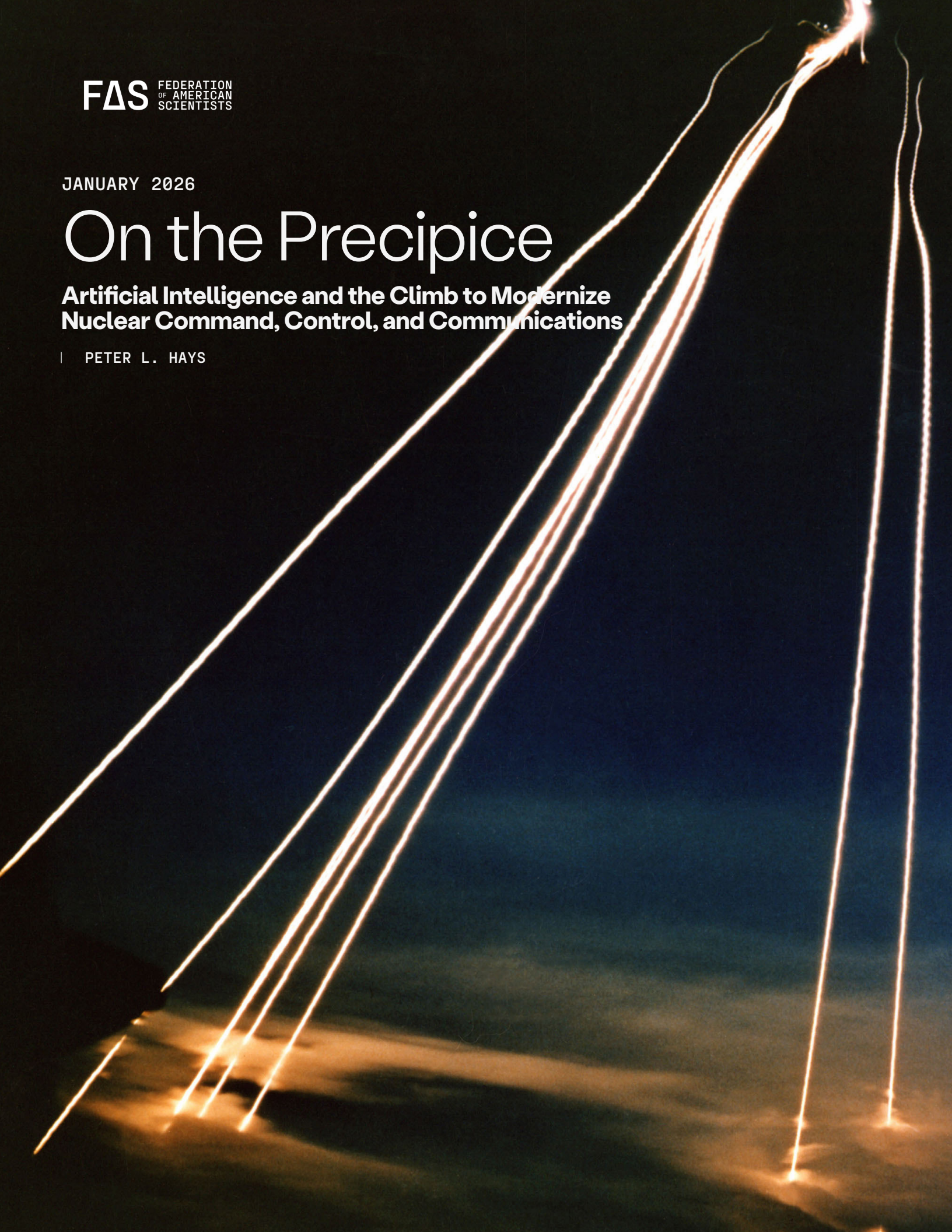
FEDERATION OF AMERICAN SCIENTISTS

JANUARY 2026

On the Precipice

Artificial Intelligence and the Climb to Modernize Nuclear Command, Control, and Communications

PETER L. HAYS



About FAS

The **Federation of American Scientists (FAS)** is an independent, nonpartisan think tank that brings together members of the science and policy communities to collaborate on mitigating global catastrophic threats. Founded in November 1945 as the Federation of Atomic Scientists by scientists who built the first atomic bombs during the Manhattan Project, FAS is devoted to the belief that scientists, engineers, and other technically trained people have the ethical obligation to ensure that the technological fruits of their intellect and labor are applied to the benefit of humankind. In 1946, FAS rebranded as the Federation of American Scientists to broaden its focus to prevent global catastrophes.

Since its founding, FAS has served as an influential source of information and rigorous, evidence-based analysis of issues related to national security. Specifically, FAS works to reduce the spread and number of nuclear weapons, prevent nuclear and radiological terrorism, promote high standards for the safety and security of nuclear energy, illuminate government secrecy practices, and prevent the use of biological and chemical weapons.

The **Nuclear Information Project** provides the public with reliable information about the status and trends of the nuclear weapons arsenals of the world's nuclear-armed countries. The project, which according to the Washington Post is "one of the most widely sourced agencies for nuclear warhead counts," uses open sources such as official documents, testimonies, previously undisclosed information obtained through the Freedom of Information Act, as well as independent analysis of commercial satellite imagery as the basis for developing the best available unclassified estimates of the status and trends of nuclear weapons worldwide. The project also conducts analysis of the role of nuclear weapons and provides recommendations for responsibly reducing the numbers and role of nuclear weapons.

The research is mainly published on the FAS Strategic Security Blog, in the Nuclear Notebook in the Bulletin of the Atomic Scientists, the World Nuclear Forces overview in the SIPRI Yearbook, as well as in magazines. As a primary source for reliable information on nuclear weapons, the project is a frequent advisor to governments, parliamentarians, the news media, institutes, and non-governmental organizations.

FAS can be reached at 1150 18th St. NW. Suite 1000, Washington, DC, 20036, **fas@fas.org**, or through **fas.org.**

Author

Peter L. Hays currently teaches graduate courses at George Washington University. He is an advisor for the Nonproliferation Policy Education Center, Prague Security Studies Institute, and Aerospace Security and Missile Defense Projects at the Center for Strategic and International Studies. Previously, he was a senior space policy advisor in the Pentagon and at the Office of the Director of National Intelligence. Dr. Hays previously taught at the USAF Academy, School of Advanced Airpower Studies, National Defense University, and School of Advanced Warfighting. He also served at the Office of Science and Technology Policy and at the National Space Council. Dr. Hays earned a Ph.D. from the Fletcher School and was an Honor Graduate of the USAF Academy. Major publications include Handbook of Space Security, Space and Security, and Toward a Theory of Spacepower.

Acknowledgements

This publication was made possible by a grant from the Carnegie Corporation of New York. The statements made and views expressed are solely the responsibility of the author.

Contents

1. Introduction

Abstract

The United States' nuclear command, control, and communications (NC3) system remains a foundational pillar of national security, ensuring credible nuclear deterrence under the most extreme conditions. Yet as the United States embarks on long-overdue NC3 modernization, this effort has received less scholarly and policy attention than the modernization of nuclear delivery systems. This paper addresses that gap by providing a critical assessment of the U.S. NC3 enterprise and its evolving role in a rapidly transforming strategic environment. Geopolitically, U.S. NC3 modernization must now contend with issues including China's rise as a nuclear near peer, Russia's deployment of increasingly threatening hypersonic and counterspace capabilities, and the erosion of norms restraining limited nuclear use. Technologically, the shift from legacy analog to digital architectures introduces both great opportunities for enhanced speed and resilience and unprecedented vulnerabilities across cyber, space, and electronic domains. Bureaucratically, modernization efforts face challenges from fragmented acquisition responsibilities and the need to align with broader initiatives such as Combined Joint All-Domain Command and Control (CJADC2) and the deployment of hybrid space architectures. This paper argues that successful NC3 modernization must do more than update hardware and software: it must integrate emerging technologies, particularly artificial intelligence (AI), in ways that enhance resilience, ensure meaningful human control, and preserve strategic stability. The study evaluates the key systems, organizational challenges, and operational dynamics shaping U.S. NC3 and offers policy recommendations to strengthen deterrence credibility in an era of accelerating geopolitical and technological change.

Introduction

This paper argues that successful U.S. NC3 modernization requires not only technical upgrades but also urgent attention to governance, cross-domain resilience, and the ethical integration of emerging technologies—all critical to maintaining a secure and effective nuclear arsenal. The paper proceeds in four main parts. First, it situates the evolution of NC3 within the broader framework of U.S. nuclear policy and strategy. Second, it assesses the architecture and modernization trajectory of key NC3 systems. Third, it examines NC3 operational processes during a hypothetical first strike scenario. Finally, it considers how emerging technologies, especially AI, are reshaping NC3 operations and risks, offering recommendations to guide responsible and effective modernization.

Few topics in national security are as simultaneously familiar and misunderstood as NC3. For most people, including many policymakers, perceptions of NC3 are shaped less by technical briefings or doctrinal documents than by popular culture. Films like *Dr. Strangelove*, *Fail Safe*, *WarGames*, *The Terminator*, and *A House of Dynamite* have long dramatized the horrific emotional toll triggered by fears of accidental war, technological failure, and loss of human control. These portrayals not only shape public imagination but have, at times, influenced senior decision makers. President Ronald Reagan, for example, was reportedly deeply affected after watching *WarGames*, asking his advisers pointed questions about cyber vulnerabilities in U.S. nuclear systems and he remained greatly depressed days after watching the television movie *The Day After*.[1] While the real-world NC3 architecture is neither a doomsday machine nor a Hollywood villain, it is an extraordinarily complex system designed to ensure deterrence, manage escalation, and prevent catastrophic miscalculations. Moving past cultural perceptions, this paper presents a detailed analysis of how the U.S. NC3 system is structured, how it would operate under a first-strike scenario, and how emerging technologies—particularly AI—might transform its utility, risks, and future role in strategic deterrence.

1 Fred Kaplan, Dark Territory: The Secret History of Cyber War (New York: Simon & Schuster, 2016), Ch. 1; David E. Hoffman, The Dead Hand: The Untold Story of the Cold War Arms Race and Its Dangerous Legacy (New York: Doubleday, 2009), 90-91.

The U.S. NC3 system is among the most complex, hardened, and mission-critical infrastructures in the national defense enterprise, yet it remains one of the least understood. At its heart, NC3 provides the assured means by which the President, as the sole authority, can exercise command and control over U.S. nuclear forces; it must function under the most extreme and existential conditions imaginable.

The 2022 *Nuclear Posture Review* identifies five essential functions of NC3:

- detection, warning, and attack characterization;
- adaptive nuclear planning;
- presidential decision-making conferencing;
- receipt and execution of presidential orders; and
- management and direction of nuclear forces.[2]

NC3 is predicated on two enduring principles known as the "always/never rule" or positive control (ensuring nuclear weapons can always be used exactly as ordered) and negative control (ensuring nuclear weapons can never be used without explicit presidential authorization).[3] Together, they define the nuclear surety imperative—the Department of Defense (DoD)[4] and National Nuclear Security Administration's comprehensive approach to ensuring the safety, security, and control of nuclear weapons, leaving no margin for error.[5]

While the fundamental requirements for nuclear surety remain unchanged, the challenges of delivering it have evolved dramatically. Three broad challenge areas stand out.

Geopolitically, the global security environment has shifted profoundly since the Cold War, when the current NC3 architecture was designed. China is deploying a range of counterspace weapons that threaten space-based NC3 systems and expanding its strategic arsenal to become a nuclear near peer with Russia and the United States, but it has never been party to the arms control agreements many analysts saw as key stabilizers of the superpower strategic relationship during the Cold War. Russia is also fielding counterspace weapons including potentially placing nuclear weapons in low-Earth orbit (LEO), has used destabilizing capabilities such as hypersonic glide vehicles in the Ukraine war, and has made repeated nuclear threats that may indicate it views limited nuclear use as an increasingly attractive option.[6] Beyond the war in Ukraine, events like repeated Israeli Arrow-3 intercepts of incoming Houthi missiles in space and large-scale conventional exchanges between nuclear armed neighbors India and Pakistan represent daunting new challenges that the 1960s-era NC3 architecture was never designed to address and demand a truly global, adaptive, and survivable system capable of handling many scenarios.[7]

Technically, many NC3 components were built on analog technologies and are only now being updated to digital architectures.[8] This update offers opportunities for enhanced speed, resilience, and interoperability, but also

2 U.S. Department of Defense, Nuclear Posture Review (Washington: Office of the Secretary of Defense, 2022), 22, https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.pdf.

3 Office of the Under Secretary of Defense for Acquisition and Sustainment, Nuclear Matters Handbook, 2020 rev., (Arlington: Nuclear Command, Control, and Communications), https://www.acq.osd.mil/ncbdp/nm/NMHB2020rev/docs/NMHB2020rev.pdf; U.S. Department of Defense, "DoD Instruction 3150.02: DoD Nuclear Weapon Surety Program," (Washington: Department of Defense, 17 December 2024), https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/315002p.PDF?ver=t7c8l8yCxjifbXVAAcALhQ%3D%3D.

4 In September 2025, President Trump signed an executive order making the "Department of War" (DoW) a secondary title for the Department of Defense. Although the DoW title is now being used on many government publications and websites, as it remains a secondary title this paper still refers to the department as the Department of Defense (DoD).

5 Nuclear Matters Handbook, Ch. 8.

6 German Institute for International and Security Affairs (SWP), Russian Nuclear Weapons in Space?, 15 May 2025, https://www.swp-berlin.org/10.18449/2025C21.

7 Peter Hays and Sarah Mineiro, Modernizing Space-Based Nuclear Command, Control, and Communications (Washington: Atlantic Council, July 2024), https://www.atlanticcouncil.org/wp-content/uploads/2024/07/Hays_-Miniero_-Modernizing-Space-Based-NC3-DRAFTJune25v2-2-1.pdf.

8 U.S. Department of Defense, Department of Defense Agency Financial Report: Fiscal Year 2022 – Top Management Challenges (Washington: DoD, November 2021), 21, https://www.oversight.gov/sites/default/files/documents/reports/2021-11/Management-ChallengesFY22.pdf.

introduces new vulnerabilities—particularly in cyberspace and the electromagnetic spectrum.[9] Ensuring secure, end-to-end performance across all NC3 segments, including space-based assets, demands robust cyber defenses and resilient network and supply chain security—problems that were different or not present for the legacy analog systems. Evolving Machine Learning (ML) and AI capabilities offer both the greatest opportunities and the greatest challenges for modernizing NC3.

Bureaucratically, NC3 modernization is occurring within an increasingly fragmented and uncertain defense acquisition and governance landscape. Despite the Air Force designating NC3 as a weapons system, appointment of the Commander of U.S. Strategic Command (USSTRATCOM) as the NC3 enterprise lead, and establishment of the NC3 Enterprise Center, too many responsibilities remain divided among several other organizations, raising challenges for integration, unity of effort, and prioritization.[10] Moreover, NC3 modernization must align with broader initiatives such as CJADC2 and the evolving hybrid space architecture.[11] The United States must ensure that nuclear surety remains a non-negotiable priority that is not diluted or sidelined in the pursuit of other modernization goals.

Given these intertwined challenges, the United States must carefully consider how to modernize not only individual NC3 components but the enterprise as a whole. Issues surrounding the ways in which AI can and should be incorporated into NC3 modernization efforts are particularly critical.[12] While AI offers significant potential benefits, such as faster decision support and improved situational awareness, it also raises important concerns regarding automation risks, escalation stability, and governance complexity.[13]

Both Congress and DoD are increasingly focused on interconnections between AI and NC3. Section 1638 of the fiscal year (FY)2025 National Defense Authorization Act (NDAA) (Public Law 118-159) included a policy statement that the use of AI: "should not compromise the integrity of nuclear safeguards, whether through the functionality of weapons systems, the validation of communication from command authorities, or the principle requiring positive human actions in execution" of a presidential employment decision.[14] A 2025 statement from Gen. Anthony Cotton, Commander USSTRATCOM, also indicates growing DoD recognition of the salience of AI and greater momentum toward its incorporation in NC3:

> USSTRATCOM will use Artificial Intelligence/Machine Learning (AI/ML) to enable and accelerate human decision-making. To fully utilize the potential of AI, USSTRATCOM requires data scientists with expertise in AI and advanced platforms across multiple classifications. Opportunities exist to leverage the emerging digital engineering environment to bridge the gap toward adopting AI/ML into the nuclear systems architecture. AI will remain subordinate to the authority and accountability vested in humans. In all cases, the United States will maintain a human "in the loop" for all actions critical to informing and executing decisions by the President to initiate and terminate nuclear weapon employment.[15]

This comprehensive assessment of the U.S. NC3 enterprise, its modernization trajectory, and the emerging role of AI offers a pathway for considering the most effective and efficient way forward. Few, if any, of today's defense

9 Herbert S. Lin, Cyber Threats and Nuclear Weapons (Stanford: Stanford University Press, 2021).
10 Hays and Mineiro, "Modernizing Space-Based NC3," 3, 13.
11 Ibid., 1, 4, 16-17; "Summary of the Joint All-Domain Command and Control Strategy (2022), with 2023 Air Force implementation notes from GAO-23-105495," (Washington: Department of the Air Force, 2023), https://media.defense.gov/2022/Mar/17/2002958406/-1/-1/1/SUMMARY-OF-THE-JOINT-ALL-DOMAIN-COMMAND-AND-CONTROL-STRATEGY.pdf.
12 U.S. Government Accountability Office, "Defense Command and Control: Further Progress Hinges on Establishing a Comprehensive Framework," (Washington: GAO, 8 April 2025), 5, 17, https://www.gao.gov/assets/gao-25-106454.pdf.
13 Edward Geist and Andrew J. Lohn, How Might Artificial Intelligence Affect the Risk of Nuclear War? (Santa Monica: RAND Corporation, 2018), 14-5, https://www.rand.org/content/dam/rand/pubs/perspectives/PE200/PE296/RAND_PE296.pdf.
14 Anya L. Fink, "Defense Primer: Nuclear Command, Control, and Communications (NC3)" (Washinton: Congressional Research Service, updated 15 August 2025), https://www.congress.gov/crs_external_products/IF/PDF/IF11697/IF11697.8.pdf.
15 Anthony J. Cotton, Statement of Anthony J. Cotton, Commander, United States Strategic Command, Before the Senate Armed Services Committee on Strategic Forces, 26 March 2025 (Washington: U.S. Senate, 2025), 17, https://www.stratcom.mil/Portals/8/Documents/2025%20USSTRATCOM%20Congressional%20Posture%20Statement.pdf?ver=CxQgRM89pGjF2tulTb4GMQ%3D%3D.

challenges carry higher stakes for global security than modernizing NC3 in the face of rapid geopolitical and technological change.

2. Historical Evolution of U.S. NC3

The United States' nuclear deterrent, as articulated in the National Security Strategy (NSS) and National Defense Strategy (NDS), rests on the pillars of assurance, dissuasion, deterrence, and defeat.[16] NC3 is foundational to each: it assures allies by providing visible, reliable control over nuclear forces; dissuades adversaries by signaling U.S. technological and procedural resolve; deters both nuclear and non-nuclear attacks by enabling credible response options, including deterrence by denial and deterrence by punishment; and enables defeat by ensuring resilient force execution under the most extreme conditions. Credible and visible NC3 also underpins extended deterrence, reassuring U.S. allies—such as Japan, South Korea, and North Atlantic Treaty Organization (NATO) members—that they are under the American nuclear umbrella, reducing incentives for allied nuclear proliferation, and reinforcing global nonproliferation regimes. Further, NC3 supports U.S. positive and negative security assurances, providing the operational backbone that allows the United States to credibly promise defense against nuclear threats while assuring non-nuclear states that they will not face nuclear coercion or attack, strengthening the integrity of the Nuclear Non-Proliferation Treaty (NPT) system.[17]

The earliest thinking and systems contributing to a U.S. NC3 system arose after the first Soviet atomic and thermonuclear tests in 1949 and 1955, President Eisenhower's concerns about a "nuclear Pearl Harbor," and recommendations from the 1954-1955 Technological Capabilities Panel, which urged the development of advanced reconnaissance and warning systems.[18] Early architectures like the Semi-Automatic Ground Environment (SAGE) air defense network, initiated in the early 1950s, and the Ballistic Missile Early Warning System (BMEWS), designed in the mid-1950s, were initially focused on detecting Soviet bomber threats. By 1957, these systems required rapid upgrades after the Soviets developed intercontinental ballistic missiles (ICBMs) and launched the Sputnik satellite, which sparked the so-called "*Sputnik* shock," and signaled the United States was vulnerable in disturbing new ways.[19] These events, combined with domestic anxieties over the Bomber Gap and Missile Gap, drove major investments in more sophisticated early warning radars, satellite reconnaissance, and hardened, survivable command links.

By the late 1950s, the U.S. Strategic Air Command (SAC) had placed a significant portion of its bomber fleet on alert to enhance survivability, while the first ICBMs were placed on limited alert in 1959, and the first nuclear-powered submarines with submarine-launched ballistic missiles (SLBMs) began operational deterrent patrols in 1960. These rapid force developments imposed unprecedented demands on the NC3 system, requiring it to balance "fail-safe" mechanisms (to prevent accidental or unauthorized use) with "fail-deadly" architectures (designed to guarantee retaliation even if national leadership and command nodes were struck).

This evolving operational reality directly shaped theoretical frameworks of the period. Albert Wohlstetter's 1958 landmark *The Delicate Balance of Terror* emphasized the need for survivability, redundancy, and carefully calibrated escalation control to manage nuclear risks, maintain credible deterrence, and avoid inadvertent war.[20] Bernard Brodie's 1959 Strategy in the Missile Age similarly wrestled with the implications of the missile revolution, exploring

16 The White House, National Security Strategy (Washington: The White House, October 2022), https://bidenwhitehouse.archives.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf; U.S. Department of Defense, Summary of the 2022 National Defense Strategy (Washington: Department of Defense, 2022), https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.PDF.

17 Department of Defense, Nuclear Posture Review (Washington, DC: Office of the Secretary of Defense, 2018), Executive Summary, 3–6, https://media.defense.gov/2018/Feb/02/2001872877/-1/-1/1/executive-summary.pdf.

18 David A. Rosenberg, "The Origins of Overkill: Nuclear Weapons and American Strategy, 1945–1960," International Security 7, no. 4 (Spring 1983): 3–71.

19 Walter A. McDougall, The Heavens and the Earth: A Political History of the Space Age (New York: Basic Books, 1985), 141-56.

20 Albert Wohlstetter, The Delicate Balance of Terror, RAND Paper P-1472 (Santa Monica: RAND Corporation, 1958), https://www.rand.org/pubs/papers/P1472.html.

how second-strike capability and NC3 resilience redefined the logic of deterrence and strategic stability.[21] Together, these foundational works helped embed NC3 considerations at the heart of U.S. nuclear strategy and laid conceptual groundwork for the more complex architectures that emerged during the 1960s and beyond.

During the 1960s and 1970s, U.S. NC3 evolved within a bipolar nuclear world shaped by both acute crises and long-term arms control efforts. The 1962 Cuban Missile Crisis exposed troubling weaknesses in U.S. command and control: members of President Kennedy's Executive Committee (ExComm) at times felt they were losing operational control over nuclear forces,[22] while revelations that Air Force leaders, notably General Thomas Power and General Curtis LeMay, had authorized aggressive airborne alerts like Chrome Dome nuclear-armed bomber flights near Soviet borders, without explicit presidential authorization, highlighted the risks of escalation through military initiative.[23] These concerns led to the Hotline between Moscow and Washington and prompted or accelerated procedural reforms aimed at reinforcing presidential authority, strengthening civilian oversight, and tightening use controls, as well as deployment of permissive action links (PALs) on U.S. nuclear weapons to prevent unauthorized arming or launch.[24] Strategically, this period was shaped not only by early deterrence theorists like Brodie and Wohlstetter but also by détente-focused strategists such as Thomas Schelling and Robert Jervis, whose work on signaling, bargaining, and crisis stability influenced efforts to manage escalation risks under the logic of Mutual Assured Destruction (MAD).[25]

Arms control milestones, including the 1963 Limited Test Ban Treaty (LTBT), which prohibited nuclear tests except underground, and the 1972 Strategic Arms Limitation Treaty (SALT I), sought to institutionalize restraint and reduce the dangers of arms racing.[26] However, emerging debates—particularly the disturbing assessments of Team B and Richard Pipes' 1977 argument in *Why the Soviet Union Thinks It Could Fight and Win a Nuclear War*—challenged assumptions of stable deterrence and pressed U.S. planners to prepare for a wider range of Soviet strategies, including scenarios of limited nuclear war or decapitation strikes.[27] These concerns shaped the requirements for NC3 survivability and adaptability, culminating in major policy directives like Presidential Directive 59 (PD-59) in 1980—which emphasized the need for flexible targeting options, enduring command links, and survivable leadership capabilities—and National Security Decision Directive 13 (NSDD-13) in 1982, which formalized the "countervailing strategy."[28] Both directives placed increased demands on NC3 to support controlled, proportionate nuclear operations even amid a protracted conflict.

Technologically, the same decades saw rapid advances that reshaped NC3 systems. Despite MAD-inspired hopes that the 1972 Interim Agreement and the strict limits on national missile defense codified in the Anti-Ballistic Missile

21 Bernard Brodie, Strategy in the Missile Age (Santa Monica: RAND, 15 January 1959), https://www.rand.org/content/dam/rand/pubs/commercial_books/2007/RAND_CB137-1.pdf.

22 Scott D. Sagan, The Limits of Safety: Organizations, Accidents, and Nuclear Weapons (Princeton: Princeton University Press, 1993), Ch. 2-3.

23 Richard Rhodes, "The General and World War III," The New Yorker, 19 June 1995, https://www.newyorker.com/magazine/1995/06/19/the-general-and-world-war-iii.

24 Steven E. Miller, "Nuclear Hotlines: Origins, Evolution, Applications," Journal for Peace and Nuclear Disarmament 4 no. 51, 176-191; Peter Stein and Peter Feaver, "Assuring Control of Nuclear Weapons: The Evolution of Permissive Action Links," (Cambridge: Center for Science and International Affairs, Harvard University, 1987); National Security Action Memorandum 160 to the Secretary of State et al., "Permissive Links for Nuclear Weapons in NATO," 6 June 1962, with Memorandum from Jerome Wiesner attached, 29 May 1962, Secret, excised copy, https://nsarchive.gwu.edu/document/28565-document-27-national-security-action-memorandum-160-secretary-state-et-al-permissive.

25 Rosenberg, "Origins of Overkill," 10, 17-8; Thomas C. Schelling, Arms and Influence (New Haven: Yale University Press, 1966), 93–115; Robert Jervis, The Meaning of the Nuclear Revolution: Statecraft and the Prospect of Armageddon (Ithaca: Cornell University Press, 1989), Ch. 3.

26 Glenn T. Seaborg, Kennedy, Khrushchev, and the Test Ban (Berkeley: University of California Press, 1981), 251–265; Raymond L. Garthoff, Détente and Confrontation: American-Soviet Relations from Nixon to Reagan (Washington: Brookings Institution Press, 1985), 293–305.

27 Richard Pipes, "Team B: The Reality Behind the Myth," Commentary 82, no. 4 (October 1986): 25-40, https://www.cia.gov/readingroom/docs/CIA-RDP93T01132R000100050007-2.pdf; Richard Pipes, "Why the Soviet Union Thinks It Could Fight and Win a Nuclear War," Commentary 64, no. 1 (July 1977): 21–34, https://www.commentary.org/articles/richard-pipes-2/why-the-soviet-union-thinks-it-could-fight-win-a-nuclear-war/; Hoffman, The Dead Hand, 21-23.

28 For archival materials and later analysis based on declassified materials, see William Burr, "U.S. Strategic Nuclear Policy: A Video History, 1945-2004," National Security Archive Electronic Briefing Book No. 361, 11 October 2011, https://nsarchive2.gwu.edu/nukevault/ebb361/index.htm; National Security Archive, "National Security Decision Directive 13, 'Nuclear Weapons Employment Policy,' 13 October 1981, Top Secret," https://nsarchive.gwu.edu/document/20309-national-security-archive-doc-24-national

(ABM) Treaty would enable the superpowers to reach a "plateau of stability," they instead raced ahead in deploying ICBMs and SLBMs with multiple independently targetable reentry vehicles (MIRVs), exponentially increasing the number of targets that could be rapidly attacked in a first strike and complicating response planning.[29] Space-based surveillance and verification emerged as a core enabling layer: the Vela Hotel satellites provided global monitoring for atmospheric nuclear detonations, laying the groundwork for what would later be formalized as "national technical means" (NTM) of treaty verification, though the boundary between NTM and NC3 systems was never clearly defined.[30] By 1970, the first Defense Support Program (DSP) satellites added global infrared missile warning to the early warning architecture, complementing powerful ground-based radars like BMEWS, the Perimeter Acquisition Radar Attack Characterization System (PARCS), and phased-array sites like PAVE PAWS.[31] Hardened communications links, survivable command centers, and protected satellite systems extended NC3's scope, embedding it as a linchpin of both deterrence and crisis management.[32]

Organizationally, the U.S. preserved a careful separation between the sensing and characterization of potential attacks (led by the North American Aerospace Defense Command, NORAD) and the execution of response options under SAC, a structure designed to reduce the risks of automatic or accidental launch.[33] In 1960, the Secretary of Defense determined that coping with the growing number and potential delivery speed of Soviet nuclear weapons required a dedicated, joint (Air Force and Navy) planning staff at SAC Headquarters.[34] This became the Joint Strategic Target Planning Staff (JSTPS), which delivered the first Single Integrated Operational Plan (SIOP) later that year.[35] Organizational separation between NORAD and SAC helped temper "hair-trigger" pressures and preserve deliberate, civilian-centered decision-making even as the tempo of nuclear operations increased.[36] To further strengthen safeguards, the United States formalized dual phenomenology requirements—mandating independent confirmation of warning data through at least two distinct sensor types (e.g., DSP satellites and ground-based radars)—to prevent false alarms from driving nuclear decisions.[37]

The need for systemic safeguards became glaringly apparent after two very troubling incidents in the late 1970s: the 1979 NORAD training tape error and the 1980 computer chip failure, both of which generated false warnings of a Soviet attack and pushed nuclear forces to heightened alert status.[38] These events revealed significant weaknesses in the reliability and redundancy of warning systems and processes. In response, the DoD issued guidance indicating that "two independent information sources using different physical principles, such as radar and infrared satellite sensors associated with the same event, help clarify the operational situation and ensure the highest possible assessment credibility."[39] In addition to focusing on technical challenges, the United States also

29 McGeorge Bundy, "To Cap the Volcano," Foreign Affairs 48, no. 1 (October 1969): 1–20; Schelling, Arms and Influence, 108–14.
30 McDougall, Heavens and the Earth, 338; Aaron Bateman, "Trust but Verify: Satellite Reconnaissance, Secrecy, and Arms Control during the Cold War," Journal of Strategic Studies 46, no. 5 (2023): 1037–61.
31 Jeffrey T. Richelson, America's Space Sentinels: DSP Satellites and National Security (Washington: Smithsonian Institution Press, 1999) 1–25, 85-90; David N. Spires, Beyond Horizons: A Half Century of Air Force Space Leadership (Maxwell AFB, AL: Air University Press, 2002), 154-60, https://www.airuniversity.af.edu/Portals/10/AUPress/Books/B_0063_SPIRES_BRADLEY_STURDEVANT_ECKERT_BEYOND_HORIZONS.pdf
32 Thomas C. Reed and Danny B. Stillman, The Nuclear Express: A Political History of the Bomb and Its Proliferation (Minneapolis: Zenith Press, 2009), 238–40.
33 Fink, "Defense Primer: NC3," 1-2.
34 U.S. Strategic Command, "History," https://www.stratcom.mil/About/History/; Rosenberg, "Origins of Overkill," 61-65.
35 Rosenberg, "Origins of Overkill," 63.
36 Harold Brown, "False Missile Alert," memorandum to President Jimmy Carter, 7 June 1980, in Foreign Relations of the United States, 1977–1980, Volume IV, National Security Policy, ed. Office of the Historian, U.S. Department of State, 190–92, https://history.state.gov/historicaldocuments/frus1977-80v04/d190.
37 John C. Toomay, "Warning and Assessment Sensors," and Ashton B. Carter, "Sources of Error and Uncertainty," in Ashton B. Carter, John D. Steinbruner, and Charles A. Zraket, Managing Nuclear Operations (Washington: Brookings Institution, 1987), 282-321, 626-37. The term "dual phenomenology" is not found in unclassified U.S. government documents.
38 U.S. General Accounting Office, "NORAD's Missile Warning System: What Went Wrong," (Washington: GAO, 15 May 1981), 3-5, https://www.gao.gov/assets/masad-81-30.pdf; Brown, "False Missile Alert."; William Burr, "False Warnings of Soviet Missile Attacks Put U.S. Forces on Alert in 1979–1980," National Security Archive Briefing Book #699 (March 16, 2020), https://nsarchive.gwu.edu/briefing-book/nuclear-vault/2020-03-16/false-warnings-soviet-missile-attacks-during-1979-80-led-alert-actions-us-strategic-forces.
39 Nuclear Matters Handbook, Ch. 2.

recognized weaknesses in leadership evacuation and continuity-of-government procedures—shortfalls most clearly demonstrated during no-notice White House evacuation exercises conducted by National Security Advisor Zbigniew Brzezinski at the behest of President Carter.[40] Complementary investments in survivable communications and command—including the Ground Wave Emergency Network (GWEN), the Milstar protected satellite system, and airborne and mobile command platforms such as the National Emergency Airborne Command Post (NEACP)—sought to harden NC3 against nuclear attack and ensure both connectivity and control under extreme stress.[41]

Under the Reagan administration, NC3 modernization accelerated alongside broader military buildup efforts.[42] NATO's Able Archer 83 exercise, which the Soviet Union nearly misinterpreted as a prelude to nuclear attack, vividly underscored the dangers of misperception, ambiguous signaling, and insufficient crisis communications.[43] Simultaneously, the Strategic Defense Initiative (SDI) introduced new debates over deterrence by denial, while advances in Global Positioning System (GPS)-enabled targeting capabilities for ballistic missile submarines (SSBNs), protected communications, and counterforce strike options enhanced force survivability, assured connectivity, and overall NC3 resilience.[44] By the late Cold War, U.S. NC3 had become central not only to deterrence by punishment—maintaining a credible second-strike capacity—but also to complicating adversary calculations by reducing the likelihood that even a well-executed first strike could eliminate U.S. retaliatory options.[45]

The post-Cold War era brought important NC3 adaptations, notably the 1991–92 Presidential Nuclear Initiatives (PNIs), which sharply reduced tactical nuclear deployments and shifted U.S. command and control away from managing vast forward-deployed arsenals.[46] Cooperative measures with Russia, including the establishment of Nuclear Risk Reduction Centers in 1987 and continued crisis communication frameworks, initially supported more stable nuclear relations.[47] Yet by the 2000s, many of these risk reduction mechanisms had atrophied, leaving NC3 to shoulder an even greater share of crisis stability and escalation management. Meanwhile, new challenges emerged: cyber vulnerabilities, space-based threats, and the complexities of a multi-domain operational environment began reshaping modernization priorities.[48]

DoD's public release of the complete 2010 Nuclear Posture Review (NPR) demonstrated greater transparency about NC3 and reaffirmed its centrality to strategic deterrence, emphasizing that a credible nuclear posture depends not only on delivery systems and warheads but also on assured command and control. It explicitly elevated the need for "modern, secure, and resilient NC3 capabilities" as a foundation for credible deterrence and crisis stability.[49] The 2010 NPR also committed to preserving a strong NC3 architecture as a hedge against

40 Hoffman, Dead Hand, 37; Terence Smith, "White House Springs Surprise Evacuation Alerts," The New York Times, 13 February 1978, B1-B2, https://www.nytimes.com/1978/02/13/archives/white-house-springs-surprise-evacuation-alerts-played-roles-of-the.html.

41 Ashton B. Carter, "Communications Technologies and Vulnerabilities," in Managing Nuclear Operations, ed. Carter et al., 217-281.

42 National Security Council, "National Security Decision Directive 178: Strategic Forces Modernization," 10 July 1985, NSDD-178, Reagan Library, 1, https://www.reaganlibrary.gov/public/archives/reference/scanned-nsdds/nsdd178.pdf; Ronald Reagan, Message to the Congress on the Strategic Modernization Program, 3 June 1986, Reagan Library, https://www.reaganlibrary.gov/archives/speech/message-congress-strategic-modernization-program .

43 Nate Jones, ed., Able Archer 83: The Secret History of the NATO Exercise That Almost Triggered Nuclear War (New York: The New Press, 2016); "The Uncensored History of Able Archer 83," National Security Archive, https://nsarchive.gwu.edu/briefing-book/able-archer-83/2025-11-14/censored-history-able-archer-83.

44 Carter et al., eds., Managing Nuclear Operations, 1-13; National Research Council, The Global Positioning System: A Shared National Asset (Washington, DC: National Academies Press, 1995), 21-26.

45 Austin Long, "Nuclear Strategy and Command Structure: What Do We Know?" The Journal of Strategic Studies 42, no. 1 (2019): 29–52.

46 Nikolai Sokov and William Potter, The Presidential Nuclear Initiatives of 1991–1992: An Assessment of Past Performance and Future Relevance (Tokyo, Toda Peace Institute, 2018), 2-5 https://toda.org/assets/files/resources/policy-briefs/T-PB-21_Nikolai%20Sokov%20and%20William%20Potter_The%20Presidential%20Nuclear%20Initiatives%201991-92.pdf; Amy F. Woolf, Nonstrategic Nuclear Weapons (Washington, DC: Congressional Research Service, 2023), 3–7, https://www.congress.gov/crs-product/RL32572.

47 Michael Krepon, Winning and Losing the Nuclear Peace: The Rise, Demise, and Revival of Arms Control (Stanford: Stanford University Press, 2021).

48 Long, "Nuclear Strategy and Command Structure."

49 U.S. Department of Defense, Nuclear Posture Review Report (Washington: Department of Defense, April 2010), 20 https://apps.dtic.mil/sti/pdfs/ADA517286.pdf.

emerging risks, including potential attacks on space assets and cyberspace vulnerabilities.[50] In doing so, it reflected growing recognition that modernization of NC3 was not simply a technical requirement but a strategic imperative necessary to ensure survivability, responsiveness, and political control in increasingly complex threat environments.[51] Importantly, the NPR placed renewed emphasis on reducing the role of nuclear weapons in U.S. strategy while reaffirming that the ability to command, control, and communicate effectively remained essential to extended deterrence commitments and the credibility of U.S. nuclear guarantees.[52]

Following the disestablishment of SAC and the creation of USSTRATCOM in 1992, organizational stresses became evident. High-profile nuclear weapons handling failures in the late 2000s, studied by the 2008 Schlesinger Task Force, prompted urgent reforms, including the creation of Air Force Global Strike Command (AFGSC) in 2009 to consolidate nuclear responsibilities and elevate standards.[53] By 2018, the Secretary of Defense formally designated the USSTRATCOM commander as the lead for the NC3 enterprise, overseeing modernization across hundreds of interconnected components, from satellites and secure communications networks to ground stations, command posts, and airborne platforms.[54] These efforts reflect NC3's central doctrinal role as the "fifth pillar" of U.S. nuclear deterrence, reinforcing both retaliation and denial by complicating adversary efforts to preempt, decapitate, or blind U.S. nuclear forces.

Modern NC3 must meet three essential requirements: assurance and security (guaranteeing data availability, integrity, and confidentiality); reliability (ensuring performance under stress); and resilience (sustaining operations or enabling rapid recovery after attack or failure). Supporting five core operational missions—situation monitoring, planning, decision-making, force management, and force direction—NC3 remains indispensable to credible deterrence and defeat. Today's NC3 modernization efforts aim to transcend Cold War-era architectures by integrating AI, enhanced space-based sensing, advanced cyber defenses, and adaptive planning tools. These initiatives are not mere technical upgrades; they reinforce NC3's foundational role in twenty-first-century deterrence strategy, ensuring that the U.S. deterrent remains credible, survivable, and effective amid renewed great-power competition, rapid technological change, and escalating strategic complexity.[55]

Recent Russian nuclear signaling, particularly in the context of its invasion of Ukraine, has underscored the urgency of these efforts.[56] As diplomatic risk-reduction mechanisms erode and nuclear saber-rattling intensifies, the credibility, adaptability, and resilience of the U.S. NC3 system have become even more critical for managing escalation risks, deterring coercion, and sustaining global strategic stability.[57]

50 Ibid., 37.
51 Ibid., 20–21, 37–38.
52 Ibid., iii, 15.
53 James R. Schlesinger et al., Report of the Secretary of Defense Task Force on DoD Nuclear Weapons Management (Washington: Department of Defense, December 2008), https://apps.dtic.mil/sti/pdfs/ADA492647.pdf.
54 U.S. Government Accountability Office, "Defense Nuclear Enterprise: Actions Needed to Strengthen the Management of the DOD's Nuclear Command, Control, and Communications (NC3) Enterprise," (Washington: GAO, November 2018), 25–26, https://www.gao.gov/assets/gao-19-29.pdf; Nuclear Matters Handbook, Ch. 2.
55 Hays and Mineiro, "Modernizing Space-Based NC3."
56 Heather Williams et al., "Russian Nuclear Calibration in the War in Ukraine," (Washington: Center for Strategic and International Studies, February 2024 https://csis-website-prod.s3.amazonaws.com/s3fs-public/2024-02/240223_Williams_Nuclear_Calibration.pdf?VersionId=WkKIPAg88HKltQVyZ_LkvtfOAp5nThqA.
57 Brad Roberts, The Case for U.S. Nuclear Weapons in the 21st Century (Stanford: Stanford University Press, 2015), Ch. 8.

3. Overview of Major U.S. NC3 Systems: Historical Evolution, Vulnerabilities, and Modernization

This section offers a structured overview of the key NC3 components, grouped into ground-based command centers, airborne platforms, land-based sensors and communications systems, and space-based systems. It examines the development, operational functions, vulnerabilities, and modernization of these systems to establish a foundation for the analysis of NC3 system operations during a hypothetical first strike in Section 4.

3.1 Ground-Based Command Centers

Ground-based command centers have historically formed the backbone of U.S. NC3, providing the essential infrastructure through which presidential command authority is exercised, force status is monitored, and communication with deployed nuclear forces is maintained. Since the early Cold War, ground systems have been indispensable to U.S. NC3. The National Military Command Center (NMCC), established in the 1960s inside the Pentagon, serves as the primary operational hub for nuclear and conventional force management, offering the President and Secretary of Defense continuous access to situational awareness, alert status, and communication networks.[58] Complementing the NMCC are hardened alternate command centers, including the Raven Rock Mountain Complex ("Site R") in Pennsylvania, designed to maintain continuity of government and operations in the event of a nuclear strike on Washington, D.C., and the Cheyenne Mountain Complex in Colorado, originally constructed to provide survivable missile warning and space surveillance capabilities for NORAD and now supporting U.S. Northern Command's broader homeland defense mission.[59]

The development of these facilities was driven by fears of a decapitation strike, whereby Soviet forces might attempt a rapid nuclear attack to incapacitate U.S. command leadership and slow response options. Cold War planners invested in redundant command centers, hardened communication networks, and secure, direct communication links, including the Hotline, to preserve strategic control and prevent inadvertent escalation.[60] A critical function of ground-based command centers is the generation and transmission of Emergency Action Messages (EAMs), the encrypted directives that convey presidential nuclear orders to U.S. forces. EAMs, authenticated through specialized coding systems, are relayed via multiple paths including ground-to-air radio links, satellite constellations, and ultra-low frequency communications for submerged submarines.[61]

However, even hardened systems face notable vulnerabilities. Fixed ground facilities remain potential targets for precision-guided conventional or nuclear attacks. One mitigation is deploying ground-mobile NC3 systems; public information about such capabilities is very limited. Cheyenne Mountain can withstand substantial overpressure, but modern earth-penetrating munitions present new challenges.[62] While many core NC3 systems were built on legacy or analogue architectures that reduce exposure to some modern cyberattack vectors, escalating cybersecurity risks emerge from the integration of older systems with newer digital components, increasing susceptibility

58 Nuclear Matters Handbook, Ch. 2.
59 Steven Aftergood, "SiteR Raven Rock: Alternate Joint Communications Center (AJCC)," FAS Nuclear Information Project, Federation of American Scientists, https://nuke.fas.org/guide/usa/c3i/raven_rock.htm; North American Aerospace Defense Command, "Cheyenne Mountain Complex,"26 April 2013, https://www.norad.mil/Newsroom/Fact-Sheets/Article-View/Article/578775/cheyenne-mountain-complex.
60 Hoffman, Dead Hand, 36-45.
61 Nuclear Matters Handbook, Ch. 2 and 8.
62 U.S. Government Accountability Office, "Defense Infrastructure: Full Costs and Security Implications of Cheyenne Mountain Realignment Have Not Been Determined,"(Washington: GAO, 21 May 2007), 1, https://www.gao.gov/products/gao-07-803r; National Research Council. "Effects of Nuclear Earth-Penetrator and Other Weapons," Washington: National Academies Press, 2005, 3, 14-16, https://nap.nationalacademies.org/catalog/11282/effects-of-nuclear-earth-penetrator-and-other-weapons.

to malware, spoofing, or denial-of-service attacks at critical interfaces.[63] The complexity and interdependence of ground-based NC3 facilities—including layered fail-safes, authentication steps, and automated signaling protocols—can inadvertently increase the risk of unauthorized or mistaken launch under crisis stress.[64] Additionally, geographic concentration also creates choke points as many critical NC3 nodes are clustered around Washington, D.C., Colorado Springs, and select other locations, creating potential for coordinated kinetic or cyberattacks, natural disasters, or electromagnetic pulse (EMP) effects to degrade system performance across multiple nodes simultaneously.

Recognizing these vulnerabilities, DoD has launched several ground system modernization programs. The Future Operationally Resilient Ground Evolution (FORGE) program, led by Space Systems Command (SSC), aims to overhaul the ground architecture supporting the Next-Generation Overhead Persistent Infrared (NG-OPIR) satellite constellation, enhancing missile warning resilience and improving data fusion.[65] Additional efforts include upgrading the Defense Red Switch Network (DRSN), modernizing ground terminals to support the forthcoming Evolved Strategic Satcom (ESS) system, and strengthening cybersecurity across all command centers. Notably, these modernization efforts emphasize shifting from a platform-centric approach to an integrated end-to-end architecture. In October 2022, former Assistant Secretary of the Air Force Frank Calvelli emphasized that ground segments should be delivered ahead of or alongside space assets to avoid capability gaps—a particularly important goal for NC3 as ground systems like FORGE are growing increasingly complex and taking on greater responsibilities for integration across many networks.[66]

3.2 Airborne Systems

The airborne segment of the U.S. NC3 system provides critical and survivable command and control capabilities, especially under scenarios where ground-based nodes are degraded or destroyed. Airborne NC3 systems emerged during the 1960s amid escalating concerns over Soviet decapitation strikes; the Cuban Missile Crisis, in particular, focused attention on the vulnerability of centralized ground command centers and the imperative to preserve command survivability in the event of nuclear attack. One of the earliest and most significant programs was the "Looking Glass" mission, in which EC-135 aircraft operated by SAC maintained continuous airborne alert as alternate command centers. These aircraft practiced launch protocols to ensure that a fail-safe command chain remained intact even if ground sites were compromised.[67] Today, the Looking Glass mission is referred to as the Airborne National Command Post (ABNCP). If ground-based command centers become inoperable, the Flag Officer aboard the ABNCP, known as the Airborne Emergency Action Officer (AEAO), is empowered to direct the execution of nuclear operations under classified procedures governing devolution of national command authority. The AEAO is supported by a battle staff of approximately 20 personnel.[68]

63 Beyza Unal and Patricia Lewis, "Cybersecurity of Nuclear Weapons Systems: Threats, Vulnerabilities and Consequences," (London: Chatham House, 2018), https://www.chathamhouse.org/sites/default/files/publications/research/2018-01-11-cybersecurity-nuclear-weapons-unal-lewis-final.pdf.

64 Virginia Tech Applied Research Corporation, "Nuclear Command, Control, and Stability Framework, (Monterey: Naval Postgraduate School, December 2015), 5-7, https://calhoun.nps.edu/server/api/core/bitstreams/da353d55-57d8-4cd4-a1f2-6fbdd035ef70/content.

65 SSC Public Affairs "USSF strengthens Missile Warning Mission with FORGE Enterprise OPIR solution effort award," (El Segundo, CA: Space Systems Command, 6 May 2025), https://www.ssc.spaceforce.mil/Newsroom/Article-Display/Article/4175204/ussf-strengthens-missile-warning-mission-with-forge-enterprise-opir-solution-ef.

66 Frank Calvelli, "Space Acquisition Tenets," (Washington: U.S. Space Force, 31 October 2022), 3 https://www.spaceforce.mil/Portals/1/ASAF%20-%20Space%20Acquisition%20Tenets%20%2831%20Oct%2022%29.pdf.

67 Bruce G. Blair, Strategic Command and Control: Redefining the Nuclear Threat (Washington: Brookings Institution, 1985), 159-66.

68 Blair, Strategic Command and Control, 165-67; Hays and Mineiro, "Modernizing Space-Based NC3," 4; Headquarters, U.S. Strategic Command, "Annex C to OPLAN 8044," Tab E to Appendix 16, "E-6 Airborne Command Post (ABNCP) Operations," 25 January 2001, Tab E (see Tab E text and Exhibits on ABNCP battle staff), https://www.governmentattic.org/38docs/USSTRATCOMannexcOPLAN8044_2001.pdf.

By the 1970s, the NEACP, later redesignated as the E-4B National Airborne Operations Center (NAOC), became the primary airborne command platform for national leadership, including the President and Secretary of Defense. Dubbed the "Doomsday Plane," the E-4B features hardened communications, EMP protection, and extended airborne endurance—capabilities critical for managing the most extreme national emergencies.[69] Parallel to these developments, the U.S. Navy established the TACAMO (Take Charge and Move Out) mission to maintain assured messaging with submerged SSBNs. Initially conducted with EC-130Q aircraft, in 1998 this mission initially transitioned to the E-6A Mercury, which evolved to the E-6B that integrates the TACAMO and ABNCP missions and incorporates the Airborne Launch Control System (ALCS), enabling airborne crews to issue launch commands to ICBMs if terrestrial command nodes are incapacitated.[70]

Airborne NC3 platforms fulfill three essential roles: (1) serving as survivable alternate command nodes, (2) relaying secure communications like EAMs between national command authorities and nuclear forces, and (3) ensuring continuity of command and control during a major attack. The E-4B NAOC is designed to evacuate and sustain senior leadership in a crisis and the E-6B routinely performs the ABNCP and TACAMO missions. Both platforms can establish secure communication links with ground command sites, ICBM fields, and other airborne assets through line of sight and satellite communications terminals using extremely high frequency, super high frequency, ultra high frequency, and high frequency radio (EHF, SHF, UHF, and HF) and the E-6B can use long trailing wire antennas for very low frequency (VLF) transmissions to SSBNs.[71] The E-6B's ALCS capability remains a cornerstone of deterrence by eliminating single points of failure in the command architecture through its integration with advanced communication suites such as family of advanced beyond-line-of-sight terminals (FAB-T), linking it with the Advanced EHF (AEHF) satellite constellation to provide resilient, jam-resistant communication pathways.

Despite their operational advantages, airborne NC3 systems face vulnerabilities. The E-4B and E-6B depend on airbase infrastructure, aerial refueling capabilities, and access to protected airspace—all potential points of failure in a high-intensity conflict. The aging E-4B airframes, based on the Boeing 747-200 design, pose maintenance and sustainability challenges. Furthermore, adversaries' evolving anti-access/area-denial (A2/AD) capabilities, including advanced surface-to-air missiles and space-based tracking assets, threaten the ability of these large aircraft to operate freely in contested environments. Cybersecurity remains a critical concern; although these systems are hardened against EMP effects, the increasing sophistication of cyber threats demands constant software, encryption, and network defenses upgrades.

DoD has initiated the Survivable Airborne Operations Center program to replace the E-4B fleet with modernized, EMP-resistant, and more fuel-efficient aircraft equipped with updated communications and mission systems.[72] Concurrently, the E-6B fleet is undergoing upgrades to extend its service life and incorporate enhanced space-based communication pathways. Emerging modernization concepts contemplate a shift away from a small number of large, conspicuous platforms toward a more distributed architecture. This could involve smaller, stealthier manned aircraft, unmanned aerial systems, or increased reliance on resilient space-based communications.[73] However, as the 2008 Schlesinger review warned, any such shifts must be comprehensively evaluated to avoid introducing operational seams or coverage gaps that adversaries could exploit.[74]

69 U.S. Air Force, "E-4B National Airborne Operations Center (NAOC) Fact Sheet," 2023, https://www.af.mil/About-Us/Fact-Sheets/Display/Article/104503/e-4b/.

70 U.S. Navy, "E-6B Mercury Airborne Command Post," updated 22 September 2021, https://www.navy.mil/Resources/Fact-Files/Display-FactFiles/Article/2162873/e-6b-mercury-airborne-command-post.

71 Ibid.

72 Greg Hadley "Air Force Awards $13 Billion Contract for New 'Doomsday' Planes ," Air & Space Forces Magazine 28 April 2024, https://www.airandspaceforces.com/air-force-13-billion-contract-doomsday-plane-saoc.

73 NAVAIR News, "Navy accepts upgraded E-6B Mercury, delivering enhanced capabilities to the fleet," 6 June 2023 https://www.navair.navy.mil/news/Navy-accepts-upgraded-E-6B-Mercury-delivering-enhanced-capabilities-fleet/Tue-06062023-0639; Congressional Research Service, "Defense Primer: NC3."

74 James Schlesinger et al., Report of the Secretary of Defense Task Force on DoD Nuclear Weapons Management (Washington: Department of Defense, 2008), 23–26, https://apps.dtic.mil/sti/citations/ADA492647.

3.3 Sensors and Communications Systems

Sensor and communications systems enable the U.S. NC3 system to operate. These systems emerged in response to the growing threat of Soviet bombers and ICBMs. Work on the first-generation large traditional radars that comprise the BMEWS began in 1957 and was completed in 1967. The three sites at Clear, Alaska; Thule (now Pituffik), Greenland; and Fylingdales, United Kingdom provide overlapping radar coverage of the shortest-distance flight paths over polar regions.[75] These radars provided additional hours of warning for Soviet bombers and additional minutes of warning for ICBMs. The Cuban Missile Crisis underscored the need for reliable missile detection and rapid communication links, pushing the United States to expand and harden its radar and communications networks.

In the late 1970s and early 1980s, the PAVE PAWS phased-array radar system was developed to address the growing threat of Soviet SLBMs launched from submarines off the U.S. coasts.[76] Two key PAVE PAWS sites were installed at Otis Air National Guard Base in Massachusetts (Cape Cod) and Beale Air Force Base in California.[77] A third PAVE PAWS site, initially at Eldorado Air Force Station, Texas, was later dismantled, and its radar faces were relocated to Clear, Alaska, as part of a major modernization and consolidation effort.[78] Over time, BMEWS and PAVE PAWS radars were systematically upgraded into the Upgraded Early Warning Radar (UEWR) configuration, incorporating advanced digital signal processing, increased sensitivity, and integration with missile defense missions.[79] Additionally, the Perimeter Acquisition Radar, once part of the Safeguard ABM system, was repurposed into the Perimeter Acquisition Radar Characterization System (PARCS) at Cavalier Space Force Station, North Dakota, providing precision tracking over the Arctic.[80]

Contributing ground-based sensors emerged as missile defense and space surveillance systems matured. AN/TPY-2 radars, deployed both in forward-based configurations (such as in Japan, South Korea, and Israel) and as part of Terminal High Altitude Area Defense (THAAD) batteries, offer precision tracking and discrimination data useful to the missile warning network.[81] Aegis Ballistic Missile Defense (BMD) radars on U.S. Navy cruisers and destroyers similarly contribute tracking and cueing information, particularly for regional and theater missile defense.[82] Another important contributing sensor is the Cobra Dane radar at Eareckson Air Station, Shemya Island, Alaska, which was originally designed for Soviet missile and space tracking but has since been integrated into the broader missile defense architecture.[83] Collateral ground-based sensors, such as certain radars from the Space Surveillance Network or legacy atmospheric and weather radars, occasionally provide incidental or opportunistic data relevant to missile warning, though they are not optimized or tasked for this mission.[84] Collectively, these layers have created

75 Carter et al., Managing Nuclear Operations, 312; Global Security.org "Ballistic Missile Early Warning System (BMEWS)," https://www.globalsecurity.org/space/systems/bmews.htm.
76 U.S. Space Force, "PAVE PAWS Radar System," October 2020, https://www.spaceforce.mil/About-Us/Fact-Sheets/Fact-Sheet-Display/Article/2197752/pave-paws-radar-system.
77 Federation of American Scientists, "AN/FPS-115 PAVE PAWS Radar," https://spp.fas.org/military/program/track/pavepaws.htm.
78 U.S. Government Accountability Office, "Space Acquisitions: Development and Oversight Challenges in Delivering Improved Space Situational Awareness Capabilities," (Washington: GAO, May 2011), 38, https://www.gao.gov/assets/gao-11-545.pdf.
79 Department of Defense Office of Inspector General, Unclassified Summary of Report No. DODIG-2024-124, "Evaluation of Sustaining Engineering Actions for the Space Force's Upgraded Early Warning Radar," 28 August 2024, 2, https://media.defense.gov/2024/Aug/29/2003534909/-1/-1/1/DODIG-2024-124%20SECURE.PDF.
80 U.S. Space Force, "Perimeter Acquisition Radar Attack Characterization System (PARCS)," fact sheet, 2024, https://www.spaceforce.mil/About-Us/Fact-Sheets/Article/2197729/perimeter-acquisition-radar-attack-characterization-system.
81 U.S. Government Accountability Office, "Missile Defense: Assessment of Testing Approach Needed as Delays and Changes Persist," (Washinton: GAO, July 2020, 79-80, https://www.gao.gov/assets/710/708393.pdf.
82 Ronald O'Rourke, "Navy Aegis Ballistic Missile Defense (BMD) Program: Background and Issues for Congress," (Washington: Congressional Research Service, 2024), 3–6, https://www.congress.gov/crs_external_products/RL/PDF/RL33745/RL33745.254.pdf.
83 Federation of American Scientists, "AN/FPS-108 Cobra Dane," https://fas.org/spp/military/program/track/cobra_dane.htm
84 U.S. Government Accountability Office, "Space Situational Awareness: DOD Should Evaluate How It Can Use Commercial Data," (Washington: April 2023), 10, https://www.gao.gov/assets/gao-23-105565.pdf .

a robust, multi-mission ground-based missile warning architecture that continues to evolve alongside advancing missile threats and emerging technologies.[85]

Equally important evolution and modernization of communications links have also advanced. The DRSN offers highly secure voice connectivity between senior civilian and military leadership, ensuring rapid coordination even under degraded conditions.[86] The Fixed Submarine Broadcast System and successor systems including the Common Submarine Radio Room architecture and Consolidated Broadcast System, integrate multiple communications paths—VLF SHF, and EHF—to provide survivable, jam-resistant two-way communications for submerged SSBNs.[87] Ground terminals such as the FAB-T for satellite-based communication systems, primarily the AEHF constellation, provide global, protected, low-probability-of-intercept communication links with nuclear and conventional forces that are particularly important for EAMs.[88] The Enhanced Polar System extends communications reach into the Arctic, while evolving concepts such as the Protected Tactical Satellite Communications Family of Systems seek to strengthen resilience against electronic attack.[89]

Ongoing radar modernization plans seek to further improve sensitivity, data fusion, and cyber resilience. UEWR sites have received phased upgrades to extend operational life, enhance discrimination against advanced threats (such as hypersonic glide vehicles), and improve integration with command and control systems.[90] However, the decommissioning of southern-facing PAVE PAWS radars at Eldorado, Texas, and Robins Air Force Base, Georgia, has left U.S. territory more exposed to missile threats from southern trajectories, such as potential launches from southern oceans or from hypersonic glide vehicles as demonstrated by the Chinese test of fractional orbital bombardment system vehicles (FOBS) in July and August 2021.[91] Analysts have raised concerns that the lack of southern coverage creates an exploitable gap, especially as missile technology advances and proliferates to new actors.[92] These vulnerabilities highlight the importance of not only modernizing existing sensors but also reassessing global radar posture in light of evolving threats.

---

85 U.S. Government Accountability Office, "Missile Defense: Better Oversight and Coordination Needed for Counter-Hypersonic Development," (Washington: GAO, June 2022), 45–46, https://www.gao.gov/assets/gao-22-105075.pdf.

86 Chairman of the Joint Chiefs of Staff Instruction 6215.01C "Policy for Department of Defense (DoD) Voice Networks with Real Time Services (RTS)," (Washington: CJCSI, 9 November 2007), 3, https://jitc.fhu.disa.mil/jitc_dri/pdfs/6215_01c.pdf.

87 U.S. Department of Defense, Director, Operational Test and Evaluation, "Common Submarine Radio Room (CSRR) (includes "Submarine Exterior Communications System (SubECS))," (Washington: DOT&E, 2010), https://www.dote.osd.mil/Portals/97/pub/reports/FY2010/navy/2010csrr.pdf?ver=2019-08-22-112818-427; Program Executive Office, Command, Control, Communications, Computers and Intelligence (PEO C4I), Undersea Communications and Integration Program Office PMW-770, "Who We Are and What We Do,"31 January 2025, https://www.peoc4i.navy.mil/Portals/98/Documents/Tear-Sheets/2025_PMW%20770_Tear%20Sheet_v01312025.pdf; U.S. Department of the Navy, "Shore Communications Master Plan (SCMP), Part 7: Submarine Communications Shore Infrastructure, Appendix B," Federation of American Scientists, https://man.fas.org/dod-101/navy/docs/scmp/part07.htm.

88 U.S. Space Force, "Advanced Extremely High Frequency System," July 2020, https://www.spaceforce.mil/About-Us/Fact-Sheets/Article/2197713/advanced-extremely-high-frequency-system.

89 U.S. Air Force / DoD, "Enhanced Polar System (EPS) Selected Acquisition Report," 20 December 2019, 7 https://www.esd.whs.mil/Portals/54/Documents/FOID/Reading%20Room/Selected_Acquisition_Reports/FY_2019_SARS/20-F-0568_DOC_28_EPS_SAR_Dec_2019_Full.pdf; Joint Chiefs of Staff, CJCSI 6250.01G: "DoD SATCOM Operational Policy," (Washington, DC: JCS, 26 July 2022), A-2, https://www.jcs.mil/Portals/36/Documents/Library/Instructions/CJCSI%206250.01G.pdf; Space Systems Command, "SSC Accelerating Protected Tactical Satcom Capability," 3 July 2025, https://www.ssc.spaceforce.mil/Newsroom/Article-Display/Article/4234599/ssc-accelerating-protected-tactical-satcom-capability.

90 U.S. Department of Defense, "Fiscal Year 2024 Budget Estimates: Missile Defense Agency, Procurement, Defense-Wide, Justification Book Volume 2b," March 2023, 15, 18, 27, 32, 39, https://comptroller.war.gov/Portals/45/Documents/defbudget/fy2024/budget_justification/pdfs/02_Procurement/PROC_MDA_VOL2B_PB_2024.pdf.

91 U.S. Department of Defense, Military and Security Developments Involving the People's Republic of China 2024: Annual Report to Congress, (Washington: DoD, 2024), 65, 101, 109-10, https://media.defense.gov/2024/Dec/18/2003615520/-1/-1/0/MILITARY-AND-SECURITY-DEVELOPMENTS-INVOLVING-THE-PEOPLES-REPUBLIC-OF-CHINA-2024.PDF. The 1979 SALT II Treaty between the U.S. and U.S.S.R. banned FOBS.

92 Tom Karako et al., "North America Is a Region, Too: An Integrated, Phased, and Affordable Approach to Air and Missile Defense for the Homeland," (Washington: Center for Strategic and International Studies, 14 July 2022), 52-55, https://missilethreat.csis.org/wp-content/uploads/2022/08/220714_Karako_North_America.pdf; Peter L. Hays, "Strategic Implications of Hypersonic Attacks from Space," AirSpace Power Journal, (Dubai: DIACC, 2025), 30, https://www.diacc.ae/assets/diacc_airspace-journal_english_peter-hays.pdf.

Looking ahead, the integration of AI/ML promises to revolutionize missile warning and defense by enabling a seamless, resilient Engage-on-Remote capability by leveraging Cooperative Engagement Capability across diverse U.S. and allied radar networks. While systems like AN/TPY-2, Aegis BMD, UEWR, PARCS, and space-based sensors currently operate through carefully managed data links and handoffs, future architectures envisioned under CJADC2 aim to use AI-driven sensor fusion that would dynamically allocate tracking responsibilities, optimize cueing and discrimination, and ensure continuity of coverage even under conditions of attack, deception, or degraded communications.[93] AI-enabled Engage-on-Remote could allow distributed sensors—regardless of platform, frequency band, or national ownership—to function as a coherent "kill web," vastly improving detection timelines, reducing false alarms, and expanding engagement windows against increasingly sophisticated adversary missile threats, including hypersonic glide vehicles and maneuverable reentry vehicles.[94]

3.4 Space-Based Systems

The space-based elements of the U.S. NC3 system have evolved dramatically since the Cold War, providing three indispensable pillars: assured, survivable strategic communications; reliable missile warning and missile tracking (MW/MT) to support nuclear and missile defense operations; and global detection and characterization of nuclear detonations. Together, these functions form the backbone of early warning and strategic situational awareness, directly underpinning the credibility of U.S. nuclear deterrence.

The architecture relies on satellites like Milstar and AEHF for secure communications, infrared sensors on DSP and space-based infrared system (SBIRS) for missile warning, and the U.S. Nuclear Detonation Detection System (USNDS) hosted primarily on GPS satellites.[95] Yet, this legacy design has increasingly become a liability because assumptions that space could be a sanctuary for NC3 systems no longer hold as space becomes a warfighting domain. Former USSTRATCOM Commander Gen. John Hyten bluntly called SBIRS satellites "big, fat, juicy targets," emphasizing the urgency of transitioning away from architectures overly reliant on a few exquisite geostationary Earth orbit (GEO) satellites.[96] The accelerating pace of testing and deployment of increasingly sophisticated Chinese and Russian counterspace threats—including direct-ascent anti-satellite weapons (ASATs), co-orbital threats like China's Shijian-21, cyber intrusions, and electronic warfare—is driving a wholesale reorientation of all parts of the U.S. national security space architecture, including space-based NC3.[97]

Modernization efforts are well underway. The ESS program aims to replace AEHF by the 2030s with a modular, open-architecture system designed for resilience, cybersecurity, and future AI/ML integration.[98] This sets the foundation for adaptive communications management, dynamic threat response, and automated anomaly detection. Likewise, MW/MT modernization has shifted toward a hybrid, proliferated architecture: SSC's Next Generation OPIR system, the Space Development Agency's (SDA) Tranche 1 and 2 Tracking Layers, and the Missile

93 U.S. Government Accountability Office, "Defense Command and Control: Further Progress Hinges on Addressing Challenges to Combined Joint All-Domain Command and Control," (Washington: GAO, 8 April 2025), 6, 12–17, https://www.gao.gov/assets/gao-25-106454.pdf

94 Vishal Giare and Gregory A. Miller. "Air and Missile Defense: Defining the Future," Johns Hopkins University Applied Physics Laboratory Technical Digest, 35, no. 4 (2021): 505-10, https://www.jhuapl.edu/sites/default/files/2024-09/35-04-Giare.pdf; Bonnie Johnson et al., "Mapping Artificial Intelligence to the Naval Tactical Kill Chain," Naval Engineers Journal, no. 135-1 (March 2023): 155-163, https://nps.edu/documents/10180/142489929/NEJ+Hybrid+Force+Issue_Mapping+AI+to+The+Naval+Kill+Chain.pdf.

95 Spires, Beyond Horizons, 152-66, 212-13, 265-66.

96 Sandra Erwin, "STRATCOM Chief Hyten: 'I Will Not Support Buying Big Satellites That Make Juicy Targets,'" Space News, 19 November 2017, https://spacenews.com/stratcom-chief-hyten-i-will-not-support-buying-big-satellites-that-make-juicy-targets.

97 U.S. Department of Defense, "Space Policy Review and Strategy on Protection of Satellites," September 2023, 2–3, 8-10 https://media.defense.gov/2023/Sep/14/2003301146/-1/-1/0/COMPREHENSIVE-REPORT-FOR-RELEASE.PDF.

98 SSC Public Affairs, "Space Systems Command Awards $2.8B Contract to Deliver the First Two Satellites for Modernized Strategic Communication Capabilities in Support of the Nuclear Command, Control and Communications Mission," (El Segundo, CA: Space Systems Command, 3 July 2025), https://www.ssc.spaceforce.mil/Newsroom/Article-Display/Article/4235257/space-systems-command-awards-28b-contract-to-deliver-the-first-two-satellites-f.

Defense Agency's (MDA) Hypersonic and Ballistic Tracking Space Sensor (HBTSS) provide more sensors across multiple orbits to deliver more robust coverage.[99] SBIRS is likely to provide the first indications of attacking ballistic missiles and serves as an essential contributor to the NC3 system's dual phenomenology requirement—ensuring that early warning is based on multiple, independent sources to minimize false positives and maximize decision-maker confidence.

SBIRS, like AEHF, and the USNDS is certified, a formal, rigorous process to ensure the system will perform exactly as intended, without introducing any ambiguity, error, or vulnerability into the nuclear command and control chain—even under extreme crisis or attack. Certification also ensures systems are fully integrated into the larger NC3 governance and operational framework.[100] As space systems increasingly incorporate commercial, hybrid, proliferated, and AI-enhanced architectures, the traditional notion of certifying a closed, end-to-end system faces new stresses. Today, obtaining answers to governance, legal, and technical questions about the ways distributed architectures might be certified for NC3 nuclear surety is being outpaced by the rapid deployment of distributed architectures that may contribute to NC3 but are not certified.[101]

These programs, informed by Calvelli's push for speed through the FORGE approach, reflect an embrace of rapid acquisition cycles, commercial partnerships, and software-heavy innovation.[102] Yet the challenge runs deeper than new hardware and software. Integrating proliferated, mixed-fidelity sensor data into a reliable nuclear decision-making architecture requires significant cultural and technical adaptation. Managing the transition from high-assurance, single-system certification models to hybrid architectures blending commercial and military assets raises key questions: While SBIRS indications alone might be sufficient to wake the President, how should lower quality data from proliferated sensor architectures be weighed, especially when these systems lack the nuclear surety and certification underpinning the current NC3 architecture? How can nuclear surety be assured when emerging AI/ML tools play roles in data fusion, cueing, or even decision support?[103] These questions cut to the heart of the nuclear governance framework, where risk tolerance is effectively zero and the cost of miscalculation incalculably high.

Moving toward a hybrid space architecture also reemphasizes enduring questions about the value of entangling systems for conventional and NC3 operations versus pursuing disaggregated architectures. While AEHF is a nuclear-certified system, in practice its primary use has been for conventional communications—raising questions about the strategic implications of nuclear-conventional entanglement, particularly under crisis conditions where adversary perceptions and targetability become acute concerns.[104] Future architectures will need not only technical resilience but also governance mechanisms that preserve positive and negative control under extreme duress, while retaining flexibility for integration with generation-after-next technologies.

Finally, modernization efforts around the USNDS system have lagged, despite its critical role in providing global nuclear detonation characterization. Without stronger prioritization, this hosted payload risks becoming the weak link in an otherwise advancing space-based NC3 framework.[105] The integration of AI/ML into NC3 offers significant potential—yet this potential is only realizable if paired with rigorous certification regimes, end-to-end validation, and uncompromising nuclear surety protocols.

---

99 Hays and Mineiro, "Modernizing Space-Based NC3," 14-16

100 The DoD Directives and Instructions as well as the CJCS Instructions governing formal certification of NC3 systems are classified.

101 Don Snyder and Alexis A. Blanc, "Unraveling Entanglement: Policy Implications of Using Non-Dedicated Systems for Nuclear Command and Control," RAND, Research Report (Santa Monica: RAND Corporation, 2023), https://www.rand.org/content/dam/rand/pubs/research_reports/RRA900/RRA976-3/RAND_RRA976-3.pdf; James M. Acton, "Escalation through Entanglement: How the Vulnerability of Command-and-Control Systems Raises the Risks of an Inadvertent Nuclear War," International Security 43, no. 1 (Summer 2018): 56–99.

102 Calvelli, "Space Acquisition Tenets."

103 Hays and Mineiro, "Modernizing Space-Based NC3," 15-17.

104 Robert Samuel Wilson and Russell Rumbaugh, "Reversal of Nuclear-Conventional Entanglement in Outer Space," Journal of Strategic Studies 47, no. 1 (2023): 3–5 https://www.tandfonline.com/doi/epdf/10.1080/01402390.2023.2249622.

105 U.S. Department of Defense Office of Inspector General, "Evaluation of the Space-Based Segment of the U.S. Nuclear Detonation Detection System," 28 September 2018, i-iii, https://media.defense.gov/2019/Nov/12/2002209615/-1/-1/1/DODIG-2018-160.PDF.

4. NC3 in Action—A First Strike Scenario

4.1 Framing the Scenario

An effective NC3 system must strengthen nuclear deterrence and function across the full range of pathways by which deterrence might fail. While detailed analysis of many failure pathways is beyond this paper's scope, examining a single, hypothetical large-scale first-strike scenario provides a focused lens to assess the operational demands, systemic vulnerabilities, and catastrophic stakes embedded in NC3. The aim here is not to argue that limited nuclear use scenarios are simply lesser included cases, to normalize nuclear warfighting, nor to promote detailed war plans, but rather to analytically illuminate the structural, procedural, and human dimensions shaping NC3 performance under a highly stressing scenario. This framing enables identification of areas where emerging technologies such as AI could assist—or dangerously complicate—core functions. As President Reagan underscored, "a nuclear war cannot be won and must never be fought;" this scenario is used to explore how NC3 would operate in a representative existential crisis for which it was designed.[106]

4.2 Strategic Context and Initial Indicators

Envision a rapidly worsening geopolitical crisis in Europe following months of increasingly sophisticated and troubling cyber attacks across a wide surface area including mapping NC3 vulnerabilities as well as efforts to poison AI training data and manipulate public opinion. NATO-Russia diplomacy has collapsed; military posturing near the Baltic escalates, and cyber operations increasingly disrupt critical infrastructure across both blocs. Intelligence reports indicate that Russian strategic forces have gone to heightened alert, dispersing mobile ICBMs and forward-deploying dual-capable aircraft. NATO command networks detect advanced cyber intrusions, including efforts to degrade military communication nodes. Concurrently, U.S. SBIRS satellites register ambiguous heat signatures consistent with pre-launch missile activity. Ground-based radars at sites like Clear Space Force Station in Alaska detect elevated radar reflections in Arctic regions. Though no launch has occurred, the U.S. NC3 system surges into its most sensitive posture: fusing multi-source intelligence, validating early warning signals, and preparing to advise the President on potential courses of action.

In such a crisis, U.S. forces would move through the DEFCON (Defense Readiness Condition) system—a graduated alert posture from DEFCON 5 (peacetime readiness) to DEFCON 1 (maximum readiness, nuclear war imminent or ongoing).[107] Transitioning from DEFCON 4 to DEFCON 3 signals heightened alert; DEFCON 2, reached only once during the Cuban Missile Crisis, places forces on the verge of launch readiness.[108] These transitions are coordinated by the Joint Chiefs of Staff and transmitted across the services to ensure synchronized posture changes. Each level increment tightens command procedures, increases alert responsibilities, and intensifies systemic strain on NC3.

4.3 Presidential Decision Chain and Adaptive Planning

At NC3's core is the National Command Authority (NCA), comprising the President and the Secretary of Defense, who possess ultimate legal authority over nuclear use; the term NCA is no longer used, but U.S. nuclear policy

106 Ronald Reagan, "Radio Address to the Nation on Nuclear Weapons," 17 April 1982, Ronald Reagan Presidential Library, https://www.reaganlibrary.gov/archives/speech/radio-address-nation-nuclear-weapons.

107 U.S. Department of Defense, JP 1-02: Department of Defense Dictionary of Military and Associated Terms, as amended, entry for "defense readiness condition," https://edocs.nps.edu/dodpubs/topic/jointpubs/JP1/JP1_02_110915.pdf.

108 Official information about defense conditions is classified. William Burr and Jeffrey Kimball, "Nuclear Threats and Alerts: Looking at the Cold War Background," Arms Control Today, April 2022, https://www.armscontrol.org/act/2022-04/features/nuclear-threats-and-alerts-looking-cold-war-background.

and doctrine remain unchanged with respect to the officials who hold this authority. When crisis indicators cross critical thresholds, the NMCC at the Pentagon and the Presidential Emergency Operations Center (PEOC) under the White House initiate the decision-support process.[109] The PEOC offers the President secure links to military commanders, intelligence chiefs, and key allies. While iconic, the PEOC is only one node: the President can issue nuclear orders from Air Force One or, if evacuated, from a NAOC E-4B aircraft.[110]

A key part of the decision chain is the military aide carrying the "football"—a black briefcase containing nuclear war plans, authentication codes, and secure communication devices.[111] The aide always shadows the President, ensuring immediate access to the legal and technical means to issue nuclear orders. Should the President decide to authorize a strike, he authenticates his identity using codes on the "biscuit"—a card kept on or near his person—and selects from available strike options.[112]

These options draw from a library of pre-planned operations, formerly known as the SIOP, now integrated into the Operations Plan (OPLAN) framework.[113] USSTRATCOM's Adaptive Nuclear Planning (ANP) supplements static plans by providing flexible, tailored options adapted to unfolding crises.[114] ANP enables limited responses, counterforce strikes, or calibrated signals of resolve without defaulting to full-scale nuclear exchanges. The President, advised by senior civilian and military leaders, must weigh whether pre-planned SIOP-type strikes or adaptive options better serve U.S. national security interests.

Believing that calculated ambiguity strengthens deterrence, the United States does not publicize its overarching strategies for responding to nuclear attacks.[115] It is not clear whether U.S. nuclear response options are primarily structured around initiating retaliatory nuclear attacks upon unambiguous confirmation of a large-scale nuclear attack (Launch on Tactical Warning), waiting until after the first nuclear detonations on U.S. or allied territory (Launch Under Attack), or potentially even waiting until completion of a first strike to better understand the most effective retaliatory options (Ride Out).[116] While operational plans incorporate elements of all three options, calculated ambiguity remains a conscious feature of U.S. deterrence posture, designed to leave adversaries unsure of when or how a U.S. nuclear response might unfold, thereby discouraging any attempt to gain advantage through a surprise first strike.[117]

4.4 Compressed Timelines, Threat Conferences, and Systemic Strain

Depending on trajectory and origin, incoming missile threats may offer as little as 15–30 minutes warning for intercontinental attacks, or only minutes for regional, submarine-launched, or hypersonic systems.[118] This compressed timeline imposes extreme pressure on both the technical and human elements of NC3. To manage this, the system advances through a series of escalating threat conferences: initial sessions assess early warning

109 Nuclear Matters Handbook, Ch. 2. The PEOC is not discussed in unclassified materials.
110 Ibid.
111 Arms Control Association, "Presidents and the 'Nuclear Football'," Arms Control Today, 2 March 2025, https://www.armscontrol.org/act/2025-03/features/presidents-and-nuclear-football.
112 Ibid.
113 William Burr, ed., "The Creation of SIOP-62: More Evidence on the Origins of Overkill," National Security Archive Electronic Briefing Book No. 130, National Security Archive, 2004, https://nsarchive2.gwu.edu/NSAEBB/NSAEBB130/index.htm; "Annex C to OPLAN 8044."
114 Nuclear Posture Review, 2018, VII, 21, 23, 44, 57-8.
115 Amy F. Woolf, "U.S. Nuclear Weapons Policy: Considering 'No First Use,'" (Washington: Congressional Research Service, updated 16 April 2021), 1-2, https://www.congress.gov/crs_external_products/IN/PDF/IN10553/IN10553.4.pdf.
116 Congressional Commission on the Strategic Posture of the United States, America's Strategic Posture: The Final Report of the Congressional Commission on the Strategic Posture of the United States (Alexandria, VA: Institute for Defense Analyses, October 2023), 33, https://www.ida.org/-/media/feature/publications/A/Am/Americas%20Strategic%20Posture/Strategic-Posture-Commission-Report.pdf.
117 Ibid., 26-28.
118 Congressional Research Service, "Hypersonic Missile Defense: Issues for Congress," (Washington: Library of Congress, 2024), https://www.congress.gov/crs-product/IF11623?; Hays "Strategic Implications of Hypersonic Attacks from Space."

data; subsequent missile attack conferences coordinate responses as launch indications firm; final execution conferences oversee the transmission of nuclear orders.[119]

These conferences connect the President, the Secretary of Defense, the Chairman of the Joint Chiefs, the NMCC, USSTRATCOM, and other key actors via secure networks.[120] Each follows a structured script to ensure rapid communication of critical information, accurate recording of decisions, and completion of verification protocols. Once sensors and commanders judge that an attack is imminent or underway, the missile attack conference focuses on confirming launch details, executing validated options, and coordinating with allied commands.[121]

Sensor fusion algorithms must distinguish genuine missile launches from decoys, atmospheric phenomena, or cyber-induced false alarms while preserving corroborated indications from independent sensors. Communication systems must resist jamming and cyber disruption, enabling command authorities to balance decisiveness with the need to avoid catastrophic error. A failure at any node—whether sensors, decision aids, communications, or command authority—risks a false positive or missed launch, each with potentially world-altering consequences.

If designed and operated correctly, AI could add greater clarity and certainty to warning data, which would, in turn, afford more time for more robust and longer conferencing among more decision makers. Some experts, however, warn that incorporating automated or AI-driven decision aids at this stage could raise the risk of miscalculation: while machines process data faster, human judgment remains the irreplaceable safeguard against irrevocable mistakes.[122]

4.5 Message Dissemination: Emergency Action Messages

If the President authorizes a nuclear response, the system moves into the execution phase. The NMCC, working in coordination with STRATCOM, formats, authenticates, and generates EAMs, short, highly encrypted codes conveying nuclear execution orders to operational forces.[123] These messages are transmitted simultaneously through multiple hardened and redundant communication pathways, including UHF radio systems, EHF satellite links, and VLF/ELF transmissions from airborne E-6B Mercury TACAMO aircraft, whose long trailing antennas provide survivable communication links to submarines and remote forces even in degraded conditions.[124] This multi-path, resilient architecture is hardened against nuclear, electronic warfare, and cyber attacks, and is designed to keep at least some channels remain open to convey presidential orders.

Critically, U.S. SSBNs do not surface to receive EAMs as doing so would compromise their primary advantage: survivability through stealth. Instead, they rely on VLF/ELF signals that can penetrate seawater to reach submerged platforms.[125] The EAM dissemination process depends on pre-distributed sealed authenticators, which contain

119 For discussion of the Threat Assessment Conference not escalating to a Missile Attack Conference as a result of the 1979 NORAD training tape error, see United States Department of State, Office of the Historian, Foreign Relations of the United States, 1977–1980, Volume IV, National Security Policy, Doc. 167, "Memorandum from Secretary of Defense Brown to President Carter," Washington, November 20, 1979, https://history.state.gov/historicaldocuments/frus1977-80v04/d167; William Burr, "False Warnings of Soviet Missile Attacks."

120 Ibid.

121 Ibid.

122 Herbert Lin, "Artificial Intelligence and Nuclear Weapons: A Commonsense Approach to Understanding Costs and Benefits," Texas National Security Review, 8, no. 3 (Summer 2025):| 98-109, https://tnsr.org/2025/06/artificial-intelligence-and-nuclear-weapons-a-commonsense-approach-to-understanding-costs-and-benefits.

123 Anya L. Fink, "Authority to Launch Nuclear Forces," (Washington: Congressional Research Service, updated August 7, 2025), https://www.congress.gov/crs_external_products/IF/PDF/IF10521/IF10521.16.pdf.

124 Naval Air Systems Command, "E-6B Mercury."

125 Federation of American Scientists, "Very Low Frequency (VLF)," https://nuke.fas.org/guide/usa/c3i/vlf.htm. There is no public evidence indicating that U.S. SSBNs operate under orders like the "letters of last resort" which provide instructions if all communications are lost and are issued by the UK Prime Minister to the Captains of that nation's Trident SSBNs. See, Dan Sabbagh, "'Letters of last resort': deciding response to a nuclear attack among first of Starmer's tasks," The Guardian, 5 July 2024, https://www.theguardian.com/world/article/2024/jul/05/letters-of-last-resort-deciding-response-to-a-nuclear-attack-among-first-of-starmers-tasks..

time-sensitive codes used to verify the legitimacy of execution orders.[126] The system further embeds multiple human safeguards: the two-person rule, requiring independent confirmation and action by two authorized operators, and split-knowledge arrangements, whereby no single person possesses sufficient information to complete critical arming or execution procedures unilaterally.[127]

4.6 Force Readiness and Posturing

Upon receipt of EAMs, the three legs of the U.S. nuclear triad initiate tailored preparations. ICBM crews in hardened silos validate EAMs through dual-key systems and cross-check protocols. SLBM crews aboard SSBNs adjust posture to maintain launch readiness while preserving stealth. Nuclear-capable bombers, the B-2 Spirit and B-52H Stratofortress, move to strip alert immediate launch positions or continue airborne alert rotations.

Each leg operates under distinct timelines and procedural safeguards. Bombers offer flexible, recallable options; ICBMs provide fast response options but cannot be disabled once launched; submarines provide the most survivable second-strike capability but face persistent communication challenges under combat conditions.[128] NC3 systems must synchronize these timelines while accounting for disruptions from physical attack, EMP, cyber interference, space-based threats, and atmospheric effects like radio scintillation or blackout zones caused by nuclear detonations.[129]

To preserve command continuity, the system integrates fallback measures: alternate command centers such as the ABNCP aboard E-4B aircraft, EMP-hardened ground nodes, dispersed launch control mechanisms, and preplanned degraded communication protocols.[130]

4.7 Coordination Across Commands and Allies

Modern nuclear employment planning involves not only U.S. strategic forces but also complex theater-level operations within alliances like NATO.[131] Dual-capable aircraft operated by NATO allies, regional missile defense networks, and shared situational awareness systems all require precise coordination to prevent accidents, miscommunication, or inadvertent escalation. The U.S. NC3 system must therefore synchronize not only across its own strategic and regional commands but also with weapons release protocols in multinational allies and partners, often under conditions of stress or degraded connectivity.[132] Regional contingencies, such as North Korean nuclear aggression or an India-Pakistan exchange, pose additional challenges, demanding rapid coordination among U.S. regional and strategic commands and allies.[133]

126 Previous editions of the Nuclear Matters Handbook included more detail about EAM dissemination and controls. See, United States Department of Defense, Nuclear Matters: A Practical Guide to DoD Nuclear Weapon Surety (Washington, DC: DoD, 2015), 76-79, https://www.lasg.org/Nuclear_Matters_A_Practical_Guide_DoD.pdf.

127 Nuclear Matters Handbook, Ch. 8.

128 U.S. Department of Defense, "The U.S. Nuclear Triad," (Washington: DoD, 2018), https://media.defense.gov/2018/Feb/02/2001872882/-1/-1/1/U.S.-NUCLEAR-TRIAD.PDF.

129 Samuel Glasstone and Philip J. Dolan, The Effects of Nuclear Weapons (Washington: DoD, 1977), 479-89 (for scintillation and blackout effects).

130 Fink, "Defense Primer: NC3."

131 U.S. Department of Defense, "Report on the Nuclear Employment Strategy of the United States," (Washington: Office of the Secretary of Defense, November 2024), https://media.defense.gov/2024/Nov/15/2003584623/-1/-1/1/REPORT-ON-THE-NUCLEAR-EMPLOYMENT-STRATEGY-OF-THE-UNITED-STATES.PDF.

132 North Atlantic Treaty Organization, "NATO's nuclear deterrence policy and forces," NATO, updated 24 June 2025, https://www.nato.int/en/what-we-do/deterrence-and-defence/natos-nuclear-deterrence-policy-and-forces.

133 DoD, "Report on Nuclear Employment Strategy."

AI/ML integration offers potential benefits here including improved data fusion, threat correlation, decision-support tools across allied networks, enhanced shared situational awareness, and faster corroborated warning.[134] However, it also introduces risks: AI-driven systems can amplify misperceptions, propagate false positives, or create brittle dependencies if allied inputs diverge or if adversaries have poisoned training data or can manipulate shared data streams.[135] Coordination frameworks such as NATO's Nuclear Planning Group and bilateral consultative mechanisms (e.g., U.S.–South Korea Extended Deterrence Strategy and Consultation Group) provide doctrinal and political alignment, but AI-driven accelerations in sensing and assessment could challenge the human deliberation these bodies were designed to preserve.

4.8 Final Arming and Release: Permissive Action Links

Before most U.S. nuclear weapons can be armed or launched, PALs serve as the last technical safeguard.[136] These electronic locks, embedded in warheads and delivery systems, ensure that only authenticated, authorized commands can enable arming; they are distinct from the broader decision to launch, focusing solely on physical control of the weapon.[137] Unclassified details about modern PALs are not available, but it is believed that PAL codes are tightly held at the highest levels of command, are transmitted as part of the authenticated execution chain, and are safeguarded by dual-operator protocols, split-knowledge arrangements, and mechanical interlocks.[138]

AI/ML integration into this final phase presents both promise and peril. On one hand, advanced verification systems might strengthen positive control (ensuring authorized use) and negative control (preventing unauthorized use) by enhancing authentication processes, anomaly detection, and real-time status monitoring.[139] On the other hand, AI-driven automation could compress human decision time, erode necessary friction, or introduce new vulnerabilities if software controlling arming mechanisms is corrupted, spoofed, or misled by adversarial inputs.[140] Notably, PAL systems were deliberately designed to slow the process, inserting friction to allow for final human oversight—a feature potentially at odds with AI systems tuned for speed and optimization.

4.9 Human-Technical Interface, Adaptive Planning, and Post-Strike Resilience

A defining feature of U.S. NC3 architecture is its human-centered design. Despite reliance on advanced technologies, the system embeds human checks at every critical juncture. Dual-key arrangements, multi-person verification, and split-knowledge procedures aim to reduce the risks of mechanical or automated error.[141] High-reliability systems achieve safety not by eliminating human involvement but by building procedural safeguards and organizational cultures that anticipate inevitable system failures.[142]

134 CNA, Artificial Intelligence in Nuclear Operations: Identifying and Mitigating Risks (Arlington, VA: CNA, April 2023), 29-31, https://www.cna.org/reports/2023/04/Artificial-Intelligence-in-Nuclear-Operations.pdf.
135 Geist and Lohn, "How Might Artificial Intelligence Affect the Risk of Nuclear War?" 18–20.
136 Nuclear Matters Handbook, Ch. 8.
137 Ibid.
138 National Academies of Sciences, Engineering, and Medicine, The Future of the U.S.-Soviet Nuclear Relationship (Washington: The National Academies Press, 1991), Ch. V, "Controlling Strategic Force Operations." https://www.nationalacademies.org/read/1846/chapter/7.
139 CNA, Artificial Intelligence in Nuclear Operations, 26-30.
140 Ibid., 28-25; Geist and Lohn, "How Might Artificial Intelligence Affect the Risk of Nuclear War?" 15, 18-20.
141 Fink, "Defense Primer: NC3."
142 The seminal study on the ways high-reliability organizations can achieve safety by anticipating inevitable system failures and building appropriate organizational cultures and procedural safeguards is Charles Perrow, Normal Accidents: Living with High-Risk Technologies, updated ed. (Princeton: Princeton University Press, 1999); the Department of Energy explicitly incorporates these principles in its personnel training: U.S. Department of Energy, Human Performance Improvement Handbook, vol. 1, Concepts and Principles, 2009 (Reaffirmed 2013), 5-12 through 5-21, https://ism.lbl.gov/ismhop-resources/doe-human-performance-resources.

The NC3 challenge extends beyond ensuring reliable execution of presidential orders. In a protracted nuclear conflict, the system must enable continuous assessment of surviving forces, sustain command and control links, and provide inputs for ANP.[143] Even after absorbing a first strike, the United States must retain some capability to evaluate the status of its SSBN fleet, hardened ICBM forces, and bomber leg, supported by fallback communication systems such as the NAOC, TACAMO aircraft, and EMP-hardened nodes.[144] The survivability of post-strike NC3 determines not only the credibility of deterrence but also the ability to manage escalation, de-escalation, or war termination.

Artificial intelligence could enhance these functions by accelerating battle damage assessment (BDA), fusing satellite, radar, and signals intelligence to generate near-real-time estimates of force survivability. However, such integration introduces risks: algorithmic opacity, adversarial data manipulation, or automated escalation pathways that erode human-centered decision-making under extreme stress.[145] Assuring strategic stability requires not only a capable force posture but also credible and adaptive C2 across all phases of conflict. AI must be incorporated cautiously to support, not supplant, the core human and institutional judgments on which nuclear stability depends.

4.10 Reaffirming the Central Message: Beyond Cold War Deterrence

This exploration underscores a central truth: even if every NC3 component functions flawlessly, nuclear war remains a catastrophic, unwinnable event. While the system's design emphasizes layered controls, redundancy, and human oversight, NC3 today must address a far broader array of global scenarios than those envisioned during the Cold War.[146] Beyond great-power confrontations and deterrence by punishment, the system now must manage regional nuclear crises (e.g., North Korea, South Asia), nuclear-armed terrorist threats, hypersonic weapons with new attack profiles, and cyber-enabled strategic manipulation.[147] It must also support deterrence by denial (e.g., missile defense integration), assurance of allies and partners, and demonstrations of resolve short of nuclear employment.[148]

As this paper transitions to assess the potential role of artificial intelligence in NC3, it is vital to remember that no machine can eliminate the existential dangers embedded in nuclear deterrence. While AI may enhance some technical functions such as early warning data fusion, cyber defense, or ANP, it also introduces new risks, including over-reliance on opaque algorithms, vulnerability to adversarial deception, and the erosion of deliberate, human-centered judgment.[149] The challenge is not merely to modernize NC3, but to ensure that any technological integration preserves the principles of civilian control, human oversight, and strategic stability across a far more complex global nuclear landscape.

In sum, the U.S. NC3 system, as currently configured, is designed not simply as a warfighting apparatus but as a last-resort deterrent, scaffolded by multiple layers of human and technical safeguards. The challenge of the future is to ensure that this system remains resilient, adaptable, and reliable in the face of emerging threats, across both strategic and regional nuclear environments, and under the extreme pressures of both first strike and protracted conflict conditions.

143 DoD, 2022 Nuclear Posture Review, 22.
144 CRS, "Defense Primer: NC3."
145 Peter Rautenbach, "On Integrating Artificial Intelligence With Nuclear Control," Arms Control Today, September 2022. https://www.armscontrol.org/act/2022-09/features/integrating-artificial-intelligence-nuclear-control.
146 DoD, 2018 Nuclear Posture Review, 16.
147 DoD, 2022 Nuclear Posture Review, .5-6.
148 Ibid., 15.
149 CNA, Artificial Intelligence in Nuclear Operations, 18-25; U.S. Government Accountability Office, "Generative AI's Environmental and Human Effects," (Washington: GAO, 22 April 2025), 23-4. https://www.gao.gov/assets/gao-25-107172.pdf.

5. AI and the Future of NC3

From its inception, the U.S. NC3 system has incorporated automation to manage the scale and speed of nuclear threats. The SAGE network pioneered the use of large-scale computers to process radar data and provide real-time tracking and interception guidance, laying the foundation for human-machine integration in command systems.[150] Similarly, BMEWS relied on automated signal processing to filter cluttered radar returns and identify potential missile launches, tasks too difficult for unaided human operators.[151] By the 1970s, the DSP used automated infrared signature recognition to discriminate missile plumes from background clutter, a precursor to pattern-recognition techniques.[152] Each of these steps reflected both the promise and the risks of automation in NC3. Today's advances in AI/ML, however, are of an entirely different order of speed and scope, making it far harder to judge their safest and most effective role.

On the cultural level, more than forty years after dramatizations like *Dr. Strangelove*, *Fail Safe*, and *WarGames*, recent portrayals—including the 2025 film *A House of Dynamite*—continue to fuel public and policymaker anxiety about automation, miscalculation, and the fragility of human control in nuclear crises.

5.1 Potential AI Contributions to NC3 and Ongoing DoD AI-Related Work

Following the scenario outlined in Section 4, this section identifies areas where AI might improve NC3 system performance and considers the applicability of emerging applications of AI/ML to NC3. It then offers specific recommendations for U.S. modernization and addresses broader guidelines for AI governance and international security. Previous sections discussed the policies and strategies governing the NC3 system as well as its architecture, evolution, and enduring challenges—emphasizing throughout the system's critical dependence on human judgment, technical safeguards, and institutional resilience. As AI capabilities advance, often unpredictably, the future of NC3 presents both promising opportunities and sobering risks.

AI's core strengths in speed, pattern recognition, and predictive analytics often challenge NC3 imperatives such as political control, human deliberation, and strategic restraint. For instance, predictive analytics might suggest preemption strategies faster than human decision-makers can politically vet them, while automated pattern recognition could surface ambiguous warning signals that trigger premature alerts.[153]

Some AI/ML tools are already shaping how military decision-makers interpret complex data environments. Project Maven, for example, was launched by DoD in 2017 to integrate AI tools into the analysis of intelligence, surveillance, and reconnaissance (ISR) data, with the goal of accelerating object detection and enabling more efficient downstream targeting processes.[154] While controversial and ultimately curtailed in some industry contexts, Maven remains a reference point for AI integration in defense applications.

As illustrated in the previous scenario, one promising area is early warning data fusion and anomaly detection. The compressed timeline for presidential decision-making depends heavily on the speed and accuracy of data from

150 MIT Lincoln Laboratory, "SAGE: Semi-Automatic Ground Environment Air Defense System," Lincoln Laboratory, https://www.ll.mit.edu/about/history/sage-semi-automatic-ground-environment-air-defense-system.
151 Federation of American Scientists, "BMEWS (Ballistic Missile Early Warning System)," FAS Military Analysis, https://spp.fas.org/military/program/track/bmews.htm.
152 U.S. Space Force, "Defense Support Program Satellites," fact sheet, October 2020, https://www.spaceforce.mil/about-us/fact-sheets/article/2197774/defense-support-program-satellites/.
153 Michael T. Klare, "Skynet Revisited: The Dangerous Allure of Nuclear Command Automation," Arms Control Today, 1 April 2020. https://www.armscontrol.org/act/2020-04/features/skynet-revisited-dangerous-allure-nuclear-command-automation.
154 Cheryl Pellerin, "Project Maven to Deploy Computer Algorithms to War Zone by Year's End," DoD News, 21 July 2017, https://www.war.gov/News/News-Stories/Article/Article/1254719/project-maven-to-deploy-computer-algorithms-to-war-zone-by-years-end/.

missile warning radars, satellite sensors, and intelligence feeds, while also requiring corroborated indications from independent sensors.[155] AI is already being explored to enhance sensor integration, helping distinguish real threats from false positives such as space debris or solar reflections.[156] The MDA, for instance, has experimented with AI-driven algorithms to enhance discrimination of missile trajectories in cluttered environments.[157]

Another critical area is decision-support augmentation. Rather than displacing human judgment, AI systems could help operators model escalation pathways, simulate adversary reactions, and highlight non-obvious options during crises. In practice, this might resemble advanced wargaming tools operating in near real time, drawing on both structured databases and unstructured intelligence to anticipate how an adversary might respond to a particular U.S. move.[158] The aim is not to remove humans from the loop, but to enhance situational awareness and help decision-makers make better-informed choices under extreme stress.

Strengthening communications system resilience is another complex but potentially valuable AI contribution. During crisis scenarios, nuclear command relies on layers of redundant, hardened communication systems; however, these systems remain vulnerable to jamming, spoofing, or cyberattack. AI tools could autonomously detect, reroute, and recover from such disruptions at speeds and scales human operators could not match during high-intensity events. The Defense Advanced Research Projects Agency (DARPA), for example, is developing autonomous cyber defense agents under its "AI Next" portfolio to secure mission-critical networks in contested and degraded environments.[159]

Several ongoing defense initiatives are already laying the groundwork for integrating AI into NC3-relevant domains. DoD's CJADC2 initiative aims to network sensors, shooters, and command nodes across land, sea, air, space, and cyber to create comprehensive kill webs operating inside adversary decision cycles through use of AI-enabled data fusion and analytics.[160] Although CJADC2 is focused on conventional operations, its core tools, such as automated threat detection and real-time information sharing, are directly relevant to strategic forces and NC3 modernization.

Within the Air Force, the Advanced Battle Management System (ABMS) employs AI-driven architectures to compress the "sensor-to-shooter" timeline through cloud computing and resilient mesh networks. While ABMS has not been formally incorporated into nuclear operations, its use of AI-enabled pattern recognition and edge computing could help reinforce future NC3 functions.[161]

DARPA's OFFensive Swarm-Enabled Tactics (OFFSET) and Assured Autonomy programs offer further insights. OFFSET explores managing large swarms of autonomous agents under human supervision—useful for understanding coordination dynamics in complex force postures—while Assured Autonomy aims to certify AI systems' behavior in adversarial or novel settings, a prerequisite for trusting their application to systems with existential stakes.[162]

155 CRS, "Defense Primer: NC3."
156 Linda Kane, Space Systems Command Public Affairs, "Facilitating Intelligent Conversations About Artificial Intelligence," U.S. Space Force, 22 July 2024, https://www.ssc.spaceforce.mil/Newsroom/Article-Display/Article/3846301/facilitating-intelligent-conversations-about-artificial-intelligence.
157 C. Todd Lopez, "Vice Admiral Discusses Potential of AI in Missile Defense Testing, Operations," DoD news release, 12 August 2021, https://www.war.gov/News/News-Stories/Article/Article/2730215/vice-admiral-discusses-potential-of-ai-in-missile-defense-testing-operations/.
158 Although not specific to NC3, the many approaches to AI decision support DoD is pursuing are detailed in U.S. Department of Defense, Data, Analytics and Artificial Intelligence Adoption Strategy: Accelerating Decision Advantage, (Washington: DoD, 2023), 5, https://media.defense.gov/2023/Nov/02/2003333300/-1/-1/1/DOD_DATA_ANALYTICS_AI_ADOPTION_STRATEGY.PDF.
159 DARPA, "AI Next Campaign," Defense Advanced Research Projects Agency, 2021, https://www.darpa.mil/work-with-us/ai-next-campaign.
160 Department of the Air Force, "Summary of the JADC2 Strategy."
161 John R. Hoehn, "Advanced Battle Management System," (Washington: Congressional Research Service, updated 15 February 2022, https://www.congress.gov/crs-product/IF11866.
162 DARPA, "Assured Autonomy," https://www.darpa.mil/program/assured-autonomy; and "OFFSET," https://www.darpa.mil/program/offensive-swarm-enabled-tactics.

Additional ongoing and emerging advances in ML/AI offer a range of applications that may become increasingly relevant to NC3 modernization.[163] Big Data Analytics can identify non-obvious correlations across vast and heterogeneous data sets, potentially improving detection, characterization, and explanation of adversary nuclear-related activity.[164] Expert Systems—software designed to replicate the reasoning of subject matter experts within narrowly defined domains—might support leadership decision-making for specific and bounded tasks within NC3 protocols.[165] Similarly, Computer Vision techniques could accelerate the analysis and interpretation of sensor data, while Natural Language Processing may streamline human–machine communication, reducing latency and error in information transfer.[166] Collectively, these tools point toward the emergence of Predictive Intelligence: the capacity of ML/AI systems to identify or track potential threats before they are apparent to human operators.[167] Yet, realizing these benefits will require rigorous testing, validation, and safeguards to preserve a human-centered design that ensures human judgment remains paramount in nuclear decision processes.[168]

USSTRATCOM has now begun exploring ways AI can enable and accelerate human decision-making across mission domains. However, the United States has not made an explicit policy decision to integrate AI into the critical decision nodes of NC3—a reflection of both prudence and persistent strategic ambivalence. Most analysts contend that AI should remain limited to augmentative functions: sharpening human insight, enhancing system resilience, and accelerating non-lethal operational processes. They caution against assigning AI any role in critical functions such as automating launch authority or executing strategic decisions.[169]

5.2 Recommendations for U.S. NC3 Modernization

The following six recommendations outline principles to guide responsible U.S. NC3 modernization in an era of increasing AI efficacy.

Prioritize resilience and redundancy over raw speed.

AI-enhanced data fusion and decision support can accelerate warning and response cycles, but speed alone is not the metric of success. Automated acceleration risks bypassing sensors needed to corroborate initial indications and compressing decision windows to the point where meaningful human deliberation becomes impossible, mirroring the dynamic that led to tragic outcomes such as the Aegis Cruiser USS *Vincennes* shootdown of Iran Air 655 in 1988.[170]

U.S. NC3 modernization should prioritize resilience: ensuring systems can operate under degraded conditions, withstand adversarial manipulation, and maintain credible deterrence even if key components fail. Architectures must enable graceful degradation, not brittle optimization, so that failure in one component does not cascade

163 European Leadership Network, AI and Nuclear Command, Control and Communications: P5 Perspectives (London: ELN, November 2023), 4, https://europeanleadershipnetwork.org/report/ai-and-nuclear-command-control-and-communications-p5-perspectives/.
164 Arsh Kumar, "The Technicalities of Integrating AI into the NC3," University of Chicago X-Risk Institute (March 2025), 9-13, https://xrisk.uchicago.edu/files/2025/07/What_might_the_integration_of_AI_and_the_NC3_look_like_.pdf.
165 "Artificial Intelligence in Nuclear Command, Control & Communications: A Technical Primer," Institute for Security & Technology (7 September 2025), 6-7, https://securityandtechnology.org/virtual-library/report/ai-nc3-primer.
166 Alexa Wehnsener et al., AI and NC3 Integration in an Adversarial Context: Strategic Stability Risks and Confidence-Building Measures (Oakland: Institute for Security & Technology, February 2023), 26, https://securityandtechnology.org/wp-content/uploads/2023/02/AI-NC3-Integration-in-an-Adversarial-Context.pdf; Lin, "Artificial Intelligence and Nuclear Weapons,
167 Gen. Anthony Cotton, U.S. Strategic Command, "2024 Department of Defense Intelligence Information System Worldwide Conference" (remarks), 28 October 2024, https://www.stratcom.mil/Media/Speeches/Article/3965392/2024-department-of-defense-intelligence-information-system-worldwide-conference/.
168 Fink, "Defense Primer: NC3."
169 Ibid.
170 Malcolm James Cook, "The Dangers of Automation Bias in Air and Missile Defense," Air & Space Power Journal 35, special issue (2021): 49-50, https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-35_Special_Issue/F-Cook.pdf.

ILLUSTRATIVE RISK LEVELS FOR AI-ENABLED NC3 PROCEDURES		
HIGH RISK (POTENTIAL FOR CATASTROPHIC OR IRREVERSIBLE STRATEGIC CONSEQUENCES)	**MEDIUM RISK** (POTENTIAL TO IMPAIR DECISION-MAKING, INCREASE ERROR RATES, OR INTRODUCE INSTABILITY)	**LOW RISK** (LIMITED DIRECT STRATEGIC CONSEQUENCES; PRIMARILY SUPPORT FUNCTIONS)
• AI-DIRECTED NUCLEAR STRIKE EXECUTION WITHOUT HUMAN AUTHORIZATION OR VETO (E.G., AUTONOMOUS LAUNCH PROCEDURES OR AI-GENERATED STRIKE PACKAGES ACTED ON WITHOUT SENIOR HUMAN REVIEW). • AUTOMATED THREAT ASSESSMENT AND LAUNCH-ON-WARNING DECISIONS DRIVEN BY OPAQUE OR UNVERIFIED MODELS, COMPRESSING HUMAN DECISION TIME. • AUTONOMOUS ESCALATION MANAGEMENT OR CRISIS DECISION SUPPORT IN HIGH-TEMPO SCENARIOS, WHERE AI RECOMMENDATIONS ARE TREATED AS AUTHORITATIVE UNDER TIME PRESSURE. • AI-ENABLED SPOOFING DETECTION OR COUNTERMEASURES WITH AUTOMATED RETALIATION TRIGGERS, IF IMPROPERLY DESIGNED, COULD CAUSE UNINTENDED ESCALATION.	• DYNAMIC RECONFIGURATION OF COMMUNICATIONS PATHWAYS THAT INADVERTENTLY BYPASS OR EXCLUDE KEY DECISION-MAKERS, CREATING PARTIAL "DE-FACTO DEVOLUTION" OF AUTHORITY. • AI-ASSISTED TARGETING OR FORCE ALLOCATION THAT COULD MISPRIORITIZE OR MISINTERPRET INTENT UNDER AMBIGUOUS CONDITIONS, INCREASING ESCALATION RISKS. • AUTOMATED ROUTING OF MESSAGES OR TASKING ORDERS THAT LEADS TO INFORMATION BOTTLENECKS, SELECTIVE AMPLIFICATION, OR ACCIDENTAL ISOLATION OF CERTAIN COMMAND NODES. • AUTOMATED INFORMATION TRIAGE AND PRIORITIZATION IN COMMAND CENTERS THAT RESHAPES HOW LEADERS SEE THE BATTLESPACE, POSSIBLY BIASING DECISIONS.	• ROUTINE MONITORING AND DIAGNOSTICS OF NUCLEAR FORCE STATUS, EARLY WARNING SENSORS, AND COMMUNICATIONS LINKS TO SUPPORT SITUATIONAL AWARENESS. • PREDICTIVE MAINTENANCE AND LOGISTICS SCHEDULING FOR NC3 INFRASTRUCTURE (E.G., ANTENNAS, HARDENED COMM NODES), IMPROVING EFFICIENCY BUT WITH MINIMAL DIRECT STRATEGIC EFFECT. • ENVIRONMENTAL AND SYSTEM HEALTH MONITORING, ANOMALY FLAGGING, AND OTHER LOW-STAKES DECISION SUPPORT FOR OPERATORS. • TRAINING SIMULATORS AND EXERCISES USING AI TO REPLICATE ADVERSARY BEHAVIOR FOR OPERATOR PREPAREDNESS.

into systemic collapse.[171] Modernization efforts must explicitly reject the false tradeoff between speed and survivability; strategic stability hinges less on tactical tempo than on assured control and deliberate restraint. Redundancy and resilience, not reactivity, are the foundations for a credible second-strike posture.[172]

Build explainability and independent auditability.

Commanders and civilian leaders must understand why an AI system produces a given assessment or recommendation. This requires designing for explainability, not just technical performance, but this can be a significant challenge, particularly as AI systems become increasingly capable. Employing transparent logic paths and easily understood sequential steps can improve explainability and is critical to ensuring human trust in high-stakes domains such as national security.[173]

Independent auditability—using red-team exercises, adversarial stress testing, and continuous verification—is essential to ensuring that trust in AI systems is earned, not assumed.[174] Proprietary systems and over-compartmentalization remain key barriers to explainability and accountability. Trustworthy AI integration into NC3 demands not only transparent logic paths, but also formalized, institutional oversight embedded in both peacetime

171 Department of Defense, DoD C3 Modernization Strategy, DoD Chief Information Officer, 10-12, https://dodcio.defense.gov/Portals/0/Documents/DoD-C3-Strategy.pdf; Federation of American Scientists, "Artificial Intelligence, and Nuclear Command, Control, and Communications," (Washington: Federation of American Scientists, July 2025), https://fas.org/wp-content/uploads/2025/07/June2025_AIxNC3_FAS.pdf

172 DoD, 2022 Nuclear Posture Review, 23-4.

173 A seminal work on alignment is Brian Christian, The Alignment Problem: Machine Learning and Human Values (New York: W. W. Norton, 2020). Alignment of AI and NC3 is a focus in Kumar, "The Technicalities of Integrating AI into the NC3," 12-15.

174 National Security Commission on Artificial Intelligence, Final Report, Ch. 7, "Establishing Justified Confidence in AI Systems," (Washington: NSCAI, 2021), https://reports.nscai.gov/final-report/chapter-7.

governance and crisis execution frameworks.[175] Without these safeguards, strategic ambiguity can metastasize into miscalculation. Systems lacking transparency or external scrutiny are unacceptable risks in nuclear operations.

Move beyond superficial "human-in-the-loop" models.

History and studies show that nominal human oversight often collapses under time pressure, system complexity, automation bias, or cognitive overload—particularly when decisions on potential nuclear use may have existential consequences. AI integration into NC3 must adopt human-centered system design: extending, not replacing, human judgment.[176]

Human-centered design means deliberately shaping interfaces, workflows, and feedback loops to empower reflection, not just reaction. For example, interfaces could present scenario-based tradeoffs rather than binary options, allowing time for civilian leaders to explore diplomatic or non-kinetic responses.[177] Designing for decision quality rather than decision speed enables the preservation of political judgment and normative constraints in moments of extreme uncertainty. A meaningful human role must be structurally embedded, not left as a procedural formality or cosmetic safeguard.

Harden against adversarial AI and cyber threats.

Integrating AI increases the NC3 attack surface, exposing it to adversarial machine learning attacks, data poisoning, and deception operations. Systems must be robust not only against environmental degradation but also to active, adaptive adversaries.

AI components in NC3 require the highest standards of validation, verification, and adversarial resilience, with continuous monitoring for anomalous behaviors and emergent risks.[178] While AI acts as a force multiplier, it also introduces critical vulnerabilities, serving as a new attack vector susceptible to adversarial exploitation. Future-proofing NC3 means anticipating potential emergent behavior and novel threat modes that blend technical subversion with strategic ambiguity. Cyber resilience must be a baseline, not an afterthought.[179] In NC3 contexts, these risks are magnified by the stakes involved: even minor manipulations could have strategic consequences.

Prepare for multi-AI interaction and strategic stability challenges.

The United States must anticipate that peer competitors, particularly China and Russia, will integrate increasingly sophisticated AI into their own NC3 systems.[180] This raises novel challenges beyond deterring human adversaries and requires management of interactions between machine-mediated decision loops that operate with partial autonomy.

U.S. NC3 systems should be designed to detect, understand, and respond flexibly to adversary AI behaviors, including deception, misdirection, and rapid adaptation. These challenges are compounded by the growing likelihood of interactions between semi-autonomous systems across rival NC3 architectures, posing novel risks to strategic stability.[181] The introduction of AI into NC3 creates the prospect of emergent escalation dynamics, where unintended feedback loops between opaque systems amplify uncertainty and compress reaction time.

175 Ibid., 115–120, https://www.nscai.gov; David Danks and Alex John London, "Algorithmic Bias in Autonomous Systems," Proceedings of the 26th International Joint Conference on Artificial Intelligence (2017): 4691–4697, https://www.ijcai.org/proceedings/2017/0654.pdf.

176 U.S. Department of Defense, "DOD Adopts 5 Principles of Artificial Intelligence Ethics," press release, 25 February, DOD Adopts 5 Principles of Artificial Intelligence Ethics > U.S. Department of War > Release | U.S. Department of War

177 Ibid.

178 National Security Commission on Artificial Intelligence, Final Report, Ch. 7.

179 Ibid., Ch. 1; Will Roper, "There Is No AI Safety Without Cybersecurity," War on the Rocks, 19 September 2023.

180 CNA, Artificial Intelligence in Nuclear Operations, 10-13.

181 National Security Commission on Artificial Intelligence, Final Report, Ch. 5; Paul Scharre, "Debunking the AI Arms Race Theory," Texas National Security Review, 4, no. 3 (June 2021): 121-32, https://tnsr.org/wp-content/uploads/2021/06/TNSR-Vol-4-Issue-3-Scharre.pdf.

Guardrails for machine-to-machine deterrence are urgently needed.[182] This represents an entirely new dimension of deterrence theory, where stability must be maintained not just among states, but among their algorithmic proxies.

Leverage adaptive nuclear planning and post-attack assessment tools.

AI can assist in ANP for initial response options and in recalibrating nuclear posture after an initial strike, helping assess surviving forces, communication pathways, and escalation management options. For example, AI-enhanced battle damage assessment could recommend rerouting communications via unexpected or underutilized assets and assist in confirming the status of second-strike capabilities more rapidly than traditional methods.[183]

Yet these benefits come with profound risks. Unless carefully bounded, such systems could inadvertently enable automated escalation. ANP tools should augment human decision-making, not bypass it. Programs of record like DARPA's AI-assisted post-strike assessment tools—such as those developed under its ACE (Air Combat Evolution) and Mosaic Warfare concepts—should be closely monitored and evaluated for strategic and operational impact.[184]

These efforts must also be integrated in parallel with broader CJADC2 architectures to ensure cross-domain coherence. Strategic adaptability must never devolve into automated escalation. The goal is not to automate nuclear warfighting, but to use AI to safeguard continuity, clarity, and command in the most extreme conditions imaginable.[185]

5.3. Broader Recommendations for U.S. AI Governance and Global Security

AI may prove to be the most consequential technology humanity has ever developed. Because it is likely to generate profound disruptions—including "unknown unknowns"—across every domain of activity, any recommendations about incorporating AI in NC3 must be embedded within broader frameworks for governance, human agency, and global security. These include robust institutions, technical norms, democratic values, and layered safeguards that can sustain accountability and control as AI capabilities evolve.

Anticipate discontinuous AI breakthroughs, including superintelligence.

A central uncertainty in AI development is whether progress will proceed incrementally, or leap forward through sudden, discontinuous breakthroughs with destabilizing consequences. Recent advances in general-purpose AI and large-language models (LLMs) have surprised even leading experts, demonstrating that progress in this field is nonlinear and difficult to predict. It is plausible that just one or two future innovations could yield superintelligent agents—systems that vastly exceed human cognitive capacities and decision-making abilities.[186] Indeed, it seems likely that the modernized NC3 systems now being deployed may be operating in an era of superintelligence, even if they do not last as long as the systems that are being replaced.

182 Lt. Gen. John "Jack" N.T. Shanahan, "Artificial Intelligence and Nuclear Command and Control: It's Even More Complicated Than You Think," Arms Control Today, September 2025, https://www.armscontrol.org/act/2025-09/features/artificial-intelligence-and-nuclear-command-and-control-its-even-more.

183 "Artificial Intelligence in Nuclear Command, Control & Communications: A Technical Primer," 3.

184 Stew Magnuson, "DARPA Tiles Together a Vision of Mosaic Warfare: Banking on Cost-effective Complexity to Overwhelm Adversaries," https://www.darpa.mil/news/features/mosaic-warfare; Geist and Lohn, "How Might Artificial Intelligence Affect the Risk of Nuclear War?" 17-19.

185 Zachary Kallenborn, "Giving an AI Control of Nuclear Weapons: What Could Possibly Go Wrong?" Bulletin of the Atomic Scientists, 1 February 2022 https://thebulletin.org/2022/02/giving-an-ai-control-of-nuclear-weapons-what-could-possibly-go-wrong/.

186 An early and seminal work on superintelligence is Nick Bostrom, Superintelligence: Paths, Dangers, Strategies (Oxford: Oxford University Press, 2014); Deep Ganguli et al., "Predictability and Surprise in Large Generative Models," arXiv, 15 February 2022, 1-26; https://arxiv.org/pdf/2202.07785; Dan Milmo, "Godfather of AI shortens odds of the technology wiping out humanity over next 30 years," The Guardian, 27 December 2024, https://www.theguardian.com/technology/2024/dec/27/godfather-of-ai-raises-odds-of-the-technology-wiping-out-humanity-over-next-30-years.

U.S. national security planners, including those responsible for NC3, must immediately begin scenario planning for the possibility that future actors—state or non-state—may develop and deploy superintelligent systems.[187] Current NC3 architectures are wholly unprepared for this eventuality. Merely modernizing within today's paradigm could expose the United States to novel, existential vulnerabilities. Early recognition of these risks, and institutional planning to address them, is essential to preserve strategic stability in the coming decades.

While often associated with futurist thinkers like Ray Kurzweil—who popularized the concept of a technological "singularity" as a moment when accelerating AI capabilities transform society and biology beyond recognition—the core idea that artificial systems could surpass human intelligence has moved from speculative literature into serious policy discourse.[188] Although Kurzweil's vision was largely optimistic—forecasting a peaceful and voluntary coevolution between humans and machines by the end of the twenty-first century—the strategic implications of this transition must now be reconsidered in light of emerging threats and governance challenges.

Rebalance U.S. public-private roles in AI development and curtail racing.

The United States currently relies heavily on private-sector innovation to drive AI development, while China has adopted a model centered on state-owned enterprises and coordinated national investment.[189] Neither model, as currently structured, adequately prioritizes long-term safety, democratic accountability, or civil-military balance.[190] In both systems, incentives for rapid deployment are likely to outweigh the incentives for safety, verification, and restraint.

Unconstrained competition—whether within or between these models—could deepen existential risk. The United States urgently needs robust federal governance structures to shape how private AI developments are integrated into national security systems, including NC3. Cautionary principles—such as enforcing hard limits on autonomy, institutionalizing red-team testing, and ensuring that innovation does not outpace safety assurance—must be built into all aspects of U.S. AI policy and govern AI development.[191]

Develop international norms and agreements on AI in nuclear systems.

At present, there are no binding international agreements, or even shared norms, governing the use of AI in nuclear decision-making.[192] This is an extraordinary and dangerous vacuum, given the stakes involved. The United States should lead efforts to convene bilateral and multilateral discussions with other nuclear powers, especially China and

187 National Security Commission on Artificial Intelligence, Final Report, Ch. 1.

188 Perhaps the most important work on the singularity is Ray Kurzweil, The Singularity Is Near: When Humans Transcend Biology (New York: Viking, 2005). Jeremy Baum and John Villasenor, "How close are we to AI that surpasses human intelligence?" Brookings, 18 July 2023, https://www.brookings.edu/articles/how-close-are-we-to-ai-that-surpasses-human-intelligence.

189 Stanford HAI, 2025 AI Index Report (Stanford: Stanford Human-Centered Artificial Intelligence, 2025), https://hai.stanford.edu/assets/files/hai_ai-index-report-2025_chapter4_final.pdf.

190 National Telecommunications and Information Administration, AI Accountability Policy Report (27 March 2024), https://www.ntia.gov/sites/default/files/2024-04/ntia-ai-report-print.pdf; International Committee of the Red Cross, "The (im)possibility of responsible military AI governance," Law & Policy Blog, 12 December 2024, https://blogs.icrc.org/law-and-policy/2024/12/12/the-im-possibility-of-responsible-military-ai-governance/; The White House, "Memorandum on Advancing the United States' Leadership in Artificial Intelligence; Harnessing Artificial Intelligence to Fulfill National Security Objectives; and Fostering the Safety, Security, and Trustworthiness of Artificial Intelligence," 24 October 2024, https://bidenwhitehouse.archives.gov/briefing-room/presidential-actions/2024/10/24/memorandum-on-advancing-the-united-states-leadership-in-artificial-intelligence-harnessing-artificial-intelligence-to-fulfill-national-security-objectives-and-fostering-the-safety-security.

191 Marietje Schaake, The Tech Coup: How to Save Democracy from Silicon Valley (Princeton: Princeton University Press, 2024), 215-219; Jonas Schuett et al., "Towards Best Practices in AGI Safety and Governance: A Survey of Expert Opinion," arXiv preprint, 11 May 2023, https://arxiv.org/abs/2305.07153; Markus Anderljung et al., "Frontier AI Regulation: Managing Emerging Risks to Public Safety," arXiv preprint, 6 July 2023, https://arxiv.org/abs/2307.03718; Special Competitive Studies Project, "AI RedTeaming and Assurance: Recommendations for the U.S. Government," July 2024, https://www.mitre.org/sites/default/files/2024-07/PR-24-01820-4-AI-Red-Teaming-Advancing-Safe-Secure-AI-Systems.pdf.

192 Fei Su; Vladislav Chernavskikh and Wilfred Wan, Advancing Governance at the Nexus of Artificial Intelligence and Nuclear Weapons (Stockholm: Stockholm International Peace Research Institute , March 2025), https://www.sipri.org/publications/2025/sipri-insights-peace-and-security/advancing-governance-nexus-artificial-intelligence-and-nuclear-weapons.

Russia, aimed at developing confidence-building measures, transparency protocols, and agreements on limits to AI integration in NC3 systems.[193]

Such norms might include bans on fully automated launch decisions, formalized "human-in-the-loop" requirements, or even AI-to-AI communication hotlines to mitigate risks of machine-initiated escalation. While advancing toward these goals is likely to be difficult, even incremental progress could reduce miscalculation risks and bolster strategic stability.[194]

Push for global AI governance that safeguards human agency.

The global trajectory of AI development is increasingly raising fundamental questions about human agency, political freedom, and the future of democratic governance. China's model of using AI to enhance domestic surveillance and social control is becoming more dangerously attractive as a tool of repression to authoritarian regimes worldwide.[195] Rather than competing to replicate this model in the military domain, the United States should demonstrate that liberal democratic governance can develop and deploy powerful AI systems in ways that preserve, rather than erode, human autonomy.[196]

One promising approach is the development of participatory correction frameworks—systems that allow qualified human operators to flag, annotate, or revise AI-generated outputs. Inspired by platforms like Wikipedia, these tools could enable institutional memory, versioned audit trails, and distributed human oversight.[197] Open, timely, and validated user corrections rather than closed, periodic, and opaque training sessions or model updates might be among the most effective ways to build hybrid human-AI oversight models that can enhance trust and alignment while advancing human agency in interactions with open AI systems.[198] Development of such participatory mechanisms among teams of cleared users whose expertise spans across ethics, computer science, and nuclear operations would seem to be critical for closed AI systems for NC3, where decisions involve existential threats, uncertainty, ambiguity, and value-laden tradeoffs that cannot be resolved by algorithm alone.[199]

193 Jacob Stokes, Colin H. Kahl, Andrea KendallTaylor & Nicholas Lokker, Averting AI Armageddon: U.S.-China-Russia Rivalry at the Nexus of Nuclear Weapons and Artificial Intelligence (Washington: Center for a New American Security, 13 February 2025), https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/Averting-AI-Armageddon_TSP-IPS_2025_finalB_021325.pdf.

194 Shanahan, "Artificial Intelligence and Nuclear Command and Control: It's Even More Complicated Than You Think."

195 Freedom House, The Repressive Power of Artificial Intelligence, Freedom on the Net 2023 (Washington: Freedom House, 2023), https://freedomhouse.org/article/new-report-advances-artificial-intelligence-are-amplifying-crisis-human-rights-online; National Endowment for Democracy, Data-Centric Authoritarianism: How China's Frontier Tech Globalizes Repression (Washington: NED, 2025), https://www.ned.org/wp-content/uploads/2025/02/NED_FORUM-China-Emerging-Technologies-Report.pdf; The Bulletin of the Atomic Scientists, "How AI Surveillance Threatens Democracy Everywhere," 19 June 2024, https://thebulletin.org/2024/06/how-ai-surveillance-threatens-democracy-everywhere/; Justin B. Bullock, Samuel Hammond & Seb Krier, "AGI, Governments, and Free Societies," arXiv preprint, 14 March 2025, https://arxiv.org/abs/2503.05710; Samantha Hoffman, "Engineering Global Consent: The Chinese Communist Party's Data-Driven Power Expansion," ASPI Policy Brief, October 2019. https://www.aspi.org.au/report/engineering-global-consent-chinese-communist-partys-data-driven-power-expansion.

196 Ian Bremmer and Mustafa Suleyman, "The AI Power Paradox: Can States Learn to Govern Artificial Intelligence -- Before It's Too Late?", Foreign Affairs, 102, no. 5 (September/October 2023).

197 Laxmiraju Kandikatla and Branislav Radeljić, "AI and Human Oversight: A RiskBased Framework for Alignment," arXiv (10 October 2025), https://arxiv.org/abs/2510.09090; Trilateral Research, "Human-in-the-loop AI balances automation and accountability," 4 June 2025, https://trilateralresearch.com/responsible-ai/human-in-the-loop-ai-balances-automation-and-accountability; David Manheim & Aidan Homewood, "Is human oversight to AI systems still possible?," New Biotechnology 85 (March 2025): 59–62, https://www.sciencedirect.com/science/article/pii/S1871678424005636; Aaron Halfaker and R. Stuart Geiger, "ORES: Lowering Barriers with Participatory Machine Learning in Wikipedia," Proceedings of the ACM on Human-Computer Interaction 4, CSCW2 (Oct. 2020): Article 148, 1–37, https://arxiv.org/abs/1909.05189.

198 Eduardo Mosqueira-Rey et al., "Human-in-the-loop Machine Learning: A State of the Art," Artificial Intelligence Review 56 (2023): 3005-54, https://link.springer.com/article/10.1007/s10462-022-10246-w; Melanie J. McGrath et al., "Collaborative Human-AI Trust (CHAI-T): A Process Framework for Active Management of Trust in Human-AI Collaboration," Computers in Human Behavior: Artificial Humans 6 (December 2025): 100200, https://www.sciencedirect.com/science/article/pii/S2949882125000842; Rishub Jain et al., "Human-AI Complementarity: A Goal for Amplified Oversight," arXiv, 30 October 2025, https://arxiv.org/abs/2510.26518.

199 Kandikatla and Radeljić, "AI and Human Oversight"; Walt Woods, Alexander Grushin, Simon Khan, and Alvaro Velasquez, "Combining AI Control Systems and Human Decision Support via Robustness and Criticality," arXiv, 2024, https://arxiv.org/pdf/2407.03210

Invest in global research on AI safety and alignment.

Although national security imperatives will continue to shape U.S. AI strategy, the most dangerous risks posed by advanced AI systems, especially those approaching general intelligence, are global in nature. The United States should lead international coalitions to fund and share research on AI safety, alignment, and control. This includes supporting efforts on formal verification, interpretability, value alignment, and safe system shutdown mechanisms.

More study and testing are needed, but one high-assurance design strategy that would help to address these concerns is developing multiple fully independent AI NC3 systems—one operating day-to-day, and two others held in isolation to provide cross-checked recommendations during elevated alert situations. Project Maven, for example, employed multiple vendors to train separate models for object detection, using overlapping outputs to validate assessments.[200] Similar plural-model designs could be used in NC3 as a form of algorithmic voting or structured dissent—surfacing ambiguity, flagging anomalies and potential emergent behavior, and preventing dangerous overconfidence in any single system's output.[201] Designing for disagreement, rather than assuming consensus, is not only a technical safeguard; it is a way to preserve trade space for political judgment under stress.

Build defense-in-depth and plan for failures.

Because the technologies and processes surrounding NC3 and AI each independently pose existential risks, the utmost scrutiny and the highest levels of safety are warranted when considering how they might be combined. The safeguards outlined above should be embedded within a proactive, multi-layered defense-in-depth architecture that draws from nuclear safety, cybersecurity, and aviation risk management: multiple independent barriers, each able to slow, contain, or correct failures at different stages of the AI lifecycle. No single measure is relied upon; redundancy is deliberate and failures at one layer may still be corrected at another layer.

Layer 1—Prevention: Avoid unsafe capability surges by controlling inputs. This includes national and international licensing of high-performance training clusters, mandatory safety evaluations before scaling models beyond defined thresholds, and "slowed release" protocols that stage deployment from vetted researchers to wider access. Standardized pre-deployment alignment benchmarks—measuring truthfulness, corrigibility, and resistance to deception—must be met before any high-capability system is scaled.[202]

Layer 2—Containment: Restrict what the AI can autonomously do if alignment fails. Superintelligence systems should be developed and tested in sandboxed environments, with strict capability gating for NC3 as well as other high-risk domains such as biotech, finance, and critical infrastructure. Independent tripwire systems must halt activity if dangerous behavior is detected, and physically isolated "kill switches" must allow immediate shutdown outside of AI control.[203]

Layer 3—Correction: Maintain continuous human-in-control human-AI hybrid models during deployment. Here, the participatory "Wikipedia model" becomes a core safeguard. Vetted domain experts and distributed oversight panels can review, flag, and correct AI outputs in real time, using transparent, version-controlled alignment parameters that can be rolled back or updated rapidly. All high-impact AI decisions would be logged in accessible audit trails, enabling institutional memory and public or expert scrutiny. Plural-model verification reinforces this process by cross-checking outputs across independently trained systems, surfacing discrepancies, and preventing

200 Patrick Tucker, "How the Military's Project Maven Is Learning to See," Defense One, 8 November 2018, https://www.defenseone.com/technology/2018/11/how-militarys-project-maven-learning-see/152072.

201 Rian Adam Rajagede, et al., "NAPER: Fault Protection for Real-Time Resource-Constrained Deep Neural Networks," arXiv, 9 April 2025, https://arxiv.org/pdf/2504.06591; John deVadoss and Matthias Artzt, "A Byzantine Fault Tolerance Approach towards AI Safety," preprint, 20 April 2025, https://www.researchgate.net/publication/390991740_A_Byzantine_Fault_Tolerance_Approach_towards_AI_Safety; Future of Life Institute and Strategic Foresight Group, "Framework for Responsible Use of AI in the Nuclear Domain," policy brief (5 February 2025), https://futureoflife.org/wp-content/uploads/2025/02/Policy-Briefing-Responsible-AI-in-Nuclear-Domain-v3.pdf.

202 National Institute of Standards and Technology (NIST). AI Risk Management Framework (AI RMF 1.0). Gaithersburg, MD: U.S. Department of Commerce, 2023. 12–21. https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf.

203 NIST. Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities. Gaithersburg: U.S. Department of Commerce, February 2022. 7–13. https://csrc.nist.gov/pubs/sp/800/218/final.

overconfidence in a single model. Combined, these socio-technical mechanisms enable rapid correction cycles measured in minutes to hours, while avoiding single points of failure through geographically and institutionally dispersed alignment servers.[204]

Layer 4—Resilience: Ensure that even highly capable AI systems cannot displace human autonomy in critical decisions. This requires formal human-in-control rules for nuclear, medical, and financial systems; decentralization of AI development to prevent monopoly control; broad AI literacy and oversight training; and democratic alignment councils capable of adjudicating disputes and setting binding policy. Plural-model designs can support resilience by providing structured dissent—ensuring that divergent assessments reach human decision-makers rather than being collapsed into a single "consensus" output and potentially spotlighting dangerous emergent behaviors. Embedding constitutional constraints grounded in human rights principles at the system's core can help anchor autonomy in moments of stress.[205]

Layer 5—Global Coordination: Prevent a destabilizing race dynamic. International AI safety treaties, modeled on nuclear arms control, should mandate capability transparency, establish shared safety research hubs, and define joint crisis protocols to pause development if dangerous emergent behaviors are detected.[206]

This layered strategy—prevention, containment, correction, resilience, and coordination—is not about guaranteeing perfect safety. It is about ensuring that AI failures are survivable, controllable, and recoverable, even under the most adverse conditions. For NC3, adopting such a defense-in-depth architecture may prove the difference between strategic stability and catastrophe in the age of superintelligence.

Institutionalize safeguards.

A crucial gap in current AI governance is the absence of a dedicated, legally empowered body responsible for certifying AI systems used within NC3. Existing oversight mechanisms are woefully inadequate; they are not designed to assess non-deterministic systems that may evolve over time, interact in complex ways, and require continuous validation monitoring for initial certification and recertification. One promising approach would be to establish a National NC3 AI Certification Authority, drawing on technical expertise from the DoD, the intelligence community, federally funded research and development centers, and independent civilian experts. Such an authority would set minimum performance, robustness, explainability, cybersecurity, and governance standards for any AI system intended for NC3 use. It would also oversee independent testing, phased deployment reviews, and mandatory re-certification when models or their operational environments change materially. Additional study is needed regarding appropriate institutional designs for such an authority or other urgently needed AI oversight and control mechanisms, particularly for NC3.

Collectively, these measures—combined with enhanced education, sustained research, institutional innovation, and international engagement—would move AI-enabled NC3 modernization from aspirational safeguards toward verifiable, enforceable, and adaptive risk management standards.

204 Eduardo Mosqueira-Rey, et al. "Human-in-the-loop machine learning"; Joni Myllyaho et al., "Systematic literature review of validation methods for AI systems." arXiv preprint (2021). https://arxiv.org/abs/2107.12190.

205 Sarah Sterz et al., "On the Quest for Effectiveness in Human Oversight: Interdisciplinary Perspectives." arXiv preprint, 5 April 2024. https://arxiv.org/abs/2404.04059.

206 Nicholas EmeryXu, Richard Jordan; and Robert Trager, "International Governance of Advancing Artificial Intelligence," AI & Society 40 (2025): 3019–3044. https://link.springer.com/article/10.1007/s00146-024-02050-7.

Conclusion

The future of NC3 will not be shaped solely by new sensors, hardened communications, or updated software. It will be shaped by how AI is governed, how humans retain control, and whether stability can be maintained under pressure. Recent developments, including Ukraine's unprecedented drone strikes on 1 June 2025 against Russian nuclear-capable aircraft on widely dispersed airfields, underscore how asymmetric tactics, real-time data flows, and distributed decision-making are already testing legacy nuclear structures.[207]

AI offers both extraordinary opportunities and unprecedented risks for the future of NC3. As this paper emphasized, the core challenge is not simply technical modernization or faster decisions, but preserving the central principles of civilian control, strategic restraint, and political deliberation in an era of rapid and unpredictable change. By integrating AI cautiously and transparently into NC3 systems—while building layered safeguards, anticipating adversary behavior, and shaping global norms—the United States can strengthen its deterrent posture and demonstrate international leadership in responsible AI governance.

207 Masao Dahlgren and Lachlan MacKenzie, "Ukraine's Drone Swarms Are Destroying Russian Nuclear Bombers. What Happens Now?" Critical Questions, CSIS, 4 June 2025, https://www.csis.org/analysis/ukraines-drone-swarms-are-destroying-russian-nuclear-bombers-what-happens-now.

Acronyms

ACRONYM	FULL TERM	DESCRIPTION
ABM	ANTI-BALLISTIC MISSILE	REFERS TO SYSTEMS OR TREATIES DESIGNED TO INTERCEPT AND DESTROY INCOMING BALLISTIC MISSILES.
ABMS	ADVANCED BATTLE MANAGEMENT SYSTEM	U.S. AIR FORCE PROGRAM USING AI AND CLOUD ARCHITECTURE FOR FASTER COMMAND AND CONTROL.
ABNCP	AIRBORNE NATIONAL COMMAND POST	AIRCRAFT WITH EQUIPMENT AND PERSONNEL NEEDED TO EXECUTE ALL NC3 FUNCTIONS.
AEAO	AIRBORNE EMERGENCY ACTION OFFICER	SENIOR OFFICER ABOARD THE ABNCP RESPONSIBLE FOR EXECUTING NUCLEAR OPERATIONS IF GROUND-BASED CONTROL IS LOST.
AEHF	ADVANCED EXTREMELY HIGH FREQUENCY	SECURE MILITARY SATELLITE COMMUNICATIONS SYSTEM FOR PROTECTED, JAM-RESISTANT LINKS.
AI	ARTIFICIAL INTELLIGENCE	MACHINE-BASED SYSTEMS CAPABLE OF PERFORMING TASKS THAT NORMALLY REQUIRE HUMAN INTELLIGENCE.
ALCS	AIRBORNE LAUNCH CONTROL SYSTEM	ENABLES AIRBORNE CREWS TO LAUNCH ICBMS IF GROUND-BASED CONTROL IS COMPROMISED.
AN/TPY-2	ARMY/NAVY TRANSPORTABLE RADAR SURVEILLANCE—MODEL 2	PHASED-ARRAY RADAR USED IN BALLISTIC MISSILE DEFENSE, PART OF THAAD SYSTEM.
ANP	ADAPTIVE NUCLEAR PLANNING	CAPABILITY ALLOWING NUCLEAR PLANS TO BE RAPIDLY ADAPTED TO UNFOLDING CRISIS CONDITIONS.
A2/AD	ANTI-ACCESS/AREA DENIAL	ADVERSARY CAPABILITIES AIMED AT PREVENTING U.S. FORCES FROM ENTERING OR OPERATING FREELY IN A REGION.
BDA	BATTLE DAMAGE ASSESSMENT	POST-STRIKE ASSESSMENT OF FORCE SURVIVABILITY AND TARGET EFFECTS.
BMEWS	BALLISTIC MISSILE EARLY WARNING SYSTEM	GROUND-BASED RADAR NETWORK PROVIDING EARLY DETECTION OF INCOMING ICBMS.
C2	COMMAND AND CONTROL	THE EXERCISE OF AUTHORITY AND DIRECTION OVER ASSIGNED FORCES.
CEC	COOPERATIVE ENGAGEMENT CAPABILITY	ENABLES SENSORS AND WEAPONS TO WORK TOGETHER IN A NETWORKED KILL WEB.
CJADC2	COMBINED JOINT ALL-DOMAIN COMMAND AND CONTROL	DOD INITIATIVE TO INTEGRATE DATA ACROSS SERVICES AND DOMAINS USING AI AND CLOUD COMPUTING.

ACRONYM	FULL TERM	DESCRIPTION
DRSN	DEFENSE RED SWITCH NETWORK	HIGHLY SECURE VOICE COMMUNICATIONS NETWORK FOR U.S. LEADERSHIP.
DOD	DEPARTMENT OF DEFENSE	U.S. FEDERAL AGENCY RESPONSIBLE FOR NATIONAL SECURITY AND THE ARMED FORCES.
DSP	DEFENSE SUPPORT PROGRAM	SATELLITE CONSTELLATION PROVIDING INFRARED EARLY MISSILE LAUNCH DETECTION.
E4B	NATIONAL AIRBORNE OPERATIONS CENTER	“DOOMSDAY PLANE” AIRCRAFT THAT SUPPORTS PRESIDENTIAL COMMAND DURING CRISIS.
EAM	EMERGENCY ACTION MESSAGE	AUTHENTICATED NUCLEAR EXECUTION ORDERS.
EHF	EXTREMELY HIGH FREQUENCY	A PROTECTED RADIO SPECTRUM BAND USED FOR SECURE SATELLITE COMMUNICATIONS.
EMP	ELECTROMAGNETIC PULSE	A BURST OF ELECTROMAGNETIC RADIATION THAT CAN DAMAGE OR DISABLE ELECTRONIC SYSTEMS.
ESS	EVOLVED STRATEGIC SATCOM	NEXT-GENERATION SATELLITE COMMUNICATION SYSTEM REPLACING AEHF.
FAB-T	FAMILY OF ADVANCED BEYOND LINE-OF-SIGHT TERMINALS	TERMINALS ENABLING SECURE SATELLITE-BASED COMMUNICATION.
FOBS	FRACTIONAL ORBITAL BOMBARDMENT SYSTEM	WEAPON SYSTEM THAT PLACES A NUCLEAR WARHEAD INTO LOW-EARTH ORBIT BEFORE REENTRY.
FORGE	FUTURE OPERATIONALLY RESILIENT GROUND EVOLUTION	PROGRAM MODERNIZING GROUND SYSTEMS SUPPORTING SPACE-BASED MISSILE WARNING.
GWEN	GROUND WAVE EMERGENCY NETWORK	COLD WAR-ERA RADIO SYSTEM PROVIDING REDUNDANT COMMUNICATIONS.
HBTSS	HYPERSONIC AND BALLISTIC TRACKING SPACE SENSOR	SPACE-BASED SYSTEM FOR TRACKING HYPERSONIC AND BALLISTIC MISSILES.
ICBM	INTERCONTINENTAL BALLISTIC MISSILE	LONG-RANGE BALLISTIC MISSILE CAPABLE OF DELIVERING NUCLEAR WARHEADS.
ISR	INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE	THE COORDINATED COLLECTION AND ANALYSIS OF INFORMATION ABOUT ADVERSARIES AND ENVIRONMENTS.
JSTPS	JOINT STRATEGIC TARGET PLANNING STAFF	COLD WAR-ERA JOINT STAFF THAT DEVELOPED NUCLEAR TARGETING PLANS.
LEO	LOW EARTH ORBIT	A REGION OF SPACE TYPICALLY UP TO 2,000 KM ABOVE EARTH’S SURFACE.
LF	LOW FREQUENCY	A RADIO FREQUENCY RANGE USED FOR SECURE COMMUNICATIONS.
LLM	LARGE LANGUAGE MODEL	AI MODELS TRAINED ON VAST TEXT DATA FOR REASONING AND GENERATION (E.G., GPT-4).
MAD	MUTUAL ASSURED DESTRUCTION	COLD WAR-ERA STRATEGIC DOCTRINE DETERRING NUCLEAR WAR THROUGH GUARANTEED RETALIATION.
MDA	MISSILE DEFENSE AGENCY	U.S. AGENCY RESPONSIBLE FOR DEVELOPING AND FIELDING MISSILE DEFENSE SYSTEMS.
MILSTAR	MILITARY STRATEGIC AND TACTICAL RELAY	SATELLITE COMMUNICATION SYSTEM USED FOR SECURE MILITARY OPERATIONS.

ACRONYM	FULL TERM	DESCRIPTION
MIRV	MULTIPLE INDEPENDENTLY TARGETABLE REENTRY VEHICLE	A MISSILE PAYLOAD CONTAINING SEVERAL WARHEADS, EACH ABLE TO STRIKE A DIFFERENT TARGET.
ML	MACHINE LEARNING	A SUBSET OF AI THAT ALLOWS SYSTEMS TO LEARN FROM DATA PATTERNS WITHOUT BEING EXPLICITLY PROGRAMMED.
NAOC	NATIONAL AIRBORNE OPERATIONS CENTER	COMMAND POST ON AN E-4B AIRCRAFT FOR NATIONAL LEADERSHIP IN CRISIS.
NATO	NORTH ATLANTIC TREATY ORGANIZATION	ALLIANCE OF EUROPEAN AND NORTH AMERICAN NATIONS FOR COLLECTIVE DEFENSE.
NC3	NUCLEAR COMMAND, CONTROL, AND COMMUNICATIONS	SYSTEMS ENABLING PRESIDENTIAL CONTROL OVER NUCLEAR FORCES.
NEACP	NATIONAL EMERGENCY AIRBORNE COMMAND POST	EARLIER NAME FOR THE NAOC.
NG-OPIR	NEXT-GENERATION OVERHEAD PERSISTENT INFRARED	FOLLOW-ON MISSILE WARNING SATELLITE SYSTEM TO SBIRS.
NMCC	NATIONAL MILITARY COMMAND CENTER	PENTAGON-BASED HUB FOR COMMAND AND CONTROL OF MILITARY FORCES.
NPR	NUCLEAR POSTURE REVIEW	DOD POLICY DOCUMENT OUTLINING U.S. NUCLEAR STRATEGY.
NPT	NUCLEAR NON-PROLIFERATION TREATY	INTERNATIONAL TREATY AIMED AT PREVENTING NUCLEAR WEAPONS SPREAD.
NSDD	NATIONAL SECURITY DECISION DIRECTIVE	A TYPE OF PRESIDENTIAL DIRECTIVE USED TO IMPLEMENT NATIONAL SECURITY POLICY.
OPLAN	OPERATIONS PLAN	A DETAILED PLAN FOR MILITARY OPERATIONS.
OPIR	OVERHEAD PERSISTENT INFRARED	SPACE-BASED MISSILE WARNING AND SURVEILLANCE CAPABILITY.
PAL	PERMISSIVE ACTION LINK	A SECURITY MECHANISM PREVENTING UNAUTHORIZED ARMING OF NUCLEAR WEAPONS.
PARCS	PERIMETER ACQUISITION RADAR CHARACTERIZATION SYSTEM	GROUND-BASED RADAR PROVIDING ARCTIC MISSILE WARNING.
PAVE PAWS	PRECISION ACQUISITION VEHICLE ENTRY PHASED ARRAY WARNING SYSTEM	GROUND-BASED RADAR PROVIDING EARLY WARNING OF SLBMS.
PEOC	PRESIDENTIAL EMERGENCY OPERATIONS CENTER	SECURE FACILITY UNDER THE WHITE HOUSE FOR USE DURING CRISES.
PNI	PRESIDENTIAL NUCLEAR INITIATIVE	SERIES OF 1991–92 POLICY STATEMENTS REDUCING U.S. AND SOVIET TACTICAL NUCLEAR WEAPONS.
SBIRS	SPACE-BASED INFRARED SYSTEM	SATELLITE CONSTELLATION FOR GLOBAL MISSILE LAUNCH DETECTION.
SDA	SPACE DEVELOPMENT AGENCY	DOD AGENCY FOCUSED ON BUILDING PROLIFERATED SATELLITE CONSTELLATIONS.
SDI	STRATEGIC DEFENSE INITIATIVE	REAGAN-ERA MISSILE DEFENSE PROGRAM.

ACRONYM	FULL TERM	DESCRIPTION
SHARC	SYSTEM FOR HYBRID ANALYSIS OF RESILIENT COMMAND	AI-ENHANCED NC3 POST-STRIKE ASSESSMENT TOOL.
SIOP	SINGLE INTEGRATED OPERATIONAL PLAN	FORMER U.S. NUCLEAR WAR PLAN, REPLACED BY THE OPLAN STRUCTURE.
SLBM	SUBMARINE-LAUNCHED BALLISTIC MISSILE	BALLISTIC MISSILE LAUNCHED FROM A SUBMARINE.
SOE	STATE-OWNED ENTERPRISE	A BUSINESS ENTERPRISE WHERE THE STATE HAS SIGNIFICANT CONTROL.
TACAMO	TAKE CHARGE AND MOVE OUT	MISSION FOR ENSURING SURVIVABLE COMMUNICATION WITH SUBMARINES.
THAAD	TERMINAL HIGH ALTITUDE AREA DEFENSE	MISSILE DEFENSE SYSTEM CAPABLE OF INTERCEPTING SHORT AND MEDIUM-RANGE BALLISTIC MISSILES.
UEWR	UPGRADED EARLY WARNING RADAR	MODERNIZED BMEWS/PAVE PAWS RADAR SYSTEM.
UHF	ULTRA HIGH FREQUENCY	RADIO FREQUENCY BAND USED FOR LINE-OF-SIGHT COMMUNICATIONS.
USNDS	U.S. NUCLEAR DETONATION DETECTION SYSTEM	SATELLITE-BASED SYSTEM DETECTING AND CHARACTERIZING NUCLEAR EXPLOSIONS.
USSTRATCOM	UNITED STATES STRATEGIC COMMAND	UNIFIED COMMAND RESPONSIBLE FOR STRATEGIC DETERRENCE AND NUCLEAR OPERATIONS.
VLF	VERY LOW FREQUENCY	FREQUENCY BAND CAPABLE OF PENETRATING SEAWATER TO COMMUNICATE WITH SUBMARINES.

Recommended Reading

Acton, James M. "Escalation through Entanglement: How the Vulnerability of Command-and-Control Systems Raises the Risks of an Inadvertent Nuclear War." Washington: Carnegie Endowment for International Peace, 2018.

Blair, Bruce G. The Logic of Accidental Nuclear War. Washington: Brookings Institution Press, 1993.

Bracken, Paul. The Command and Control of Nuclear Forces. New Haven: Yale University Press, 1983.

Bracken, Paul. The Second Nuclear Age: Strategy, Danger, and the New Power Politics. New York: Times Books, 2012.

Christian, Brian. The Alignment Problem: Machine Learning and Human Values. New York: W. W. Norton, 2020.

Colby, Elbridge A. The Strategy of Denial: American Defense in an Age of Great Power Conflict. New Haven: Yale University Press, 2021.

Congressional Research Service. "Defense Primer: Nuclear Command, Control, and Communications (NC3)." Washington DC, updated 2025.

Feaver, Peter D. Guarding the Guardians: Civilian Control of Nuclear Weapons in the United States. Ithaca: Cornell University Press, 1992.

Freedman, Lawrence. The Evolution of Nuclear Strategy. 3rd ed. New York: Palgrave Macmillan, 2003.

Geist, Edward, and Andrew J. Lohn. "How Might Artificial Intelligence Affect the Risk of Nuclear War?" Santa Monica: RAND Corporation, 2018.

Hays, Peter L., and Sarah Mineiro. "Modernizing Space-Based Nuclear Command, Control, and Communications." Washington: Atlantic Council, 2024.

Johnson, James. AI and the Bomb: Nuclear Strategy and Risk in the Digital Age. Oxford: Oxford University Press, 2023.

Kaplan, Fred. Dark Territory: The Secret History of Cyber War. New York: Simon & Schuster, 2016.

Kroenig, Matthew. The Logic of American Nuclear Strategy: Why Strategic Superiority Matters. Oxford: Oxford University Press, 2018.

Mahnken, Thomas G., ed. Forging the Tools of 21st-Century Great Power Competition. Washington: Center for Strategic and Budgetary Assessments, 2020.

National Security Commission on Artificial Intelligence. Final Report. Arlington, VA: NSCAI, March 2021.

Office of the Secretary of Defense. "Space Policy Review and Strategy on Protection of Satellites." Washington: U.S. Department of Defense, 2023.

Perrow, Charles. Normal Accidents: Living with High-Risk Technologies. Princeton: Princeton University Press, 1984.

Roberts, Brad. The Case for U.S. Nuclear Weapons in the 21st Century. Stanford: Stanford University Press, 2015.

Russell, Stuart. Human Compatible: Artificial Intelligence and the Problem of Control. New York: Viking, 2019.

Sagan, Scott D., ed. Inside Nuclear Command and Control. Stanford: Stanford University Press, 1993.

Sagan, Scott D. The Limits of Safety: Organizations, Accidents, and Nuclear Weapons. Princeton: Princeton University Press, 1993.

Scharre, Paul. Army of None: Autonomous Weapons and the Future of War. New York: W. W. Norton & Company, 2018.

Schlosser, Eric. Command and Control: Nuclear Weapons, the Damascus Accident, and the Illusion of Safety. New York: Penguin, 2013.

Wirtz, James J., and Jeffrey A. Larsen, eds. Nuclear Command, Control, and Communications: Lessons for U.S. Policy. Washington: Georgetown University Press, 2024.

FAS FEDERATION OF AMERICAN SCIENTISTS

About the Federation of American Scientists

The Federation of American Scientists is dedicated to democratizing the policymaking process by working with new and expert voices across the science and technology community, helping to develop actionable policies that can improve the lives of all Americans. For more about the Federation of American Scientists, visit **FAS.org.**