DEEP DIVE DEBRIEF

CSIS BRIEFS

# NC3

## *Challenges Facing the Future System*

*By Rebecca K.C. Hersman, Eric Brewer, and Suzanne Claeys*

JULY 2020

## THE ISSUE

This brief is the first in the CSIS Project on Nuclear Issues (PONI) Deep Dive Debrief Series that explores emerging or contentious nuclear challenges. These briefs are based on a series of "deep dive" workshops convened by PONI that bring together next generation technical, operational, and policy experts from across the nuclear community to debate and discuss these nuclear challenges. This brief reflects discussion and insights from a deep dive workshop convened by PONI on May 1, 2019, at U.S. Strategic Command (STRATCOM). The brief focuses on the emerging political, informational, and fiscal risks to the U.S. nuclear command, control, and communications (NC3) architecture. Collectively, these non-technical risks pose challenges to the resiliency, durability, and reliability of NC3.

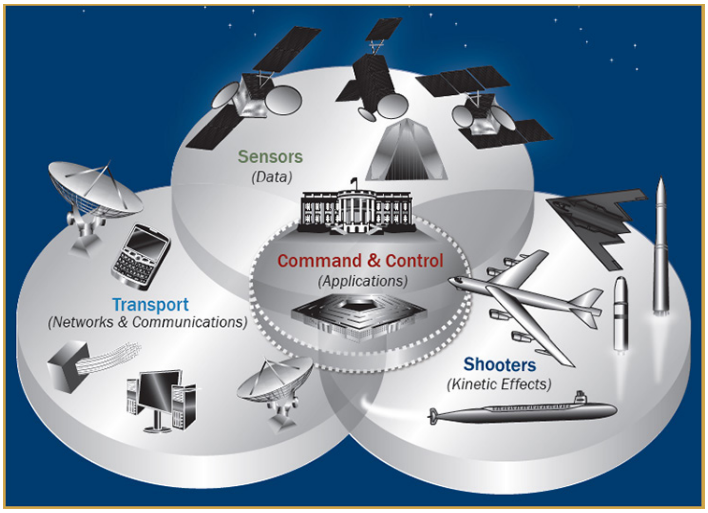
## INTRODUCTION

The current NC3 structure, last comprehensively updated in the 1980s, was designed for a vastly different security environment. Today, the Department of Defense (DoD) has embarked on an ambitious and long-overdue overhaul of the NC3 enterprise that seeks to grapple with the many complex technical demands and security challenges facing this essential system in the years and decades ahead. This system must balance the opportunities afforded by rapid advances in technology with growing concern about cyber risks and other threats to the technical security and reliability of the system. However, while many of the challenges to a resilient and effective NC3 architecture are technical or operational in nature, the resiliency, durability, and reliability of the U.S. NC3 architecture may ultimately rest not only on its technical foundation but on a political and fiscal one as well. Building an enduring and sustainable political foundation for the NC3 system will require broader public understanding of and support for the nuclear decisionmaking process; careful attention to the *public* communication and information management processes that must accompany such a system in crisis; and development of a stronger bipartisan political basis for sustained funding and support.

U.S. nuclear command and control provides the means by which the U.S. president can authorize the use of nuclear weapons in a crisis or conflict as well as the means to prevent unauthorized or accidental use. A fully functional and modernized NC3 enterprise is therefore essential in ensuring the effectiveness of the U.S. nuclear deterrent.[1]

The 2018 *Nuclear Posture Review* (NPR) cited five crucial functions of the NC3 system:

1. Detection, warning, and attack characterization;
2. Nuclear planning;
3. Decisionmaking conferencing;
4. Reception of presidential orders; and
5. Management and direction of forces.




*Source: The Office of the Deputy Assistant Secretary of Defense for Nuclear Matters (ODASD (NM)), "Chapter 2: Nuclear Weapons Employment Policy, Planning And NC3," in Nuclear Matters Handbook 2020 (ODASD(NM)), 2020), https://www.acq.osd.mil/ncbdp/nm/nmhb/chapters/chapter2.htm.*

These functions are carried out through a system of interconnected elements that include warning satellites and radars, communication satellites, aircraft and ground stations, fixed and mobile command posts, and control centers for nuclear systems.[2] The current system is often referred to as having two layers: a "thick-line," which consists of day-to-day and crisis architecture, and a "thin-line," which provides the survivable, secure, and enduring connectivity to the president, secretary of defense, and combatant commanders. NC3 serves as the link between the nuclear forces and presidential authority.[3]

As DoD works to modernize and overhaul the U.S. NC3 architecture, there are a range of complex issues to consider. These include the changing geopolitical and strategic environment, the degree of integration of nuclear and conventional command and control (C2) requirements into a single architecture, different approaches to warning and decision time, the constitutional and legal parameters of the nuclear C2 process, and the future challenges of information warfare and disinformation to the health of the U.S. NC3 system.

## KEY OBSERVATIONS

### Launch Authority, Decisionmaking Processes, and the Legal Basis for Nuclear Use

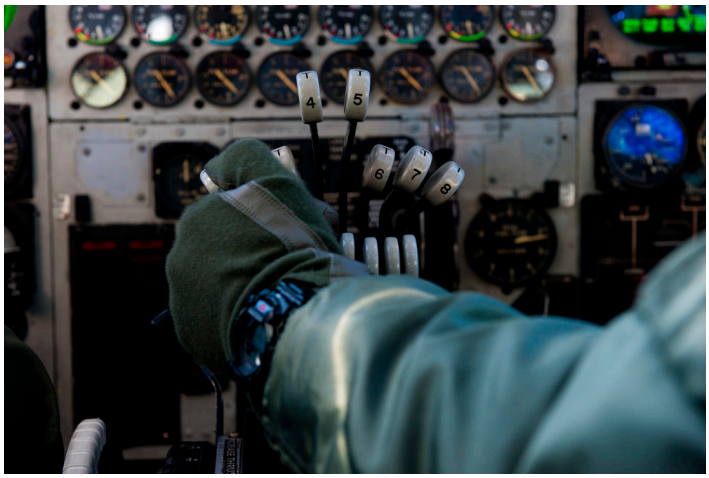
Issues such as nuclear governance, security and human error, chain of command, presidential launch authority, and related declaratory policy issues (e.g., "no first use," "sole purpose," and "launch under warning") face increased scrutiny and debate in policy and political circles. These issues are politically charged, highly polarized, and often acrimonious. These policy considerations stem from concerns about the risks of accidental, unauthorized, or premature nuclear use that could result, in part, from weaknesses in the NC3 system and fears that a system designed for speed of execution may not sufficiently account for the needs of deliberation and political discourse on decisions of such magnitude. Therefore, even as NC3 modernization rightly focuses primarily on ensuring the technical security of the system under circumstances of extreme threat, a contextual understanding of the policy challenges surrounding nuclear use and the need for public and political confidence in the processes and procedures that would guide its implementation in crisis is essential.

Part of the political foundation for the NC3 system rests on a shared understanding of the legitimacy of nuclear weapons, the legal basis for their use, and the process by which that basis is established both in peacetime and crisis. Under Article II of the U.S. Constitution, the U.S. president is commander-in-chief of the U.S. Armed Forces. The nuclear C2 architecture assumes the president to have sole authority over the decision to use U.S. nuclear weapons, a decision that does not require concurrence with military advisers or Congress.[4] The president's sole authority to use nuclear weapons is unique and not subject to the same checks and balances of other war powers. As a result, presidential sole authority has been a point of debate for many years and has resulted in challenges by some members of Congress as early as the 1970s and continuing to present day.[5] Most recently, scholars have also weighed in on the debate, recommending limitations on presidential launch authority to suppress potentially dangerous impulses.[6]

During the workshop, participants discussed a variety of proposals that could be used to formalize a consultative process in certain scenarios and how such proposals could impact the structure of a future NC3 system. Among the alternative structures discussed was the "No First Use Act," designed to prevent the president from "using the Armed Forces to conduct a first-use nuclear strike unless such strike is conducted pursuant to a congressional declaration of war expressly authorizing such strike."[7] The group also discussed other dual-key type arrangements involving other members of the cabinet or members of congressional leadership. However, concerns that limiting presidential launch authority potentially delays response to an imminent attack and damages U.S. deterrence and assurance credibility by increasing complexity and

uncertainty in the presidential decisionmaking process could not be easily overcome. Rather, well short of such complex procedural solutions, politicians and the public may be better reassured by increased education on the NC3 system's warning and authentication processes and increased public confidence in the legal basis on which it rests.

One way this could be done is through the wider dissemination of *Law of War* Manual parameters regarding nuclear attack plans and targeting. Published DoD directives describe how the law of war applies to nuclear weapons use and establish that a legal review process for nuclear operations exists; however, these matters are not generally publicly known or widely discussed. That said, the United States routinely evaluates the legal basis for any military action, and as such an assessment is foundational in any decision to use military force. Such a determination would also accompany any recommendation to use nuclear weapons. While the use of nuclear weapons is legal for the United States, per DoD's *Law of War* Manual, an order to use nuclear weapons still must adhere to the laws of war and, therefore, can only be used against military objectives and cannot be used if it is determined that civilian cost is greater than military gain.[8] Additionally, the United States will only consider nuclear weapons use in extreme circumstances to defend vital interests of the United States or its allies and partners and never against non-nuclear weapon states that are party to the Non-Proliferation Treaty and compliant with their non-nuclear proliferation obligations.[9]



*Source: Air Force Global Strike Command Air Forces Strategic-Air, https://www.afgsc.af.mil/News/Photos/igphoto/2000991184/]*

There is a lack of awareness among the public and the broader nuclear policy community concerning laws of war and whether and how they apply to nuclear weapons use. There is even less understanding, including among the broader nuclear policy community, as to how these considerations are taken into account in the nuclear decisionmaking process and supported by the NC3 system. While so much of the overhaul of the NC3 system is focused on highly classified discussions of technical risks, a more open discussion about how the system supports deliberation and incorporates core principles of civilian control and accountability even in crises of extreme duress could help to ensure confidence in the system and the decisionmaking process it supports.

**Warning, Decision-time, and the Changing Nature of Nuclear Crises**

The changing circumstances under which nuclear crises may occur also open the NC3 system to greater public scrutiny and the need for better integration with public crisis communication strategies. The range of nuclear crisis scenarios is larger and more complex today and will differ greatly from the "classic" launch-under-attack scenarios that drove traditional NC3 plans and requirements. Deep-dive participants emphasized how an increasing variety of nuclear crisis scenarios—such as responding to limited nuclear use, highly asymmetrical conflict with North Korea, and hybrid warfare during a crisis—could unfold under a broader range of timelines and circumstances in which truly private and secretive presidential decisionmaking may not be feasible. In such scenarios, crises may unfold over days, weeks, or even months in much more public ways. At the same time, specific attack or launch warning times may shrink and ambiguity between nuclear and conventional payloads on high-speed delivery platforms—such as those under development in Russia and China—grow in numbers and complexity. In addition, the increasingly dual-use functionality of the U.S. C2 system across conventional and nuclear operations will force alternative approaches to declaratory policy, redundancy/resiliency, and escalation control should some portion of the system come under attack.

*The changing circumstances under which nuclear crises may occur also open the NC3 system to greater public scrutiny and the need for better integration with public crisis communication strategies.*

The NC3 system has become increasing dual-use designed to support both conventional and nuclear operations

and this trend will likely increase in the recapitalized architecture. With the exception of nuclear weapon delivery system control capabilities, each of the assets associated with the NC3 system mentioned by the 2018 *Nuclear Posture Review* is dual-use.[10] Moving forward, the increased comingling of conventional and nuclear communication assets will require alternatives to traditional firebreaks or "disentangling" as a means to limit escalatory risks associated with dual-use systems. For example, conventional missile warning currently relies on dual-use surveillance capabilities, increasing the risk that the dual-use capabilities could be targeted in a conventional conflict for conventional purposes but with potentially profound strategic implications.[11] The "entanglement" risks associated with the integration of conventional and nuclear C2 are part of an active policy debate, especially among nongovernmental analysts and some corners of Capitol Hill.[12] If indeed, the more traditional approach of firebreaks between conventional and nuclear C2 systems as a means of escalation management will not be feasible in the future modernized NC3 system. A clear, unclassified, and accessible explanation for how these "escalation through entanglement" concerns will be addressed must be communicated if enduring, bipartisan support is to be assured.

The future NC3 architecture will therefore need to be responsive to a range of potential crisis scenarios and threat environments. It will also need to account for different decisionmaking styles and information environments. Tailoring processes and systems to the learning styles and executive approaches of individual decisionmakers must be factored into the development process. In addition, as technologies evolve and are implemented in NC3 systems, explanation and familiarization of the technology to a broader subset of decisionmakers beyond the president is needed in order to ensure confidence in the system beyond the narrower nuclear chain of command. Far more must be done to understand how a truly flexible and responsive NC3 architecture would operate and adapt under such widely varying circumstances, especially when considering the high demands for public accessibility and accountability during and after a crisis.

**Public Communication and Information Warfare**

The architecture, procedures, and policies on which the current U.S. NC3 system depends were developed to optimize security, speed, and secrecy, not public scrutiny and confidence. That confidence was assumed as the citizenry and their congressional representatives largely deferred to presidential authority in this domain and entrusted the military with wide-ranging responsibilities of execution and communication. Cloaked in secrecy, the public has little authoritative, fact-based information on many essential C2 questions. The participants discussed and raised major concerns about the risks that disinformation could pose before and during a crisis in ways that could seriously tax the legitimacy of, and confidence in, crisis decisionmaking generally and the NC3 system in particular.

Today, the NC3 system is likely a target for information warfare and disinformation as a means of disrupting presidential decisionmaking and exploiting societal divides to undermine public confidence in the government. Disinformation campaigns could be deployed to distract decisionmakers, slowing their ability to respond in a crisis and giving adversaries an advantage. Furthermore, by promoting false narratives or simply flooding the public with conflicting facts, potential adversaries could break confidence in U.S. institutions and decisionmakers, sow distrust and confusion, and coerce desirable outcomes at lower levels of conflict as publics latch on to the maliciously spread information.

*Today, the NC3 system is likely a target for information warfare and disinformation as a means of disrupting presidential decisionmaking and exploiting societal divides to undermine public confidence in the government.*

While secrecy and opacity can be advantageous in countering some threats to the NC3 system, they simultaneously increase the vulnerability of NC3 to disinformation tactics, which attack public confidence in the system rather than attacking the system itself. Weaponized social media, targeted adversary message amplification through conspiracy theorists and automated bots, and the strategic use of deepfakes are just a few examples of how the new age of information warfare could threaten the confidence in and legitimacy of NC3 systems. The future NC3 system must better balance trade-offs in complexity, effectiveness, and resiliency as well as security and transparency to address the disinformation threat.

## RECOMMENDATIONS

Workshop participants recognized the need to prioritize technical resilience and capacity but agreed that political, informational, and fiscal challenges to the national NC3 architecture are underappreciated and pose substantial challenges to fielding an effective and durable NC3 system. These challenges include adequate funding and resources, lengthy acquisition time horizons, the need for sustained political support, changes in adversaries, and threats and risks from emerging technology. The NC3 system cannot exist in a technical vacuum, and therefore the system must inspire trust and confidence not only with decisionmakers but also with the public and allies and partners. To do so, the United States requires a comprehensive understanding of the non-technical challenges facing NC3 in ways that are more transparent and more easily communicated. The United States also must preserve security and reliability in the context of NC3's essential missions.

*The future NC3 system must better balance trade-offs in complexity, effectiveness, and resiliency as well as security and transparency to address the disinformation threat.*

In light of this analysis, the group produced a series of recommendations to ensure the future NC3 system is resilient in the face of growing domestic, international, and strategic risks:

**Develop more effective, and informed, champions for the NC3 system in Congress and across the NGO community.** Participants expressed deep concern that the NC3 system lacks effective political and funding advocacy and risks politicization, especially if conjoined with more contentious nuclear issues such as sole authority, No First Use, or nuclear modernization funding. Participants advised that NC3 can and should be kept depoliticized and treated as the "no brainer" requirement regardless of how broader nuclear modernization efforts unfold in the decades to come. Continued openness and engagement from STRATCOM as the system integrator can facilitate such efforts.

**Develop and communicate a clear, consistent, and compelling narrative to explain and justify the nation's NC3 system to the public.** Openness, communication, and education on NC3 systems and purpose will build stronger public support, strengthen the system's defenses against political and budgetary attack, and establish strong legitimacy for the NC3 system while also improving resilience to adversary disinformation.

**Enhance communications and bolster confidence through increased transparency on the function and effectiveness of the system as well as the risks the current NC3 system faces from cyber, information, and hybrid warfare.** There needs to be a better appreciation of the risks these challenges pose to U.S. crisis decisionmaking processes and how the system can defend against them. Public or individual confusion as to "who" constitutes the United States' authentic national command authority could be devastating, even if senior decisionmakers remain confident in the system. In particular, the United States should work to constructively communicate these risks and U.S. strategy to manage these risks with allies and partners, who in turn communicate with their own publics. Communication with allies and partners on risks and strategy to mitigate risks is essential to building confidence and legitimacy.

**Better integrate NC3 in terms of strategy, plans, and policy to consider the potential interactions between nuclear and nonnuclear crises.** Some potential steps include: developing policies and plans to authenticate alternative sources of information; initiating risk reduction dialogues with the Russians to create "no-go-zones"; developing alternative firebreaks to limit escalation risks should a dual-use system be targeted in conventional conflict; publishing an unclassified and accessible explanation for how escalation through entanglement concerns will be addressed; and incorporating action plans to ensure crisis communications hotlines and other communication systems are hardened against information warfare in case these dialogues fail.

**Do not leave the front door open.** So much effort has been devoted to "back door" cyber risks to the U.S. NC3 system, but the "front door"—which may not require any access to the system itself—cannot be left undefended. The NC3 architecture must be inoculated against information warfare during pre-crisis and crisis times and anticipate the need to use aggressive and public authentication measures during a crisis. Authenticating "good" information and debunking "bad" information will be a hallmark of future crises. This is critical not only to inform internal decisionmaking processes but also to manage allies, partners, publics, and broader governmental institutions during crises that will require reassurance on the legitimacy and reliability of U.S. systems. The technical and policy challenges associated with counter-disinformation efforts must be incorporated into the strategy and architecture for the U.S. NC3 system. ■

***Rebecca K.C. Hersman*** *is director of the Project on Nuclear Issues and a senior adviser for the International Security Program at the Center for Strategic and International Studies (CSIS) in Washington, D.C.* ***Eric Brewer*** *is deputy director and senior fellow with the Project on Nuclear Issues at CSIS.* ***Suzanne Claeys*** *is a program coordinator and research assistant for the Project on Nuclear Issues at CSIS.*

*Nothing in this briefing should be understood to convey the view or position of any U.S. government organization or its employees. Nor does it imply the endorsement of the contents of the report by any government organization or its employees.*

*This research was made possible through the generous support of the Defense Threat Reduction Agency.*

## ENDNOTES


1. Deputy Assistant Secretary of Defense for Nuclear Matters, *Nuclear Matters Handbook* (Washington, DC: DoD, 2016), 73, https://www.acq.osd.mil/ncbdp/nm/nmhb/chapters/chapter_6.htm.
2. Office of the Secretary of Defense, *Nuclear Posture Review* (Washington, DC: DoD, 2018), 56, https://dod.defense.gov/News/SpecialReports/2018NuclearPostureReview.aspx.
3. Ibid.
4. Amy F. Woolf, "Defense Primer: Command and Control of Nuclear Forces," Congressional Research Service, *In Focus*, January 10, 2020, https://fas.org/sgp/crs/natsec/IF10521.pdf.
5. Stephen P. Mulligan, "Legislation Limiting the President's Power to Use Nuclear Weapons: Separation of Powers Implications," Congressional Research Service, November 23, 2017, 11-12, https://fas.org/sgp/crs/nuke/separation.pdf; and Owen Daugherty, "Dems Reintroduce Bill to Prevent Nuclear First Strike Without Congressional Approval," *Hill*, January 29, 2019, https://thehill.com/policy/defense/427546-dem-lawmakers-reintroduce-bill-to-prevent-president-from-launching-nuclear.
6. Rachel Elizabeth Whitlark, "Should Presidential Command Over Nuclear Launch Have Limitations? In a Word, No," *Texas National Security Review* 2, no. 3 (May 2019), https://tnsr.org/roundtable/should-presidential-command-over-nuclear-launch-have-limitations-in-a-word-no/#_ftn2; and Lisbeth Gronlund, David Wright, and Steve Fetter, "How to Limit Presidential Authority to Order the Use of Nuclear Weapons," Bulletin of the Atomic Scientists, January 23, 2018, https://thebulletin.org/2018/01/how-to-limit-presidential-authority-to-order-the-use-of-nuclear-weapons/.
7. From H.R.669 - Restricting First Use of Nuclear Weapons Act of 2017 (https://www.congress.gov/bill/115th-congress/house-bill/669) and S.200 - Restricting First Use of Nuclear Weapons Act of 2017 (https://www.congress.gov/bill/115th-congress/senate-bill/200).
8. DoD's *Law of War Manual* clearly states, "the United States has not accepted a treaty rule that prohibits the use of nuclear weapons per se, and thus nuclear weapons are lawful weapons for the United States." Department of Defense, *Law of War Manual* (Washington, DC: 2015), 7, http://archive.defense.gov/pubs/law-of-war-manual-june-2015.pdf.
9. Ibid., 393-394.
10. Rebecca Hersman et al., *Under the Nuclear Shadow: Situational Awareness Technology and Crisis Decisionmaking* (Washington, D.C.: CSIS, March 2020), 11, https://csis-prod.s3.amazonaws.com/s3fs-public/publication/200318_UnderNucearShadow_FullReport_WEB.pdf?VJm_nrx2bVVeByYH38yx8YkDvvr1QZVW.
11. Ibid.
12. James 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 (2018), https://www.mitpressjournals.org/doi/full/10.1162/isec_a_00320.