The Next Generation NC3 Enterprise: Opportunities and Challenges

Jake Hecla, Rebecca Krentz-Wee, and Andrew W. Reddie
Nuclear Policy Working Group; University of California, Berkeley
Corresponding author: areddie@berkeley.edu
Keywords: emerging technology; nuclear policy; NC3; command and control.

Executive Summary: The 2018 Department of Defense Nuclear Posture Review emphasized the importance of modernizing the existing nuclear command, control, and communications (NC3) architecture. Heightened awareness of US reliance upon technology developed in the 1970s and emerging challenges posed by frontier technologies spurred Secretary of Defense Mattis to task USSTRATCOM with identifying the technologies, processes, and institutions needed to build a next-generation NC3 system. General Hyten, USAF Commander, has noted that this will require an "overhaul of our existing processes from requirements definition to systems engineering and integration, acquisition, and budgeting. A framework is required for modern processes to enable delivery of a flexible, continuously evolving, threat-driven set of capabilities." This brief, prepared in response to Gen. Hyten's call for memoranda to address the "Next Generation NC3 Enterprise," outlines three distinct approaches to NC3 modernization, each with a system lifecycle of approximately 50 years (2030-2080): upgrading the existing system, a hybrid approach to integrating new technologies, and creating an entirely new NC3 architecture. It is organized as follows: First, it outlines the integral role of NC3 in strategic operations. Second, it examines the current status of NC3 tools and the contemporary challenges that future systems must address. Third, it provides a series of paths forward for USSTRATCOM's consideration. Fourth and finally, it recommends a "hybrid" approach to maintain the strengths of the current NC3 architecture, increase the resilience of the system, and leverage the advantages of new sensing, ISR, and communication technology.

I. The Current Roles of NC3

NC3 fulfills three broad roles. As these roles are not encapsulated in a single system, it is more accurate to conceptualize NC3 as a patchwork of overlapping capabilities rather than as a singular system.

The first role of NC3 is to provide an early warning and/or sensing of strategic actions taken by a strategic adversary. In the United States, this capacity is mainly fulfilled by the Integrated Tactical Warning/Attack Assessment (ITW/AA) system of satellites alongside fixed and mobile radar systems and information processing systems. The second role is to provide point-to-point communication between the President and U.S. nuclear forces. This system can be conceptualized as a series of nodes that pass a signal from the President to Air Force bases, missile silos, and submarines that are responsible for the U.S. strategic deterrent. The third role is to supply decision support to policy-makers and commanders.

The second and third roles require a combination of command facilities and communications equipment. The primary nuclear command and control facility is located at the Pentagon; the second land-based facility is situated at Offutt AFB, USSTRATCOM. The E-4B National Airborne Operations Center and E-6B Take Charge and Move Out (TACAMO)/Airborne Command Post provide additional, survivable alternative command posts and airborne communications in the event that land-based facilities are compromised. Other communication equipment used in the NC3 architecture include land-

based phone lines, undersea cables, and both military and commercial satellites. Having redundant forms of communication ensures that there will be survivable, secure, and enduring communications in a variety of operation scenarios and threat environments.

II. Contemporary Challenges

The 2018 Nuclear Posture Review called for "effective functioning and modernization" of the NC3 architecture to reflect emerging challenges and the address the ossification of the existing architecture[1]. Although modernization of some network communication systems began in 2015, most of them date back to the Cold War period. As a result, many hardware systems and software programs are antiquated, unsupported, and potentially unreliable—particularly systems commercial-off-the-shelf (COTS) components built by companies at deployment that no longer exist. Furthermore, given the variety of threat landscapes faced by U.S. strategic forces, including geopolitical challenges posed by Russia, China, and North Korea and technological challenges posed by disruptive artificial intelligence and quantum technologies, a modern system must be vastly more reliable and flexible than the current arrangement is[2]. Finally, a modernized NC3 architecture must be able to adequately respond to the current threat environment, which includes small states seeking nuclear weapons and cyber-attacks that probe NC3 networks[3]. At the same time, however, introducing new technologies to build the next generation of networked systems has the potential to simultaneously introduce new cyber-based or air-gapped vulnerabilities[4]. As the next generation of nuclear bombers, missiles, and submarines are built, new NC3 components and processes must remain resilient and robust to these emerging threats.

III. Path forward

Given the immediate challenges posed by aging equipment and a changing threat environment, we outline three options for addressing next-generation NC3 systems. The first is a dedicated NC3 network which leverages the existing NC3 architecture but uses modernized equipment. This is the so-called "singular option," which seeks to leverage the security inherent in a system which has been continually tested for over forty years. The second approach is a "mixed" system which updates portions of the existing NC3 structure with modernized components, but redesigns high-risk nodes including portions of the satellite network. The final option is a largely redesigned, dual-capable NC3 system which seeks to benefit from the advances of modern computing and digital communications. Given the increased vulnerability of these systems, there are several steps which might mitigate the risk including the deployment of countermeasures to reduce cyber vulnerability as well as leveraging commercial systems such as microsatellite constellations to provide a robust NC3 architecture.

IV. NC3 Options

i. Upgrades within existing NC3 architecture

The "minimal-change" option provides a replacement NC3 network that revitalizes the existing infrastructure using modern, analog componentry. This approach modernizes the physical hardware on satellites, aircraft and in various cable/RF data transmission lines but would not fundamentally alter the layout of these systems. This option takes advantage of the fact that the basic structure of the system has been well-established and tested repeatedly over the last four decades. As a result, the current state of the NC3 architecture is "both secure and resilient," as described by Gen. Hyten[5]. The modernization and hardening of legacy chips, transmitters, and electronic systems will be costly, but security is likely to remain high, as the attack surface for these systems is limited due to the high-security standards under which they were originally developed.

However, maintaining the physical structures of the existing NC3 system may not prove an ideal solution in the long-term. Notable failures of the existing NC3 network have resulted in the misplacement of nuclear weapons as well as near-launch situations including the '07 Doom 99 incident and '79 NORAD false alarm. Adversaries have also had upwards of forty years to develop strategies which take advantage of weak points in the existing structures, and multiple leaks of classified information relating to those systems have occurred. Furthermore, technology has dramatically changed since the inception of the current NC3 architecture, and certain nodes in the current NC3 architecture may therefore become more vulnerable to attack going forward. In particular, anti-satellite weapons, satellite blinding technologies, and other offensive space capabilities

are evolving rapidly and may give potential adversaries the ability to disrupt U.S. space assets. Improvements in computing may also render encryption standards used for existing NC3 systems vulnerable. Though this list is far from comprehensive, there is inherent risk in maintaining a legacy structure in the face of evolving threats.

ii. Mixed-upgrade option

The "mixed-upgrade" option keeps the contours of the existing NC3 structure intact, but adds new technologies where needed to increase the resiliency of the system while mitigating the risk posed by single points of failure. This option maintains continuity and leverages the existing strengths of the NC3 architecture. Some portions of the NC3 network are unlikely to require upgrades, such as the existing communication cables that connect sites. Other systems, however, may need to be fundamentally altered. One well-publicized area of vulnerability is the early-warning satellite network. Because of the small number of satellites and the rapidly advancing array of anti-satellite technologies, this node of the NC3 network may become significantly more vulnerable—particularly given the use of dual phenomenology in which two information systems are needed to confirm an attack. Swarms of smallsats would greatly increase the number of targets, providing redundancy and resiliency in the network. Pseudo-satellites may also provide another alternative to TACAMO aircraft during crises, making them vulnerable for a much shorter period of time. Both systems are significantly cheaper than existing satellites.

Integrating new systems to address vulnerable nodes in the network presents a challenge of integration, as different generations of technology have been built to use different protocols and standards. New systems may also lead to non-nuclear command and control, which has the potential to lead to unintended escalation in the event that they are targeted by an adversary[6,7].

iii. Maximal option – new NC3 architecture

The "maximal" option develops an entirely new NC3 network. It leverages advances in chip design, software, and hardware to enable a vastly more resilient and flexible NC3 structure using a variety of signals, including traditional wired and radio systems, along with new LIDAR, fiberoptic, and hyperspectral technologies, for communication and detection. In such a system, the speed of communication would be massively improved, especially for submarine communications, while the use of cutting-edge technologies would allow for a reduction in the number of single points of failure in the chain from detection to response. Adversaries would also face the challenge of dealing with a new attack surface.

A notable downside to using a new architecture is the time it is likely to take to completely reconceptualize the security architecture. This approach would require a much larger codebase, which offers a larger digital attack surface. A new and larger codebase also has the potential for more zero-day vulnerabilities (particularly if the system is relying upon COTS technology), making the system vulnerable as it is being developed. A completely new framework would place additional stress on the continued function of NC3, as the old architecture would need to be maintained while the new architecture is developed, and there is a risk that the existing NC3 architecture will degrade before the new system is fully and securely implemented. It is also worth noting the high cost associated with this option in terms of both human capital and funds necessary to reimagining the NC3 architecture.

V. Recommendation

Considering the changing threat environment and the age of current systems, maintaining current NC3 infrastructure is not tenable. Likewise, a complete reimagining of the command and control infrastructure is likely to be cost-prohibitive and would upgrade portions of the system that are not under threat from the changing security environment. Thus, we recommend the "mixed-upgrade" option that strategically addresses the shortcomings of identified vulnerabilities in the existing NC3 network.

References

[1]. 2018 Nuclear Posture Review: https://dod.defense.gov/News/SpecialReports/2018NculearPostureReview.aspx

[2]. Peter Hayes. "Nuclear Command, Control, and Communications (NC3): Is there a ghost in the machine," Nautilus Institute (2018): Available at: https://www.nonproliferation.org/wp-content/uploads/2018/04/180409-nc3-is-there-a-ghost-in-the-machine.pdf

[3]. Gartzke, Erik, and Jon R. Lindsay. "Thermonuclear cyberwar." Journal of cybersecurity 3, no. 1 (2017): 37-48.

[4]. Dunnmon, Jared. "Nuclear Command and Control in the Twenty-First Century: Maintaining Surety in Outer Space and Cyberspace," A Collection of Papers from the 2016 Nuclear Scholars Initiative and PONI Conference Series, CSIS Project on Nuclear Issues (2016).

[5]. Hyten, John E., and SSQ. "An Interview with Gen John E. Hyten: Commander, USSTRATCOM: Conduct 27 July 2017." Strategic Studies Quarterly 11, no. 3 (2017): 3-9.

[6]. Acton, James M. "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): 56-99;

[7] Peters, Robert, Justin Anderson, and Harrison Menke. "Deterrence in the 21st Century: Integrating Nuclear and Conventional Force." Strategic Studies Quarterly 12, no. 4 (2018): 15-43.

Jake Hecla is a graduate student in the Department of Nuclear Engineering at the University of California, Berkeley, where he studies radiation detection technologies. He holds a degree in Nuclear Science and Engineering from MIT.

Rebecca Krentz-Wee is a Ph.D. candidate in the Department of Nuclear Engineering, University of California, Berkeley, where she studies radiation detection and arms control. She holds a B.S. in Nuclear Science and Engineering from MIT.

Andrew W. Reddie is a Ph.D. candidate in the Charles and Louise Travers Department of Political Science, University of California, Berkeley, where he studies international relations, nuclear policy, and arms control. He holds an M.Phil in International Relations from Oxford University and M.A and B.A. (hons.) from the University of California, Berkeley.

Acknowledgements

The authors would like to acknowledge the contribution of UC Berkeley's Nuclear Policy Working Group to the framing and development of this project. We would like to especially thank Dr. Bethany Goldblum and Chance Boreczky for their research and editorial support. AR would like to acknowledge support from the Department of Energy National Nuclear Security Administration through the Nuclear Science and Security Consortium under Award Number DE-NA0003180. This report was prepared as an account of work sponsored by an agency of the United States Government. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.