidemic, a cyberattack on the electrical grid, etc., the White House team must correlate a host of information sources, boil the information down to essentials, tailor it for consumption by the President, put him in contact with key advisors, and provide decision support, all to inform and facilitate decision making. Data unique to nuclear crises would include open source information on related political developments, intelligence on an adversary's alerting of nuclear forces, corroborating information from allies and partners, missile launch data provided by launch detection satellites (LDS) and early warning radars, and reports on bomb damage assessment.

Figure 1. Presidential Nuclear Crisis Management

Figure 1 shows that the President communicates a nuclear force execution decision to a so-called "first tier" which, depending on circumstances, could be the Secretary of Defense, the Chairman of the Joint Chiefs, the STRATCOM Commander, the colonel on duty that day in the National Military Command Center, or the flag officer flying airborne alert on the E-6B command and control aircraft. That decision is then relayed as an EAM to forces.

The NLCC, while generally operated, maintained and modernized with DoD resources, is a White House owned and managed operation optimized to meet the needs of the President across a range of crisis contingencies. This fact of life has complicated efforts to achieve a seamless interface with other pieces of the NC2 system particularly regarding crisis communications.

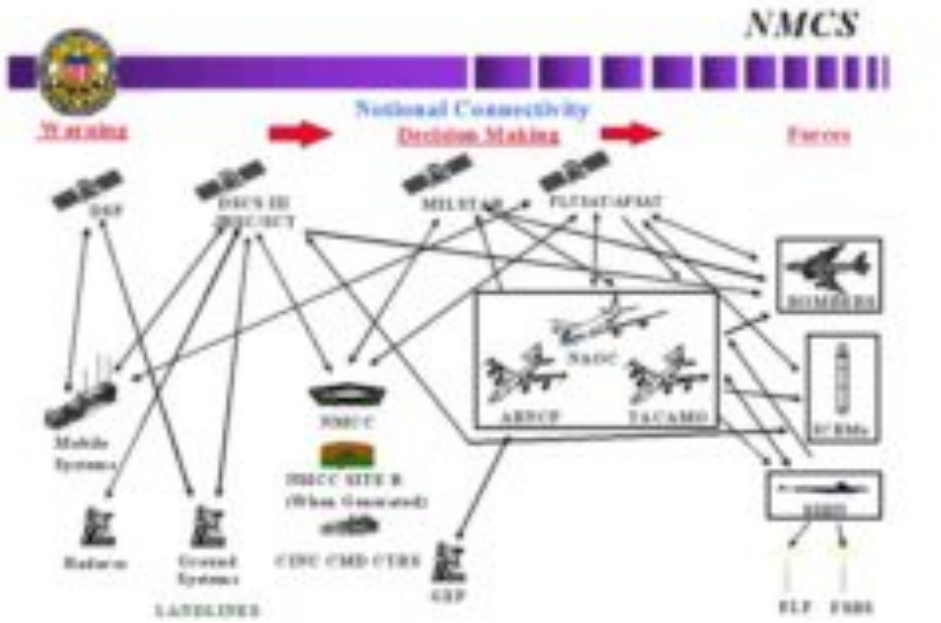
The basic elements of today's NC2 architecture include:

- Launch detection satellites (DSP, SBIRS) in geosynchronous and other orbits that, within minutes after launch, detect the hot infra-red signal generated during boost;
- Large, ground-based, phased-array early warning radars (PAVE PAWS (Cape Cod, MA and Beale AFB, CA), PARCS (North Dakota), other radars at Clear, Alaska, Shemya in the Aleutians, Thule, Greenland, and Fylingdales, UK) that detect launches in mid-course (10-20 minutes after launch) and provide independent confirmation of attack;
- Facilities located in Colorado Springs and elsewhere to interpret early warning information and assess the nature and scope of the attack;
- Air, ground-mobile, and fixed command centers (White House, STRATCOM-Omaha, NMCC-Pentagon, EUCOM, Air Force One, NAOC and E-6B aircraft, MCCC) that, among other things, provide venues to establish a conference to advise the President;

- Survivable communications links (MILSTAR and AEHF satellites, a variety of other airborne and land-line communications across the radio frequency spectrum) that transmit raw early warning data to users, provide secure means to advise the President from afar, convey execution messages to force elements (that is, ICBM launch control centers, bomber bases including those hosting NATO dual-capable aircraft, and SSBNs at sea) as well as messages to cease hostilities.

Figure 2, taken from a 2006 report of the GAO, illustrates the basic elements of the NC2 architecture and conveys its complexity.[2]

Figure 2. U.S. Nuclear Command and Control System (circa 2006)



NC2 Principles

Fielding and modernizing NC2 systems relies on a discipline grounded in certain key principles. Only the President can authorize use of U.S. nuclear weapons which has enormous implications for the NC2 system. To avoid mischaracterization of an attack, two distinct physical means for launch detection are employed. This so-called dual phenomenology is achieved from infrared sensors on launch detection satellites and subsequent detection in flight by early warning radars. To ensure connectivity in the harshest threat environments, careful attention is paid to hardening critical sub-systems and communications links to EMP and other nuclear effects. The NC2 system seeks to provide two, survivable, physically-distinct and, where possible, two-way communications links between Presidential authority and forces. In the case of bombers enroute to targets, two-way communications provide means for their recall prior to a strike, or for damage assessment after a strike. Finally, the young men and women who secure, maintain, and operate nuclear forces are subject to a rigorous personal reliability program

administrated at the base level; any logistics, maintenance or operational activity involving nuclear warheads is also subject to the "two person" rule. All of these NC2 features bolster the positive and negative control over nuclear warheads and systems for their delivery.

The Emerging Vision for "Modern" Conflict and its Implications for NC2

During the Cold War, the most likely scenario involved escalation of a conventional conflict to nuclear. Many believed that conventional war in Europe or Asia would leave the U.S. homeland relatively unscathed. Escalation to nuclear would therefore evolve with fully-alert nuclear forces, and an NC2 system not degraded from strikes during the conventional phase. That said, a massive bolt-from-the-blue attack was viewed as possible, if not plausible, and U.S. forces were postured to be resilient to that threat among other things by keeping several SSBNs at sea at all times. Indeed, the U.S. maintains and exercises capabilities to evacuate the President rapidly from Washington, DC, a primary target of a massive strike. In addition, the U.S. maintains a credible *option* for the President to launch U.S. ICBMs within a matter of minutes after receiving tactical warning of enemy launch; no enemy leader planning a precise attack on U.S. ICBMs could ever count on their assured destruction on the ground.

It is still important to assure NC2 performance to Cold War threats. But, we must also anticipate a much more dynamic security environment featuring multiple, potential sources of conflict with peer competitors, and with the emergence of nuclear-armed regional states. This environment poses more varied and complex conflict scenarios which are potentially more stressing to NC2 than traditional Cold War threats.

Four developments are driving these considerations—one political and three military-technical. First, coupled with Russia's actions under Putin that have undermined the global security order, is a seeming (and troubling) trend in Russian thinking about the limited first use of nuclear weapons evolving from an ongoing regional conventional conflict. This trend is reflected in doctrine, military exercises and ongoing modernization programs for tactical nuclear weapons. Russia's leaders may well believe that such limited use could achieve key political-military objectives short of escalation to global nuclear holocaust. Other potential nuclear-armed adversaries may share this view.

Second, are increasing capabilities for kinetic attack on satellite systems, and not just from Russia or China. Third, are increasing foreign capabilities for precision global conventional strike. Fourth, and what may be the most stressing for NC2, is the potential for cyberattack on critical NC2 assets.

Along these lines, the transition from conventional to nuclear conflict could evolve much differently than we anticipated during the Cold War, and in ways our legacy NC2 system is ill-suited to address. The conventional model for escalation—a step by step progression from peacetime to crisis to regional than global conventional conflict to nuclear use—may no longer be valid. Rather, escalation of conflict to a large-scale nuclear strike may involve a set of discrete actions that blend together in unexpected ways:

- Peacetime cyber surveillance and offensive cyber operations

- Unattributed hybrid operations in run up to crisis (as seen in Russia's war with Ukraine)
- Information operations in run up and during crisis
- Covert sabotage of critical installations
- Cyber/kinetic attack on space assets (including NC2 space assets)
- Regional conventional conflict
- Precision global conventional strikes on strategic targets
- Limited/regional nuclear use involving few casualties (EMP, demonstration shot)
- Limited/regional nuclear use on ground targets with moderate casualties

Consider the impact of a regional conflict that escalates to a global conventional phase in which U.S. nuclear forces and NC2 are degraded initially by cyber and anti-satellite attacks and, later in that phase, by long-range precision conventional strikes on military forces.

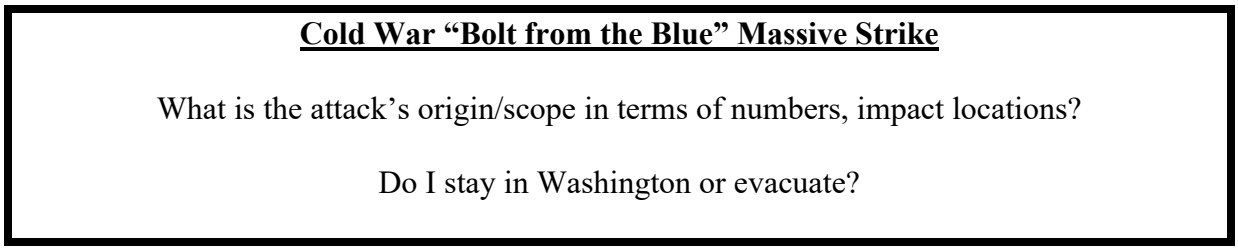
An attack on an AEHF satellite to degrade tactical communications would also degrade nuclear communications provided by that same satellite. Escalation to a "small" nuclear attack could feature high-altitude EMP and space use of nuclear weapons, along with more widespread non-nuclear attacks on general purpose command and control assets. Escalation to a "large" nuclear attack with multiple detonations on U.S. territory—that is, the Cold War scenario—could thus begin with severely degraded NC2.

During the Cold War, the focus of NC2 was to provide the President a capability to launch nuclear forces within minutes, before incoming warheads arrived. The legacy system was thus optimized for rapid execution and the required communications bandwidth was modest.

In future conflict, in which nuclear use initially may be quite limited, a President is likely to seek information from a wider array of sources, and to carry out a broader range of consultations with senior advisors, allied leaders, and possibly even with adversaries. The demand for high quality voice, video and data transmissions in these contingencies will exceed those capabilities developed for the Cold War. Bandwidth needs will be more along the lines of what could be achieved today with fast internet connections and require, in addition, both assured connectivity in nuclear environments (EMP, blackout, scintillation) and communications that cannot be exploited by an adversary. Moreover, needed capabilities must be available whether the President is in the White House, on the move, at a trip location, or at an undisclosed site.

Figure 3 illustrates how anticipated information needs for managing a nuclear crisis could differ between a Cold War scenario and one more closely associated with modern conflict.

Figure 3. Nuclear Crisis: What Will a President Want to Know?



If I "ride out" what are the implications for forces, NC2, anticipated damage to the enemy?

Which of four retaliatory strike options do you recommend?

"Modern" Conflict in the 21st Century Involving Limited Nuclear Exchange

Is Washington under attack? Where are my wife and kids?

Is the attack accidental or unauthorized, or authorized by a foreign power?

How urgent is a decision needed?

How is the conventional fight going?

What is the readiness state of U.S. nuclear forces, NC2 and defenses?

Have missile defenses shot down part or all of the threat?

Before warhead arrival: What is the anticipated damage from the strike?

After warhead arrival: What is the actual post-strike, post-BMD damage assessment?

Who will be advising me on a response? Right now, to whom am I talking?

What are options to respond? Nuke-only? Conventional? Cyber?

If I respond with nuclear weapons, how many innocent casualties?

What are other impacts (re allies, non-proliferation, etc.)?

What is the perpetrator doing/saying about the strike? What are our allies doing/saying?

When do I execute plans for continuity of government? What is the status of emergency response?

How do you know the information you are providing is accurate? How do I get more information?

What do I need to tell the American people and when?

Modernization Challenge: Providing Increased Presidential Decision Time

No President has ever fancied the choice to either launch ICBMs quickly before enemy warheads arrive on the missile fields, or wait and lose them. There are two factors today that mitigate this risk compared to the days of the Cold War. First, the evolution to single-warhead U.S. ICBMs makes this force a much less attractive target then when U.S. ICBMs typically carried three or ten warheads. Second, an increasing fraction of U.S. total strategic warheads are deployed at sea on Trident SSBNs which are inherently survivable (at least for the time being) to surprise attacks. These forces provide the President with a viable choice not to make a rapid decision, but to ride out an attack while still retaining capabilities to achieve critical targeting objectives.

President Obama's nuclear employment policy issued in 2013 called attention, with the Cold War's end, to a "significantly diminished probability of a disarming surprise nuclear attack" and directed DoD to examine options to reduce the role of ICBM launch under attack in U.S. planning. At the same time, because the risk could not be eliminated, Mr. Obama directed that DoD retain the option to do so.

Because ICBM vulnerability is a driver for rapid launch, one solution would be to field survivable ICBMs. In the 1970s-80s, when Russia's large, accurate, highly-MIRVed ICBMs posed a considerable threat, significant resources (and debate) were devoted to establishing a politically-viable, technically-achievable and cost-effective solution for ICBM survivability. Options involving deceptive basing, mobility, and increased hardness were examined. All failed, but not necessarily for technical reasons. Issues involving public interface and cost were seen as more pressing. Nearly three decades have passed and there is little interest in the Air Force, in its GBSD program to replace the Minuteman III ICBM, to explore survivable basing. At the same time, there is interest in other quarters to do so, and the option has not yet been foreclosed.

The Cold War scenario that most stressed a President's decision time and NC2, however, was not the surprise attack of Russian ICBMs, which at least provided 30 minutes warning. Rather it was the zero (or very short) warning "decapitation" strike on Washington by a low-flying cruise missile launched from a quiet Russian submarine patrolling close to the U.S. east coast coupled with an immediate follow-on attack on U.S. ICBMs. If a close-in sub were detected, certain steps could be taken to make forces, national leadership and associated NC2 more survivable and resilient. But we never adequately solved this problem. In the future, we should expect other potential adversaries to acquire capabilities for such short warning attack.

Finally, the pressure on a President to retaliate promptly to limited nuclear strikes by a non-peer adversary can be alleviated somewhat by the introduction of capable ballistic missile defenses. Defenses provide the President with additional time to assess the degree to which they succeed in blunting the attack before deciding the specifics of U.S. retaliation.

Modernization Challenge: Cyber Vulnerability/Resilience of NC2

The cyber vulnerability of U.S. nuclear forces and, specifically, NC2 is an issue that causes one to lose sleep at night! For many of us steeped in the intricacies of nuclear policy and nuclear weapons programs, cyber issues are outside our comfort zone. And, as many of us have come to realize, we are not alone; there are really very few experts out there who *really* understand the

problem, and very few of those happen to be in Washington, DC. Moreover, both offensive and defensive cyber activities tend to be very highly classified. The cyber offense experts, cleared at the highest levels, often are prevented from sharing ideas with their cyber defense colleagues, also highly cleared but not in the same security compartments, which exacerbates the problem.

Not fully understanding the problem has not stopped some from expressing opinions. Consider four views often heard on NC2 cyber resilience:

- We're OK! Air gapping, 1970s analog IT with vintage operating systems, and distributed systems acquisition, all ensure cyber resilience.
- We're not OK! The bad guys probably understand our complex system better than we do; in fact, they're probably already "inside" and can exploit it at will.
- We're so far from 'not OK' that we, Russia and others should de-alert ICBMs to avoid inadvertent launch caused by a third-party hack of launch control systems.
- We don't really know!

Not a great situation. Here's what we do know. Cyber penetration of the NC2 system raises two main concerns: the ability of hackers to prevent an authorized nuclear response to an actual strike, or cause an inadvertent launch of forces absent a real threat.[3]

On the former, an adversary could cause early warning systems to miss or mischaracterize an attack, disrupt the links that support Presidential conferencing, alter or block a force execution EAM, disrupt missile launch control systems causing a delivery platform to malfunction, or cause nuclear warheads to dud on arrival at the target. On the latter, an enemy hack could cause early warning systems to report a launch when none occurs, bypass launch control safeguards, or alter or block a war termination EAM.

While such attacks are theoretically possible, existing NC2 provides means to counter them. Rigorous and elaborate launch control safeguards include multiple redundancies, dispersed acquisition oversight for various pieces of the system, strong positive and negative control measures, "man in the loop" not automatic operations, and personal reliability programs for those who secure, operate, and maintain nuclear forces. All that said, we must continue to pay attention to this problem.

How do we assure cyber resilience of the NC2 system of the future? One important idea is to replace a culture of "tell me what I need to buy for cyber resilience so I can be done with it" with a culture of "this problem is 24/7 for the life of my system; I must assume the bad guys are already inside and my job is to confuse and deceive so that I can operate around them." This means continuous cyber surveillance of the system by really good people and tearing down the offense-defense stovepipes in establishing a permanent cyber offense "red team" to challenge defenders. Regarding people, the smart, O-3 computer science majors who take a two-year rotational assignment at Cyber Command focusing on threats to NC2 are necessary but not sufficient. Rather, it's the all but Ph.D. level folks who today command high salaries in Silicon Valley and elsewhere and who must be enticed to spend the better part of a career gaining a deep understanding of, and the attack vectors into, a very complex system. You can bet that the enemy has those same level of people working to exploit our system.

Modernization Challenge: Modernizing Legacy NC2 Systems

There are two priorities for NC2 modernization. First, is to fix the legacy NC2 system to address the nuclear scenarios we worried about during the Cold War and which have not yet gone away. Significant investment today is focused on sustaining and modernizing the so-called NC2 "thin line" defined as that part of the architecture that must function after the EMP effects from precursor high-altitude nuclear detonations. It includes alerted air and ground mobile command centers, early warning satellites and radars, communications satellites (but not necessarily all links to the ground) and surviving forces. Activities underway to sustain and modernize the "thin line" and other elements of the legacy NC2 system include:

- Survivable satellite communications (evolution of Defense Satellite Communications System and MILSTAR to Advanced Extremely High Frequency (AEHF) satellites.
- Survivable communications to forces (B-2 LF, EHF terminals, Minuteman III updates).
- Early warning satellite modernization (evolution of Defense Support Program (DSP) to Space Based Infra-Red System (SBIRS) satellites).
- Completion of the upgraded early warning radar program.
- Improved conferencing capabilities for the President (day to day and stressed environments).
- Means for improved connectivity with the President when "on the move."
- EMP hardening of critical communications links.
- Airborne and ground-mobile command post sustainment and modernization (National Airborne Operations Center, Mobile Consolidated Control Center).
- Support to TACAMO aircraft (E-6B) operations and related modernization.
- Cyber vulnerability assessment of the NC2 system and subsequent mitigation.

Over the five year period (FY17-21), the Department of Defense will spend $20.3B—about $4.0B per year—on NC2. This includes $4.0B in research, development, test, and evaluation; $6.7B in procurement; and $9.6B in operation and maintenance. This is close to NC2 funding trends in previous years, at least as far back as the beginning of President Obama's second term. The ten year estimate for NC2 continues the $4.0B per year out to FY26. For comparison, the Energy Department will spend about $10-11B per year to support the nuclear warhead enterprise over that same period. The comparable number for DoD delivery system modernization and sustainment is, on average, about $19B per year over that ten year period.[4]

Modernization Challenge: Moving Forward on an NC2 System for the 21st Century

The second modernization priority is to generate a concept and associated architecture for an NC2 system to address 21st Century conflict and then to field it. Work along these lines is at a very early stage. Efforts to generate a conceptual system architecture are just underway supported, in part, by studies carried out by the Defense Science Board, the STRATCOM Commander's Strategic Advisory Group, and others. Serious funding for systems acquisition is years away.

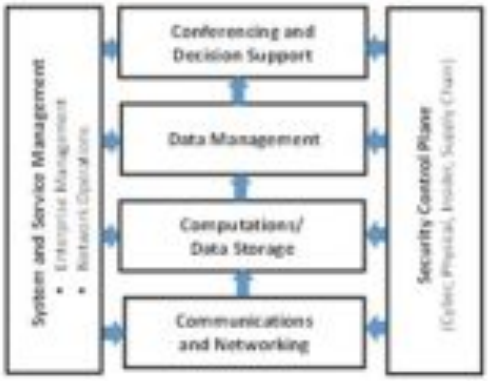


Figure 4. Conceptual Architecture for National Leadership Command Capability (NLCC)

An example of conceptual work underway on a modern NLCC systems' architecture is shown in Figure 4. Recall, the NLCC is the White House-centered operation that provides presidential crisis communications, conferencing and decision support. Figure 4 reflects a much simplified concept for a modular, hierarchical, layered architecture based loosely on the Open System Interconnection Model used in the design of IT networks.[5] Each of the horizontal boxes represents a function involved in the generation, movement, processing, and refinement of information supporting presidential crisis management. Each layer takes on a specific job and then passes its data up to the next layer. Overarching this process are two additional functions represented by the vertical blocks in Figure 4. Overall management of enterprise and associated network operations provides for seamless transitions between multiple communications links, automatic switching, connectivity with various information sources, and the ability to rapidly add (or remove) individuals from conferences. Very importantly, a security "control plane" oversees all aspects of enterprise integrity and resilience in the face of daunting cyber and physical security challenges referred to earlier. Highly-skilled career personnel employing state-of-the-art tools would provide 24/7 cyber situational awareness and facilitate effective operations when the system is under active surveillance or attack. A cyber offense "red team" would continuously challenge them by seeking chinks in the system's armor. Based on lessons learned to date, it is essential that a modern NLCC architecture have unity of design and integration, and that system acquisition be overseen by a single authority.

The future NC2 system may well exploit modern components and sub-systems from the legacy system, but it may not. It is still too soon to say. It will not be surprising, for example, if a future architecture moves away from large, multi-purpose communications satellites because of their inherent vulnerability to kinetic and non-kinetic threats. Options include small, single-purpose, "cheap-SATs" that could be launched on demand to replenish lost functionality, or long-range airborne communications relay networks that could be stood up on short notice.

Large, multiple-purpose communications satellites—used for both conventional and nuclear C2—have another disadvantage that can erode strategic stability. Nuclear-armed states engaged in regional conventional conflict may view a satellite used in tactical command and control as a legitimate target for attack. Its' adversary may construe such an attack as a precursor strike on

NC2 in advance of a disarming nuclear first strike on forces. To the degree that other missions can be disentangled from satellites supporting NC2, it will mitigate the risk of inadvertent nuclear escalation.[6]

A modern system must seek vastly improved senior leader conferencing capabilities to support decisions that go beyond what some of us call the Cold War's "multiple choice test"—that is, which major attack option to execute. To support consultations among allies, partners and potentially adversaries, in addition to senior military and advisors in complex conflict scenarios involving, say, combined offense and defense, nuclear and conventional operations—that is, the "essay test"—will require global, secure, high-quality voice, video and data transmissions that are resilient in stressed nuclear environments and go well beyond what was required for the Cold War mission.

A modern system will include updated NC2 and planning for NATO's dual capable aircraft as a critical element of regional deterrence.

As a complementary approach to hedge cyber risks, consideration could be given to a barebones, standalone, covert NC2 capability that would remain totally off line and surfaced only in an emergency. Such an approach, of course, has serious downsides, but is worth a look.

Three additional recommendations can be derived from earlier discussion:

- As part of the Air Force's GBSD program, take another look at survivable ICBM basing particularly in light of potential new technology that could make such basing affordable given a President's desire for increased decision time in executing nuclear forces.
- Examine systems/technologies to detect close-in submarines, and provide early warning of SLCM launches (facilitating evacuation of national leaders and reducing pressures for a rapid execution decision). Earlier DoD efforts to apply JLENS technology (tethered aerostats deployed with advanced radars) to detect and track cruise missiles threatening Washington were ended when a tethering cable came undone and was dragged by the aerostat through Pennsylvania farmland. That was unfortunate; JLENS was a prudent, affordable program to address a real threat and should be reinstated.
- Fund robust S&T efforts to understand future force vulnerabilities to advanced capabilities for locating quiet SSBNs at sea. The Columbia follow-on to the Ohio class SSBNs will be fielded through 2080; their long-term survivability is not a given.

Finally, we must recognize that much of the day to day operations involving U.S. nuclear forces and their command and control are carried out by young men and women in their

Figure 5: U.S. ICBM Launch Control Officers

twenties (See Figure 5). In choosing nuclear deterrence operations as a career path, they are given enormous responsibilities, probably more than they would ever receive in the civilian sector at any age. For the better part of a century, these young men and women have stepped up to their awesome duties. If this tradition of excellence is to endure for as long as the United States requires nuclear forces, than it is essential to convince them that the nation continues to value their service. There is no better way to achieve this than by taking the necessary steps to ensure that U.S. nuclear forces and systems for command and control are the best that we can offer and worthy of their continued sacrifices for our nation.

III. ENDNOTES

[1] Ashton B. Carter, *"The Command and Control of Nuclear War,"* Scientific American, Vol 252, No 1, January 1985, p. 32-39.

[2] Robert D. Critchlow, *"Nuclear Command and Control: Current Program and Issues,"* Congressional Research Service, CRS Report to Congress, RL33408, 3 May 2006.

[3] IT systems can be penetrated in several ways. The most obvious is direct access to operating systems and networks via poor password security, unauthorized use of (contaminated) flash drives (a la Stuxnet), or exploitation by insiders. Broad network surveillance enabling discovery of "backdoors" into the system is another approach. Once inside, there is opportunity to do immediate damage or to introduce custom malware that sits inertly until activated at some later time to damage or disrupt force/NC2 operations. Finally, there is the opportunity to exploit component supply chains to introduce malware into electronics intended for NC2 sub-systems.

[4] "Nuclear Weapons Sustainment: Budget Estimates Report Contains More Information than in Prior Fiscal Years but Transparency Can Be Improved," GAO Report 17-557, July 2017.

[5] For a brief review of the OSI model: https://www.webopedia.com/quick_ref/OSI_Layers.asp

[6] James M. Acton, *"Escalation through Entanglement: How the Vulnerability of Command-and-Control Systems Raises the Risks of an Inadvertent Nuclear War,"* International Security, Volume 43, No. 1, Summer 2018, p. 55-99.

IV. TECH4GS INVITES YOUR RESPONSE

Technology for Global Security invites your responses to this report. Please send responses to: info@tech4gs.org. Responses will be considered for redistribution to the network only if they include the author's name, affiliation, and explicit consent