ANALYSIS OF USSTRATCOM SI 526-01: NUCLEAR WEAPON SYSTEM OPERATIONAL TESTING AND COMMAND AND CONTROL REQUIREMENTS

DE = PA x PD

PA = PLS x WSR x PTP x (1-PCLIP)

PD = f (Y, HOB, CEP, VNTK, R95, Offset)

Legend:	
DE – Damage Expectancy	PCLIP – Probability of Clipping Terrain
PA – Probability of Arrival	Y – Yield
PD – Probability of Damage	HOB – Height of Burst
PLS – Prelaunch Survivability	CEP – Circular Error Probable
WSR – Weapon System Reliability	VNTK – Vulnerability Number/Target Type/K-factor system
PTP – Probability to Penetrate	R95 – area including 95% of the targeted facility

Figure 1. (U) Damage Expectancy Equation

Recommended Citation

Peter Hayes, "ANALYSIS OF USSTRATCOM SI 526-01: NUCLEAR WEAPON SYSTEM OPERATIONAL TESTING AND COMMAND AND CONTROL REQUIREMENTS", NAPSNet Special Reports, March 25, 2026, https://nautilus.org/napsnet/napsnet-special-reports/analysis-of-usstratcom-si-526-01-nuclear-weapon-system-operational-testing-and-comman--and-control-requirements/

PETER HAYES

MARCH 25 2026

I. INTRODUCTION

Peter Hayes argues that the methods revealed in USSTRATCOM SI 526-01 for estimating the reliability of US command and control procedures and of weapons systems in delivering nuclear weapons to targets may instill false confidence in US nuclear commanders that nuclear strikes will be achieved as planned and that NC3 will enable them control nuclear operations under conditions of nuclear attack. This document reveals new details about US nuclear weapons operational testing not previously known.

USSTRATCOM SI 526-01 may be downloaded here (PDF 10.8MB).

Peter Hayes is Director of the Nautilus Institute and Honorary Professor at the Centre for International Security Studies at the University of Sydney, and Senior Research Advisor of the Asia-Pacific Leadership Network

Acknowledgement: The research for this FOIA request and publication was funded by New Land Foundation and Ploughshares Fund.

Perplexity AI was used in the production of this text for review and fact-checking of various issues. However, author is wholly responsible for the text posted in this Special Report.

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

This report is published under a 4.0 International Creative Commons License the terms of which are found **here**.

Banner image: USSTRATCOM Instruction SI 526-01, Figure 1, p. B-2.

II. NAPSNET SPECIAL REPORT BY PETER HAYES

ANALYSIS OF USSTRATCOM SI 526-01: NUCLEAR WEAPON SYSTEM OPERATIONAL TESTING AND COMMAND AND CONTROL REQUIREMENTS

MARCH 25 2026

Abstract

USSTRATCOM June 2020 Strategic Instruction 526-01 *"MISSILE WARNING AND NUDET DETECTION OPERATIONS"* released under US Freedom of Information Act to Nautilus Institute "establishes operational testing protocols for nuclear weapon systems, prescribing how Services generate Weapon System Reliability (WSR) and Circular Error Probable (CEP) planning factors embedded in Damage Expectancy calculations.[1] The instruction treats Nuclear Command, Control, and Communications (NC3) as a testable system with quantified Command and Control Procedures (CCP) reliability. CCP is defined as "the probability that crews will receive a valid Emergency Action Message and perform all necessary actions to commit a nuclear weapon when directed"[2] Ensuring such positive control—that nuclear weapons always can be used—requires end-to-end testing from message transmission through weapon release and annual reporting of CCP methodologies, changes, and results.[3] However, CCP is not integrated into WSR calculations, creating an

analytical gap such that the overall probability of enacting positive control in nuclear weapons operations is unknown.[4] Publicly available evidence confirms systematic NC3 testing (such as annual Airborne Launch Control System or ALCS launches, twice-yearly SELM or Simulated Electronic Launch Minuteman tests, Giant Ball a test of the ground and air components ALCS connectivity),[5] but quantitative performance data remain classified. NC3 modernization toward AI-enabled, cyber-resilient architectures requires metrics beyond SI 526-01's framework—AI algorithm reliability, cyber-contested operations, software quality-of-service—for which updated assessment protocols remain opaque. Overall, SI 526-01 outlines methods for estimating the performance of CCP and weapon systems command and control procedures and weapons systems that may overstate the reliability of US NC3 in wartime conditions and thereby encourage the propensity of US nuclear commanders--especially the US president--to resort to using nuclear weapons.

Document Context and Scope

In January 2019, General John Hyten remarked that while he was confident that the US NC3 system works, he did not understand why or how it worked. He repeated this view in testimony to Congress in March:

> So one of the interesting things I've observed in my 27 months in command now -- so that -- that's a long period of time, two years and three months -- not one time in that two year, three months have I lost connectivity with the nuclear force. Can you imagine any other electronic system in the world where that has happened? That shows you how resilient, reliable and effective the current command and control system is.
>
> But what concerned me about it is I really can't effectively explain that to you. Because it's been built 50 years ago through different kind of pathways, different kind of structures, we look at it hard each and every day and we know that those things are going to have to be replaced in about a decade.[6]

Hyten was not the first STRATCOM commander to recognize this paradox. His predecessor (2007-2011) General Kevin Chilton expressed a similar view in May 2023 when he stated: “I do not have enough current information to assess the current robustness and resiliency of the existing NC3 network.”[7]

STRATCOM instruction SI 526-01, the subject of this special report, provides insight into why these commanders found it difficult to understand how and why NC3 systems perform.

Nautilus filed the original request for this and other STRATCOM documents related to NC3 in October 2018 to prepare for the conference on NC3 and Global Stability held at the Hoover Institution in 2019.[8] The response letter (20 November 2020) included in this release explains that USSTRATCOM withheld portions of SI 526-01 with some unclassified portions withheld because their aggregation would reveal classified relationships under the “mosaic” theory.[9]

The letter also corrects an error in the instruction itself and notes that paragraph 6.b. on page B-10 of SI 526-01 "should read as follows: 'The expected operational service life of the system as opposed to the design life should be considered to ensure weapon system asset availability for Initial Operational Test and Evaluation and Follow on Operational Test and Evaluation throughout the life of the system.'"[10]

The instruction applies to "USSTRATCOM and all units, organizations, and agencies involved in the validation and reporting of nuclear weapon systems capabilities in support of USSTRATCOM's nuclear weapons planning."[11] It supersedes the 2015 version, updates office symbols, refines

test-size definitions (year-to-year vs lifetime degradation), allows phased test constructs, imposes timelines on OIT&E, and emphasizes Service–DOE/NNSA collaboration.[12]

Core Testing and Planning Framework

SI 526-01's purpose is "to establish guidelines for nuclear weapon system operational testing and reporting, and [to] provide detailed background and guidance for the development of a testing program during the initial and follow-on phases of nuclear weapon systems," with test results used "to calculate estimates for Weapon System Reliability (WSR) and Circular Error Probable (CEP)."[13]

WSR is defined as

> ...the probability that a warhead on a given nuclear weapon system will detonate over or at its designated ground zero under given mission-related conditions, excluding the effects of enemy action," and CEP as "the radius of a vertical cylinder, centered on a reference point, within which 50 percent of the Reentry Vehicles (RV)/Reentry Bodies (RB)/missile payloads/gravity weapons are expected to be located at airburst or impact.[14]

These planning factors feed into Damage Expectancy (DE), the central measure of effects in OPLAN assessment. DE is defined as "the probability of achieving the desired level of damage against a targeted facility."[15] The instruction formulates Damage Expectancy algebraically as follows:

> It is the product of Probability of Arrival (PA) and Probability of Damage (PD)... PA is the product of PLS, WSR, Probability to Penetrate (PTP) and one minus Probability of Clipping Terrain (1 − PCLIP). PD is a function of weapon yield, HOB, CEP, the hardness of the target as measured by the [VNTK system], the area including 95% of the targeted facility (R95), and offset distance of the target from the aim point."[16]

The instruction includes the explicit equation with the component definitions presented as a figure copied below.[17]

DE = PA x PD

PA = PLS x WSR x PTP x (1-PCLIP)

PD = f (Y, HOB, CEP, VNTK, R95, Offset)

Legend:	
DE – Damage Expectancy	PCLIP – Probability of Clipping Terrain
PA – Probability of Arrival	Y – Yield
PD – Probability of Damage	HOB – Height of Burst
PLS – Prelaunch Survivability	CEP – Circular Error Probable
WSR – Weapon System Reliability	VNTK – Vulnerability Number/Target Type/K-factor system
PTP – Probability to Penetrate	R95 – area including 95% of the targeted facility

Figure 1. (U) Damage Expectancy Equation

USSTRATCOM uses Service-provided planning factors in its OPLANs. SI 526-01 "emphasizes the direct relation between the Service reported planning factors, confidence levels, and the quality of USSTRATCOM-generated nuclear options."[18] The Services must conduct IOT&E (Initial Operational Test and Evaluation) to provide operational planners with “reference WSR and CEP values which have a specified degree of precision. Moreover, the Services are instructed to conduct enough FOT&E (Follow-on Operational Test and Evaluation) "to detect, on an annual basis, a given amount of degradation from the previous year's established WSR and CEP planning factors within a specified level of confidence."[19]

Exact numerical thresholds and statistical properties are redacted, but the document stresses that "relevant statistical properties to achieve statistically significant objectives are specified in Enclosure B, para 4.c.[20] STRATCOM explains the fundamental difference between the two metrics in figuring out the requisite number of tests (“test sizing”) as follows:

> There are a number of statistical methods suitable for test sizing the above requirements. However, the Services must be aware of the fundamental differences between the IOT&E and FOT&E requirements. IOT&E is an expected value, confidence interval problem (i.e. not a statistical hypothesis test); whereas FOT&E is a statistical hypothesis test with two alternatives being: 1) the demonstrated WSR has not degraded be [sic] a certain threshold, and 2) the demonstrated WSR has degrade [sic] by a certain threshold.[21]

NC3 Performance Testing Framework

The instruction treats NC3 as an integrated system requiring end-to-end performance testing and quantified reliability assessment**.** Although the document uses the term "Command and Control Procedures (CCP)," the testing framework it establishes encompasses the full NC3 architecture—from strategic command centers through communication networks to tactical execution platforms. C2 appears in the instruction both as a defined planning factor and as an object of explicit measurement and reporting, with specific provisions for testing communication link performance, crew response timelines, and system-wide message delivery reliability.

Test Databases

The instruction reveals that STRATCOM maintains 3 reliability databases.

> The test database, as defined in these guidelines, includes all operational testing and related non-operational testing data obtained throughout the test program. The reliability database is part of the responsible organization's corporate memory of the test program. At a minimum, it will include enough detail to permit the reader of the evaluation report, using the provided methodology, to reproduce the calculated planning factors. Additionally, the database will provide reasons for test failures. Typically, the reliability database consists of a table of all reliability results, arranged in chronological test order, with comments explaining test failures and exclusions of data from planning factor calculations.[22]

Three databases are maintained for ballistic missiles, cruise missiles, and gravity weapons with the scope of each shown below.[23]

- Nickname or other designation for firing exercise
- Date and time of test
- Special test objectives, if any
- Test range name and launch location (if more than one is used in the test program)
- Target designation and location (if more than one is used)
- Designation of launching element (SSBN/crew designation (color), wing/launch facility)
- Test range operations number and serial number for each missile attempted to be fired
- Flight range, trajectory, footprint, deployment sequence, launch azimuth, time of flight, reentry angle, reentry velocity
- Payload type (JTA or other)
- Type of test RV/RB, fusing options, and planned HOB
- For Intercontinental Ballistic Missiles (ICBM), launch-area ground weather conditions
- For Submarine-Launched Ballistic Missiles (SLBM), sea conditions in the launch area
- Climatological and sea state conditions in the target area
- Flight performance results (including success/tests and, as appropriate, operating times) for launch, in-flight and payload performance, including:
- Launch support equipment
- Booster/missile motor
- Post-boost vehicle/equipment section
- Chaff
- RV/RB reentry
- Arming and fusing for each RV/RB
- Warhead
- Ancillary exercise and test results, including ground tests of RV/RB and warhead
- Failure cause(s)
- Reasons for scoring of data as no-test, non-realistic, non-representative, or reselection
- Data adjustments

Table 2. (U) Items for the Ballistic Missile Reliability Database

- Nickname or other designation for firing exercise
- Date and time of test
- Special test objectives, if any
- Test range name and location (if more than one is used in the test program)
- Target designation and location (if more than one is used)
- Designation of launching aircraft
- Serial number for each missile attempted to be fired
- Payload type (JTA or other)
- Flight range, time, last map to target distance, map set used in test
- Fusing option and planned HOB
- Launch area weather conditions
- In-flight climatological conditions
- Aircraft generation reliability performance results
- Flight performance results (including success/tests and, as appropriate, operating times) for launch, in-flight and payload performance, including:
- Airframe (nuclear payload certified)
- Launch support equipment
- Cruise initiation
- Cruise
- Arming and fusing
- Warhead
- Ancillary exercise and test results, including ground tests of warhead
- Failure cause(s)
- Reasons for scoring of data as no-test, non-realistic, non-representative or reselection
- Data adjustments

Table 3. (U) Items for the Cruise Missile Reliability Database

- Nickname or other designation for firing exercise
- Date and time of test
- Special test objectives, if any
- Test range name and location (if more than one has been used in the program)
- Target designations and locations (if more than one has been used)
- Designation of releasing aircraft/crew
- Serial number for each weapon attempted to be released
- Payload type (JTA or other)
- Fusing option and planned HOB
- Launch area winds
- Aircraft generation reliability performance results
- Flight performance results (including success/tests and, as appropriate, operating times) for release, in-flight, and payload performance, including:
- Releasing element
- Release support equipment
- In-flight
- Arming and fusing
- Warhead
- Ancillary exercise and test results, including ground tests of warhead
- Failure cause(s)
- Reasons for scoring of data as no-test, non-realistic, non-representative or reselection
- Data adjustments

Table 4. (U) Items for the Gravity Weapon Reliability Database

NC3 Reliability as a Core Planning Factor

Within Enclosure A (General), Command and Control Procedures are defined in parallel to WSR and PLS:

> Command and Control Procedures (CCP) reliability is the probability that crews will receive a valid Emergency Action Message (EAM) and perform all necessary actions to commit a nuclear weapon when directed.[24]

This definition encompasses the entire NC3 chain: strategic-level message origination and transmission from USSTRATCOM or the National Military Command Center, relay through military communication networks (satellite, airborne platforms, ground stations), reception at tactical platforms (ICBMs, submarines, bombers), message decoding and authentication by crews, PAL operations where required, and final execution actions to commit weapons. By framing NC3 as a probabilistic reliability measure comparable to weapon hardware reliability, the instruction treats the entire command and communications infrastructure as a testable system with quantifiable performance characteristics.

This definition is significant because it puts CCP reliability alongside PLS and WSR as a probabilistic quantity, establishing NC3 performance as a formal planning factor rather than an assumed background capability, even though CCP is not yet folded into WSR calculations.

This latter point is very important to note when reading this STRATCOM instruction.

The instruction defines PA, Probability of Arrival, in manner that assumes that attack orders already

exist and are properly issued, EAMs have been authenticated and executed properly.

However, it does not incorporate NC3/CCP or any concern about how EAMs are generated, authenticated, or possibly mis-executed. Yet CCP reliability is defined in the instruction as the probability that crews will fire their weapons after receiving valid EAMs.

PA or the Probability of Arrival then calculates the probability that the weapon will arrive on target. PA is agnostic as to the validity of CCP reliability and no formulation of the factors that determine the probability that crews will receive a valid EAM and act properly is offered. PA therefore offers a metric that assures nuclear commanders that they can always (or sufficiently nearly always) put a nuclear weapon on a target, that is, exert a positive NC3 control; but offers no insight into how command and control procedures and related probabilities that preserve negative and positive control within the NC2 system itself affect the overall probability of a controlled delivery of a nuclear weapon onto a target.

Thus, the PA calculated by STRATCOM does not address whether the EAM was properly issued and authenticated; it simply assumes a valid, correctly issued order and then tracks only the performance of hardware, defences, and delivery trajectory.[25]

CCP Testing in Operational Test Design

Enclosure B (Guidelines for Operational Testing) embeds C2 within the notion of "holistic" operational tests. The instruction notes that "a holistic construct will employ beginning-to-end testing. If feasible, all flight tests will be initiated with the transmission of an exercise EAM [Emergency Action Message]."[26] It specifies that the Office Of Primary Responsibility for this activity is "the USSTRATCOM, Global Operations Directorate, Nuclear Operations, Nuclear Operations Command and Control Division (J38)."[27]

A phased testing construct is also permitted, which "breaks up the mission into several phases, each of which must be fully tested and scored independently," but "if feasible, this should also include the Command and Control training as described in the holistic construct."[28] Examples of when phased constructs are necessary include tests with multiple re-entry vehicles from a single booster, multiple weapons from a single carrier, prematurely terminated tests, and phase-specific ground or lab tests such as Simulated Electronic Launch Minuteman SELM.[29]

Also important are Joint Assembly Tests. The instruction reveals that:

> Planning for flight tests will include Joint Test Assembly (JTA) requirements. Sufficient JTA missions, consistent with operational testing requirements, will be flown each year to allow the calculation of warhead reliability. NNSA requirements may necessitate that some of these JTAs be high fidelity. If deemed necessary by the NNSA, a high fidelity JTA or "instrumented high fidelity JTA" will be flown for each ballistic missile warhead type at least once every two years. Offices responsible for those ballistic missile weapon systems without a high fidelity JTA, for which the NNSA deems a high fidelity JTA is required, will report on the status of acquiring said JTA in the annual evaluation report of the weapon system.[30]

Taken together, these provisions are intended to ensure that C2 processes—particularly message transmission and crew response—are exercised under realistic conditions within the broader operational test regime, rather than treated as an entirely separate analytical exercise.

Dedicated CCP Metrics Requirement

The most explicit C2 testing requirement is outlined in Enclosure B, paragraph 8 ("Command and

Control Procedures (CCP)"), which focuses squarely on CCP reliability metrics:

> In order to quantify the reliability of CCP from message transmission to execution, Services will provide CCP metrics that estimate the probability crews will receive a valid EAM and the probability they perform all necessary actions within the system's required time limit to commit a nuclear weapon.[31]

The instruction then defines the CCP timeline and clarifies how CCP is treated analytically:

"The CCP timeline is from message transmission to weapon release. The timeline includes the following: message transmission, receipt, decoding, validating, authentication and verification procedures, and Permissive Action Link (PAL) operations. CCP reliability is currently required to identify deficiencies and/or trends; however, it is not used for WSR calculations"[32]—in turn meaning these CCP-determinative factors are not incorporated nor reflected in the PA or Probability of Arrival calculation.

Finally, it assigns methodological authority to the Services, subject to STRATCOM approval and transparency:

> The methodology used for calculating CCP is determined by the Services. However, a CCP planning factor should contain elements which closely resemble the current operational force. Services should address which methodology (e.g., weighted, moving average, cumulative) is used to calculate CCP at the Nuclear Planning Factors Workshop and in their annual evaluation report. The Services' chosen methodology for calculating CCP will be submitted to USSTRATCOM/J593 for approval.[33]

Thus, CCP is handled as a distinct (non-WSR) planning factor, derived from empirical metrics over the EAM-to-release timeline and governed by Service-specific statistical methods that must be explained and approved.

CCP Reporting in Evaluation Reports

Enclosure D (Reporting Criteria) requires that the CCP section of the weapon system evaluation report explicitly cover CCP changes, impact, methodology, and test results:

> CCP section of the report will identify (1) Any CCP changes which have occurred, (2) The impact of CCP changes on ability of the weapon system to successfully complete its mission, (3) CCP calculation methodology, and (4) CCP test results.[34]

This requirement establishes a reporting loop in which C2 system changes and their operational implications must be tied back to observed CCP performance and to documented analytical methods.

NC3 Communications Link Performance Metrics

Beyond crew-level CCP metrics, the instruction mandates quantitative testing and grading of specific NC3 communication links, establishing concrete performance standards for the communications architecture that enables nuclear command and control. Enclosure D mandates reporting of connectivity metrics for airborne command and control systems. For the Airborne Launch Control System (ALCS), which provides redundant airborne command capability for ICBM forces, the report must include ALCS test methodology and results, and uses a traffic-light table (Table 7) to grade Wing Launch Facility UHF connectivity over the previous 12 months during last 12 months through ALCS Giant Ball connectivity results.[35]

This grading system establishes quantified performance thresholds for NC3 link reliability: 99% connectivity is considered fully satisfactory (green), while performance below 96% is considered unacceptable (red), requiring immediate attention. For example, the requirement to test using "Giant Ball" exercises—operational exercises that test the entire ALCS-to-launch-facility communications chain under realistic conditions—ensures that NC3 testing captures real-world performance rather than laboratory measurements.

Connectivity Rate	Color Code
> 99%	Blue
98% to 99%	Green
97% to 98%	Yellow
96% to 97%	Orange
<96%	Red

Table 7. ALCS Connectivity Rate (12mo)

A separate table (Table 8) addresses "2-way UHF Voice Connectivity Rate 12 mo," covering voice communications between airborne command posts and launch facilities for a year.

Connectivity Rate	Color Code
> 97.5%	Blue
95% to 97.5%	Green
92.5% to 95%	Yellow
90% to 92.5%	Orange
<90%	Red

Table 8. 2-way UHF Voice Connectivity Rate (12mo)

Together, these metrics establish that both data and voice channels of the NC3 architecture are subject to quantitative measurement, annual reporting, and performance standards, reinforcing that connectivity and message-delivery performance are monitored quantitatively as part of the broader test and reporting system.

Operational Testing, Realism, and C2

The instruction frames CCP reliability as part of the broader goal that operational tests be realistic, representative, and sufficient. Test realism is defined to include C2 processes: operational tests should replicate the "Command and Control timeline from execution order to weapon release, including the execution order formats, decoding, authentication, and verification procedures and Permissive Action Link operations."[36] The evaluation report is required to describe such C2-related deviations from operational practice in individual tests and to fold significant findings into the assessment of realism.

Similarly, the distribution and selection of test weapons and crews are supposed to ensure that "over the long term, the test weapons comprise a true random sample of the deployed force," with the report describing selection methods, exclusion reasons, and associated performance tests.[37] Because CCP metrics are meant to "contain elements which closely resemble the current operational

force," this Service-based sampling (using variously weighted, moving average, or cumulative metrics) indirectly constrains how meaningful CCP data can be collected and interpreted.[38]

SI 526-01 is opaque on how USSTRATCOM ensures that CCP data are collected and analyzed across the services whose different CCP methodologies may render the collected results inconsistent.

Service Waivers, and Non-Operational C2 Data

As noted earlier, the Services determine which CCP methodologies to use but must present them at the Nuclear Planning Factors Workshop and submit them to USSTRATCOM/J593 for approval, mirroring the process for WSR and CEP.[39] When test-size requirements cannot be met, the Services must submit a waiver to J593 "in the form of a memorandum or white paper," including "the risk incurred by not meeting the requirement, an estimate of detectable degrade… and mitigating actions planned to reduce the risk incurred by not meeting the requirement," and must update waivers when mitigation conditions change.[40] Although the waiver language is written in terms of OIT&E/FOT&E test sizing, the same waiver and mitigation logic presumably would apply if C2 test coverage or CCP measurement regimes fell short.

The instruction also recognizes that "OTs [Operational Tests] alone may not provide sufficient information to assess all measures of performance for a nuclear system," and notes that "other flight, field, or laboratory tests may provide needed supplementary information, "including "realistic training exercises."[41] If non-operational data supplement planning factors, the evaluation report "must give the source and nature of the information," and such data "must be made available to USSTRATCOM."[42] For CCP, the carveouts and substitutes offered to Services suggests that exercises and training-based C2 metrics can be included, but only with explicit documentation of sources and methods. Again, how possibly inconsistent methodologies are synthesized into CCP reliability metrics is opaque in SI 526-01.

Key NC3 Performance Testing Issues Raised by STRATCOM Instruction SI 526-01

SI 526-01 raises at least seven concerning issues about how STRATCOM collects and synthesizes NC3 reliability data.

1. Partial Treatment of Positive Control: STRATCOM treats NC3 reliability as an explicit but non-integrated factor in damage expectancy calculations. The instruction clearly defines Command and Control Procedures or CCP reliability as "the probability that crews will receive a valid EAM and perform all necessary actions to commit a nuclear weapon," and mandates CCP metrics and planning factors; but also states that "CCP reliability is currently required to identify deficiencies and/or trends; however, it is not used for WSR calculations." This omission means that while NC3 system performance is tested and quantified in important dimensions, it is not formally incorporated into the Probability of Arrival (PA) term of the Damage Expectancy equation, which currently includes only PLS × WSR × PTP × (1 − PCLIP).

The exclusion of CCP from PA calculations represents a significant analytical gap: if an ICBM has 0.90 WSR but the crew has only 0.85 probability of receiving and acting on a valid EAM, the effective probability of weapon commitment is 0.765, not 0.90. This separation of organizational from hardware performance metrics creates a possibly false dichotomy in the way that USSTRATCOM conceptualizes and measures NC3 performance. As defined by STRATCOM, CCP reliability is determined by organizational and cultural factors interacting with technical, especially digital support systems, that affect the probability that a valid, authenticated EAM is received by a weaponeer who then acts on it to fire their nuclear weapon, which is then somehow correlated with weapon system performance that is tested physically and stringently measured, and estimated

statistically. Yet CCP is also measured only with respect to the technical performance of supporting communication networks, not with regard to crucial NC2 functions that are as much organizational as they are technical in nature.

This separation raises questions about whether Damage Expectancy and Operational Plan risk-assessments fully capture potential command system failure modes and whether nuclear war plan assessments systematically underestimate the impact of communications vulnerabilities and organizational dynamics on NC3 reliability in the performance of the overall nuclear kill chain.

2. Holistic vs. Phased C2 testing: The requirement that holistic tests, "if feasible," start with an exercise EAM and run through weapon release embeds C2 in end-to-end testing, while phased constructs can isolate segments (including C2 training) when holistic testing is impractical. However, the document also lists scenarios where holistic constructs are infeasible (such as multiple RV releases, weather-terminated tests), implying that many C2-relevant data points may come from fragmentary or constrained test environments rendering the realism of results dubious and possibly even subjective and lending false confidence in the aggregated results.

3. Service-determined CCP methodologies and comparability: The Services may choose their own methods (weighted, moving average, cumulative) for CCP estimation, provided they "closely resemble the current operational force," are presented at the Workshop, and approved by J593. This flexibility allows adaptation to Service-specific C2 architectures but complicates cross-system comparability and may obscure methodological changes over time, even though evaluation reports must identify CCP changes and their mission impact. It also renders questionable overall NC3 aggregated metrics of performance given more than 200 disparate systems constitute the “complex architecture” of the US NC3 system.[43] In fact, the US NC3 system “is a patchwork of disparate systems, each with its own characteristics. There is no one operating system or coding language”[44] In large part, this fragmentation and proliferation of disparate NC3 systems may explain why USSTRATCOM commanders find it hard to comprehend how such a sprawling system works.

4. NC3 communications link metrics are monitored but not integrated into system-level CCP or DE calculations. The ALCS connectivity table and 2-way UHF voice connectivity metrics show that link-level NC3 performance is measured and graded using operational exercises like Giant Ball, establishing concrete performance thresholds (99% satisfactory, <96% unacceptable).

However, the document does not explicitly connect these connectivity grades to changes in CCP reliability inputs or explain how communication link degradation translates into changes in crew-level CCP planning factors or ultimately into DE calculations. For example, if ALCS UHF connectivity to a wing's launch facilities drops from 99% to 96.5% (yellow/orange threshold), does this reduce the CCP reliability factor for those facilities, and if so, by how much?

The apparent gap between measured link-level NC3 performance (connectivity rates) and system-level reliability assessments (CCP planning factors) suggests that STRATCOM does not have an integrated, consistent framework and transparent method for taking measured weaknesses on individual NC3 links and using these insights to adjust the end-to-end CCP reliability numbers. The CCP section and ALCS annexes run in parallel to the more mature WSR/CEP/HOB frameworks, suggesting an ongoing effort to integrate NC3 quantitatively into planning at the same level of rigor applied to weapon hardware.

If this is the case, then it may reflect the reality that the US NC3 system is comprised of parallel, loosely coupled communications channels that provide functional redundancy without technical interoperability—but it does not lend confidence in the realism of NC3 metrics.

5. Classification constraints limit external assessment of NC3 testing rigor and planning factor conservatism. The instruction demands of STRATCOM agencies detailed reporting of command and control timelines, PAL use, test constraints, and logistic support, and establishes quantified connectivity performance standards for NC3 communication links. Unfortunately, many numerical thresholds and statistical parameters for both WSR and CEP, and some CCP-adjacent items, are redacted including specific test size requirements for CCP (how many end-to-end NC3 tests per year?), statistical confidence levels for CCP planning factors, degradation thresholds that trigger concern, and the actual CCP reliability values for deployed systems.

This opacity prevents external analysts from assessing whether NC3 testing regimes are statistically adequate, from fully reconstructing the statistical weight of command system failures or connectivity degradations in USSTRATCOM's internal planning, and from evaluating how aggressive or conservative CCP planning factors actually are compared to weapon hardware factors. Given ongoing debates about NC3 modernization costs and nuclear command system vulnerabilities to cyber-attack, electromagnetic pulse, or anti-satellite weapons, the inability to assess the empirical basis and statistical confidence of NC3 reliability planning factors represents a significant transparency gap. Whether the currently limp Congressional committees and the NC3 Oversight Council set up in 2015 provide stringent oversight on this score is an open question.

6. Lifecycle challenges for NC3 testing as systems and architectures evolve quickly. The cover letter provided a correction to SI 526-01 to the effect that "operational service life…as opposed to design life" emphasizes the need to maintain sufficient assets "throughout the life of the system" for OIT&E and FOT&E.

This lifecycle testing requirement poses unique challenges for NC3 systems because communications architectures evolve faster than weapon platforms. Satellite replacement, new encryption systems, updated airborne platforms, and cyber warfare capabilities all evolve much faster than major delivery platforms. Given that CCP measures depend on having representative crews, platforms, and communications configurations in the tests, the NC3 testing framework must continuously track whether CCP planning factors derived from tests using older communication systems, satellite generations, or network architectures remain valid for the current deployed force.

For example, if CCP metrics were established using tests with legacy UHF satellite communications, do they remain valid after transition to Advanced EHF satellites with different propagation characteristics and potential vulnerability profiles? The instruction requires reporting of "any CCP changes which have occurred" and "the impact of CCP changes on ability of the weapon system to successfully complete its mission." But the redacted content does not clarify how frequently full NC3 system retesting is required after major communications architecture changes, creating potential risk that CCP planning factors lag behind actual NC3 system performance as modernization proceeds.

7. NC3 modernization toward digital, AI-enabled, and cyber-resilient systems will require expanded performance metrics beyond SI 526-01's current framework. US NC3 modernization programs are transitioning from legacy analog systems toward "a modern cyber-defendable up-to-current-standards command and control system" incorporating software-defined networks, AI-assisted decision support, space-based hybrid architectures, and enhanced cyber defenses.[45] STRATCOM leadership has explicitly advocated incorporating AI and machine learning into NC3 for "decision advantage" and "system and network sensing, monitoring, and response capabilities," while emphasizing that "humans will always stay in control."[46] However, SI 526-01's performance metrics—designed for relatively static, human-centric NC3 architectures—do not address the reliability, safety, and failure modes typical of AI algorithms, software-defined networks, or cyber-contested environments. As explained above, the instruction's CCP reliability metric treats

NC3 as a single probability over a defined timeline, but modern NC3 introduces dynamic behaviors (automated failover or switching to backup systems, AI-based anomaly detection, adaptive routing) that change risk profiles across operational conditions and cyber threat states in seconds and minutes.[47] Similarly, the ALCS/UHF connectivity metrics measure link availability but not quality-of-service parameters (latency, jitter, packet loss) or data integrity under cyber-attack—issues central to modern IP-based NC3 networks.[48]

Comprehensive NC3 modernization would require extending SI 526-01's metric framework to include: cyber-resilient CCP conditioned on a range of attack states (no attack, intrusion detected/blocked, degraded operations); AI performance metrics (detection accuracy, false positive/negative rates, robustness under adversarial inputs, human-AI interaction timing); integrity and authenticity verification rates for cryptographic message validation; multi-path resilience and failover performance across space, airborne, and terrestrial NC3 links; and enterprise-level system-of-systems reliability that accounts for common-mode failures across triad components sharing NC3 infrastructure.[49]

It is possible that STRATCOM has revised SI 526-01 to reflect these challenges since the instruction was issued in June 2020, now six years ago.

Conclusion: Carter's Recognition of NC3 Performance Measurement Challenges Remains Valid

The need for expanded NC3 performance metrics has been recognized since the 1980s, when strategic analysts first systematically examined the impossibility of quantifying NC3 reliability with the same statistical confidence applied to weapon hardware. In his 1987 analysis "Assessing Command System Vulnerability," Ashton Carter established fundamental principles that remain relevant to contemporary NC3 modernization debates, particularly his argument that NC3 assessment can't be quantified unlike nuclear forces because whereas weapon system reliability can be calculated through statistical testing, calculating connectivity by estimating survival of nodes, modeling radio propagation through disturbed ionosphere, anti-jam margins, and EMP induced currents, etc. involves so many assumptions and uncertainties that it is impossible to arrive at single probability of connectivity without huge variances, leaving such estimates devoid of useful meaning.[50]

Carter identified the critical conceptual problem. Connectivity, he argued, is a function of time. Under conditions of nuclear attack, atmospheric disruption will block radio transmissions, aircraft will fly in and out of line-of-sight, ground control and their satellites will be attacked, backup batteries will, fail, generators will run out of fuel. Ground control for satellites will be destroyed. Undoubtedly parts of the NC3 communication networks may reconnect but there is no way to estimate the probability of such fluctuating connectivity.[51]

This temporal dynamic of real world NC3 performance—wherein reliability will change discontinuously as nuclear attacks unfold, systems degrade, backups activate then fail, and maybe—just maybe—NC3 reconstitution proceeds when the weapons stop detonating—fundamentally distinguishes NC3 testing from weapon hardware testing. Although SI 526-01 can mandate that Services report a single CCP reliability percentage for planning purposes, Carter's analysis reveals that such figures obscure the enormous underlying uncertainty about how NC3 would actually perform across the attack timeline. Carter concluded that while technical and procedural remedies can be suggested for individual vulnerabilities, it is futile to attempt a final assessment of the fragility of the NC3 system. "[I]n the end," he wrote, "the overall picture remains fuzzy, and no future remedy to the system's vulnerabilities looks absolute."[52]

His assessment directly contradicts the precision implied by SI 526-01's traffic-light grading system for ALCS connectivity (99% green, 98-99% uncertain, 97-98% yellow, 96-97% orange, <96% red), suggesting that such quantified thresholds may provide false confidence in NC3 reliability assessments. The technologies have changed; but the underlying logic and reality has not and Carter's conclusion remains as valid today as it was in 1989.

Carter also identified that nominal peacetime NC3 configurations diverge radically from wartime behavior, making peacetime testing a poor predictor of actual performance. In nuclear wartime, procedures and NC3 systems will change abruptly and whilst its operators would try to adapt and improvise, the NC3 systems are designed to discourage such innovation in the face of nuclear attack.

This tension between the need for adaptive flexibility under attack so that the NC3 system "fails gracefully" and the requirement for strict procedural control to prevent unauthorized actions creates an unresolvable measurement dilemma: the NC3 system that would actually operate in war cannot be tested in peace, because testing realistic improvisation would undermine the authentication and control procedures the system exists to enforce.

It is therefore difficult to avoid the conclusion that the reliability metrics generated by the testing procedures described in SI 526-01 may create an illusion of control that enhances a US presidential bias towards taking action—any action—when confronted by the vast, irresoluble paradoxes posed by nuclear war decision-making.

III. ENDNOTES

[1] USSTRATCOM, "GUIDELINES FOR NUCLEAR WEAPON SYSTEM OPERATIONAL TESTING AND REPORTING," USSTRATCOM Instruction SI 526-01, June 20, 2020, released by letter from USSTRATCOM FOIA 21-003 Response, SI 526-01, 20 November 2020, hereafter referred to as SI 526-01. The full document may be downloaded here. The instruction is not paginated so we have cited section and paragraph numbers. The Enclosures are paginated and are cited below.

[2] SI 526-01, Enclosure A, para. 2.e.4: "Command and Control Procedures (CCP) reliability is the probability that crews will receive a valid Emergency Action Message (EAM) and perform all necessary actions to commit a nuclear weapon when directed."

[3] SI 526-01, Enclosure B states:

para. 3.a.1: "A holistic construct will employ beginning-to-end testing. If feasible, all flight tests will be initiated with the transmission of an exercise EAM. The OPR… is the USSTRATCOM, Global Operations Directorate, Nuclear Operations, Nuclear Operations Command and Control Division (J38)."

para. 8: "The CCP timeline is from message transmission to weapon release. The timeline includes the following: message transmission, receipt, decoding, validating, authentication and verification procedures, and Permissive Action Link (PAL) operations. CCP reliability is currently required to identify deficiencies and/or trends; however, it is not used for WSR calculations."

para. 8: "In order to quantify the reliability of CCP from message transmission to execution, Services will provide CCP metrics that estimate the probability crews will receive a valid EAM and the probability they perform all necessary actions within the system's required time limit to commit a nuclear weapon."

para. 8: "The methodology used for calculating CCP is determined by the Services. However, a CCP planning factor should contain elements which closely resemble the current operational force. Services should address which methodology (e.g., weighted, moving average, cumulative) is used to calculate CCP at the Nuclear Planning Factors Workshop and in their annual evaluation report. The Services' chosen methodology for calculating CCP will be submitted to USSTRATCOM/J593 for approval."

[4] SI 526-01, Enclosure B, para. 8: "The CCP timeline is from message transmission to weapon release. The timeline includes the following: message transmission, receipt, decoding, validating, authentication and verification procedures, and Permissive Action Link (PAL) operations. CCP reliability is currently required to identify deficiencies and/or trends; however, it is not used for WSR calculations."

[5] Defence Industry Europe. (2025, December 7). "U.S. Air Force details test launch of Minuteman III missile controlled in flight by ALCS team on E-6B Mercury." https://defence-industry.eu/u-s--ir-force-details-test-launch-of-minuteman-iii-missile-controlled-in-flight-by--lcs-team-on-e-6b-mercury/ This article describes GT-254 as assessing "the reliability, readiness, and accuracy of the ICBM system" with ALCS providing "a survivable and secondary capability to transmit launch commands to our ICBMs." It notes that ALCS tests occur annually through GT missions and that "the Air Force also conducts Simulated Electronic Launch Minuteman (SELM) tests twice a year," which "run through all the procedures of a launch, including turning the keys, but stop just short of actually firing the missile."

Malmstrom Air Force Base. (2025, September 22). "Malmstrom showcases Minuteman III ICBM capabilities through simulated test launch." https://www.malmstrom.af.mil/News/Article-Display/Article/4312586/

The release describes SELM tests as performed "to verify the reliability of the Minuteman III intercontinental ballistic missile system, without physically firing a missile" and states they test "critical processes in a deployed environment."

U.S. Strategic Command. (2022, February 28). "Posture Statement Before the House Armed Services Committee Strategic Forces Subcommittee." https://www.stratcom.mil/Portals/8/Documents/2022 USSTRATCOM Posture Statement - HASC-SF Hrg FINAL.pdf

[6] In US Strategic Command, "U.S. Strategic Command and U.S. Northern Command SASC Testimony," March 1, 2019, at:

https://www.stratcom.mil/Media/Speeches/Article/1771903/us-strategic-command-and-us-northern-command-sasc-testimony/

[7] *Conversations on National Security: An Interview with General Kevin Chilton (USAF, Ret.), No. 554, May 15, 2023, at:* https://nipp.org/information_series/conversations-on-national-securit--an-interview-with-general-kevin-chilton-usaf-ret-no-554-may-15-2023/

[8] See P. Hayes et al, *Synthesis Report NC3 Systems and Strategic Stability: A Global Overview*, May 5, 2019 at: https://nautilus.org/wp-content/uploads/2019/05/NC3-Synthesis-Report--ay5-2019.pdf and the 40 papers and podcasts from this workshop. Hyten made his remarks at this event.

[9] K. Kooper, USSTRATCOM Command FOIA office, letter to Nautilus Institute, November 20,

2020, page 1.

[10] Ibid.

[11] SI 526-01, 3. Applicability.

[12] "This revision updates office symbols throughout… It adds more defining terms to test size requirements establishing a year-to-year degradation versus system lifetime degradation. It also recognizes the possibility of the Services' desire to conduct a phased testing strategy… It adds a timeline to OIT&E tests… [and] emphasizes the requirement for the Services, with Department of Energy (DOE) National Nuclear Security Administration (NNSA) collaboration." SI 526-01, 4, "Summary of Changes."

[13] SI 526-01, "Purpose," para. 1.

[14] SI 526-01, Enclosure A, para. 2.e.1-2

[15] SI 526-01, Enclosure B, General Requirements, para 3a.

[16] SI 526-01, Enclosure B, para. 3.a, Figure 1. VNTK is the Vulnerability Number/Target Type/K-factor system. It is not defined in the instruction.

Owen explains VNTK as follows:

> VNTK CONCEPT
>
> CONCEPT REPRESENTS TARGET'S SUSCEPTIBILITY TO NUCLEAR WEAPON EFFECTS
>
> VN NUMBER = ARBITRARY NUMBER DENOTING RELATIVE HARDNESS OF TARCET IN TERMS OF DAMAGE PROBABILITIES
>
> T FACTOR = LETTER DENOTINC TARGET SENSITIVITY TO TYPE OF PRESSURE WITH RELATIVE UNCERTAINTY LEVELS
>
> K FACTOR = NUMBER BETWEEN 0 & 9, FOR ADJUSTMENT TO VN INDICATING SENSITIVITY TO VARYINC PRESSURE DURATIONS AT DIFFERENT YIELDS. HIGHER NUMBER INCREASES PD PSI RATING = F (VN,T,K,YIELD)
>
> VNTK is simply a means of alphanumerically representing a target's susceptibility to nuclear effects. VNTK consists of 3 parts, as defined here. The Vulnerability Number (VN) is determined from information about target construction techniques and materials. The T-factor denotes the primary damage mechanism (i.e., dynamic pressure, overpressure, or cratering) needed to achieve the desired damage. It also includes the relative uncertainty level in a target's response to this damage mechanism as one moves further away from the target. Finally, the K-factor denotes a target's sensitivity to the pressure duration of a nuclear detonation, with 0 indicating total insensitivity and 9 indicating extreme sensitivity. This factor is an adjustment to the VN. Since VN is based on a 20 kiloton yield, if K > 0 then the VN is adjusted downward for yields greater than 20 kt. This is because larger yields produce longer pressure durations and, if a target is sensitive to this duration, then a lower amount of pressure (equating to a lower VN) applied for a longer time will induce the same level of damage as a higher pressure (higher VN) applied for a shorter time. If K = 0, then the target is only affected by the amount of pressure applied, not how long. In this case, yield has no effect on the pressure rating of the target. By taking VN, T, and K into account and, for K > 0,

including the yield, an equivalent pressure rating in psi for the target is obtained.

D.W. Owen, *STRATEGIC WEAPONS ASSESSMENT NOMOGRAPH*, Air Force Center for Studies & Analyses, February 1987, p.6 at: https://apps.dtic.mil/sti/tr/pdf/ADA362607.pdf

Also, PCLIP or Probability of Clipping Terrain is not defined in SI 526-01. If PCLIP is (by author's inference) the probability that the weapon's flight path is "clipped" by physical terrain and thus prevented from reaching the required height of burst or impact point, then 1- PCLIP would be the probability that terrain does *not* obstruct the trajectory, allowing arrival at the target, thereby affecting the Probability of Arrival as one of the correction factors in this formula that affect the Damage Expectancy calculation. PCLIP might be particularly important in terrain-following cruise missile operations.

[17] SI 526-01, Enclosure B, para. 3.a, Figure 1, p. B-2

[18] SI 526-01, Enclosure A, para. 1, p. A-1

[19] SI 526-01, Enclosure A, para. 2.b, p. A-1

[20] SI 526-01, Enclosure A, para. 2.c, p. A-1

[21] SI 526-01, Enclosure B, para. 4.d, p. B-5

[22] SI 526-01, Enclosure D, para j.1, p. D-9.

[23] SI 526-01, Enclosure D, pp. D-10 to 12.

[24] SI 526-01, Enclosure A, para. e.4, p. A-2.

[25] Positive technical and organizational control measures ensure that authorized EAMs are successfully and always executed when issued. Negative technical and organizational control measures prevent unauthorized or procedurally improper execution, ensuring that nuclear weapons are never used mistakenly.

[26] SI 526-01, Enclosure B, para. 3.a.1, p. B-3.

[27] Ibid

[28] SI 526-01, Enclosure B, para. 3.a.2, p. B-3.

[29] Ibid

[30] SI 526-01, Enclosure B, para 3.e, p. B-3. JTA tests are joint, that is, involve US Department of Energy NNSA and the relevant military service testing a nuclear weapon or delivery platform with mock nuclear weapons aboard. J. Gibson, "Up, up, and away, Flight tests offer real-life weapons performance insight," Los Alamos, June 5 2026, at: https://www.lanl.gov/media/publications/national-security-science/up-up-and-away

[31] SI 526-01, Enclosure B, para. 8, p. B-11.

[32] Ibid.

[33] Ibid

[34] SI 526-01, Enclosure D, para 9.f.1, p. D-16

[35] “Giant Ball” is an ALCS communications/exercise series rather than a single fixed site test, so the “facilities” involved are the airborne and ground nodes that make up the Minuteman NC3 path. The airborne nodes include U.S. Navy E-6B Mercury aircraft, configured as the USSTRATCOM Airborne Command Post and hosting the Airborne Launch Control System (ALCS) crew from 625th Strategic Operations Squadron and STRATCOM; E-6B radios used for HF/VLF/UHF links to ground launch control centres and other NC3 nodes. The ICBM ground network includes: the dispersed Launch Control Centers (LCCs) and associated Missile Alert Facilities in the Minuteman wings (Malmstrom, Minot, F.E. Warren AFBs) that normally command the silos; plus their fixed and mobile communications antennas (HF “top hat” masts, radio towers, associated ground radios) that receive ALCS test traffic. The Test and analysis support organizations including 625th Strategic Operations Squadron test and analysis branch, which “runs all ICBM and ALCS related tests” and specifically “runs ‘giant ball’ tests, radio tests to ensure the aircraft has good communication with every launch control centre on the ground; missile-wing ground facilities used for Simulated Electronic Launch Minuteman (SELM) tests and related exercises, which are often tied into the same communications test architecture even if “Giant Ball” itself is focused on radio connectivity. In short: a Giant Ball event exercises the NC3 system across the entire network constituted by the E-6B/ALCS airborne command post plus the full set of Minuteman launch control centres and their communications infrastructure**,** coordinated by the 625 STOS test and analysis branch. The instruction also refers to “Glory Trip” tests. These are routine operational tests of Minuteman ICBMs and often involve airborne launch crews backing up ground launch systems.

[36] SI 526-01, Enclosure B, para. 5.b.3, p. B-7

[37] SI 526-01, Enclosure D, para 2.c., p. D-2

[38] SI 526-01, Enclosure B, para. 8.b, p. B-11

[39] Ibid

[40] SI 526-01, Enclosure D, para 1.g, p. D-2

[41] SI 526-01, Enclosure D, para 3.g, p. D-6

[42] Ibid

[43] **“**Statement of The Honorable Ellen M. Lord Under Secretary of Defense for Acquisition and Sustainment Before the Strategic Forces Subcommittee, Committee on Armed Services,” US Senate, U.S. Nuclear Weapons Policy, Programs, and Strategy in Review of the Defense Authorization Request for Fiscal Year 2020 and the Future Years Defense Program, May 1, 2019, at: https://www.armed-services.senate.gov/imo/media/doc/Lord_05-01-19.pdf

[44] From answer to Question 1 at: Nuclear Command, Control, and Communications System Operational Assessment Program Solicitation Number: HC104710R4009, Agency: Defense Information Systems Agency, Office: Procurement Directorate
Location: DITCO-NCR, August 4, 2010, at:
https://www.fbo.gov/index?s=opportunity&mode=form&id=ca9ed977f427844fb095c1e170a579ee&tab=core&_cview=1

[45] See Atlantic Council. (2024, July 14). "Modernizing space-based nuclear command, control, and communications." https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/modernizing-space-based-nuclear-command-control-and-communications/

AFCEA Signal. (2021, January 6). "Nuclear C3 Looms Vital to Strategic Modernization." https://www.afcea.org/signal-media/nuclear-c3-looms-vital-strategic-modernization

CSIS. (2020, September 6). "NC3: Challenges Facing the Future System." https://www.csis.org/analysis/nc3-challenges-facing-future-system

[46] Breaking Defense. (2024, October 28). "AI has role to play in protecting American nuclear C2 systems: STRATCOM head." https://breakingdefense.com/2024/10/america-needs-ai-in-its-nuclear-c2-systems-to-stay-ahead-of-adversaries-stratcom-head/

Air & Space Forces Magazine. (2024, October 28). "STRATCOM Boss: AI 'Will Enhance' Nuclear C2." https://www.airandspaceforces.com/stratcom-boss-ai-nuclear-command-control/

[47] Federation of American Scientists. (2026, January 7). "AI and the Modernization of Nuclear Command, Control, and Communications." https://fas.org/publication/on-the-precipice/

[48] Breaking Defense. (2024, July). "NC3 space systems face critical modernization challenges, new study finds." https://breakingdefense.com/2024/07/nc3-space-systems-face-critical-modernization-challenges-new-study-finds/

[49] Global Issues. (2026, March 5). "The Impact of Artificial Intelligence in Nuclear Decision-Making." https://www.globalissues.org/news/2026/03/06/42489

Effective Altruism Forum. (2022, November 17). "Artificial Intelligence and Nuclear Command, Control and Communications." https://forum.effectivealtruism.org/posts/BGFk3fZF36i7kpwWM/artificial-intelligence-and-nuclear-command-control-and-1

University of Chicago X-Risk. (2025, July). "The Technicalities of Integrating AI Into The NC3." https://xrisk.uchicago.edu/files/2025/07/What_might_the_integration_of_AI_and_the_NC3_look_like_.pdf

[50] A. Carter, "Assessing Command System Vulnerability." In A. B. Carter, J. D. Steinbruner, & C. A. Zraket (Eds.), *Managing Nuclear Operations*, The Brookings Institution, 1987, p. 550.

[51] Ibid, p. 560.

[52] Ibid.

IV. NAUTILUS INVITES YOUR RESPONSE

The Nautilus Asia Peace and Security Network invites your responses to this report. Please send responses to: nautilus@nautilus.org. Responses will be considered for redistribution to the network only if they include the author's name, affiliation, and explicit consent.

View this online at: https://nautilus.org/napsnet/napsnet-special-reports/analysis-of-usstratcm-si-526-01-nuclear-weapon-system-operational-testing-and-command-and-control-requirements/

Nautilus Institute
608 San Miguel Ave., Berkeley, CA 94707-1535 | Phone: (510) 423-0372 | Email: nautilus@nautilus.org