RAND CORPORATION

Research Report

DON SNYDER AND ALEXIS A. BLANC

Unraveling Entanglement

Policy Implications of Using Non-Dedicated Systems for Nuclear Command and Control

The systems used for command and control in the U.S. military are undergoing modernization with an eye toward greater integration and interoperability.[1] Recent arguments have emphasized the increased risk of inadvertent escalation from integrating and comingling systems that support conventional command and control and systems that support nuclear command and control (NC2).[2] We argue that these concerns are overstated and that the risks introduced are manageable. That said, the different risks associated with using non-dedicated systems for NC2 warrant more-focused attention to (1) achieve mission assurance for command and control, (2) retain presidential and senior leader confidence in command and control capabilities even when systems degrade under attack, and (3) control the ability to send and receive signals of resolve and restraint through command and control.

KEY FINDINGS

- A concept labeled entanglement has recently gained currency within the academic nuclear policy community. Advocates of entanglement claim that using systems in common for nuclear and conventional command and control risks inadvertent escalation.
- Even if command and control systems could be perfectly disentangled, it would not guarantee the avoidance of inadvertent escalation risks.
- Risks of inadvertent escalation from the use of non-dedicated systems for nuclear command and control can be managed.

Entanglement: New? Avoidable?

A concept labeled *entanglement* has recently gained currency within the academic nuclear policy community.[3] James Acton, the most prominent advocate of entanglement, argues that

> the risks of inadvertent escalation are . . . likely to increase significantly in the future. Driving these risks is the possibility that Chinese, Russian, or U.S. C3I [command, control, communications, and intelligence] assets located outside—potentially far outside—theaters of operation could be attacked over the course of a conventional conflict. These assets include satellites used for early warning, communication, and intelligence, surveillance, and reconnaissance (ISR); ground-based radars and transmitters; and communication aircraft. Such assets constitute

> key nodes in states' nuclear C3I systems, but they are also "entangled" with nonnuclear weapons in two ways. First, they are typically dual use; that is, they enable both nuclear and nonnuclear operations. Second, they are increasingly vulnerable to nonnuclear attack—much more vulnerable, in fact, than most nuclear-weapon delivery systems.
>
> Entanglement could lead to escalation because both sides in a U.S.-Chinese or U.S.-Russian conflict could have strong incentives to attack the adversary's dual use C3I capabilities to undermine its nonnuclear operations. As a result, over the course of a conventional war, the nuclear C3I systems of one or both of the belligerents could become severely degraded. It is, therefore, not just U.S. nonnuclear strikes against China or Russia that could prove escalatory; Chinese or Russian strikes against American C3I assets could also . . . .[4]

Our review of primary source documents from the Cold War suggests that any argument or concern about entanglement that is predicated on the assumption that, in the past, the United States solely fielded systems dedicated to the nuclear mission, is flawed.[5] The Cold War–era command and control systems were never fully or substantially "disentangled." For strategic nuclear weapons, the United States fielded a few specialized assets to communicate with certain nuclear-only weapon platforms, such as the Emergency Rocket Communications System. But the ubiquity of substrategic nuclear weapons at the time also drove the use of general-purpose command and control for NC2. Any system capable of command and control of nuclear forces was considered available for such use, and the full functioning of NC2 relied on systems not dedicated to NC2 for pre-, trans-, and post-nuclear attack phases.

We found no evidence that historical decisions about command and control systems were based on concerns about inadvertent escalation stemming from entanglement. Rather these decisions were organizationally bounded and were made first and foremost on how to ensure a *survivable* set of systems for each organization that would allow for escalation control.[6] The historical record thus contradicts the notion of employing dedicated systems for the sake of mitigating the risks of inadvertent escalation. Concerns about escalation significantly motivated decisionmakers, but the primary emphasis was on sufficient survivability of command and control to operate in a protracted, limited nuclear war.

Indeed, some commingling of nuclear and conventional command and control systems is inevitable. Some processes or procedures between conventional and nuclear command and control might plausibly be entirely separated. But tactical warning systems are an example of a situation in which separation is problematic. Ground-based radars or overhead collection cannot generally distinguish between conventional- and nuclear-armed weapons.

Even if command and control systems could be perfectly disentangled, it would not guarantee the avoidance of inadvertent escalation risks. A command and control system can be used for whatever purpose the United States desires, regardless of what is implied or declared. Processes and procedures could be used to impose artificial constraints, but there is no physical or technical limitation preventing the United States from employing nominally dedicated NC2 systems to support the conventional warfighter. Therefore, without invasive, continuous inspections, it is nearly impossible for any state to

We found no evidence that historical decisions about command and control systems were based on concerns about inadvertent escalation stemming from entanglement.

fully assure adversaries that these systems can solely be used for the control of nuclear forces and not conventional forces.

But the entanglement argument cannot be dismissed on these grounds alone, if only because circumstances have changed since the Cold War. Conventional weapons will increasingly be able to hold at risk systems that support nuclear warfare in a nonnuclear conflict and do so in a manner that was not possible during the Cold War. Antisatellite weapons and their potential use against space-based early warning assets are a concrete example. Long-range precision-guided munitions and cyber weapons and their potential use to infiltrate and disable command and control networks, respectively, offer further examples.

The term *entanglement* implies an undesired snarled state of nuclear and conventional command and control that should be undone but is difficult to undo. The term also implies that the decision to field non-dedicated NC2 systems is a binary one, which mischaracterizes the decision at hand. Some systems can be dedicated and others not. To the extent that non-dedicated systems create entanglement, that entanglement will vary depending on the number of non-dedicated systems, the roles that they play, and how decisionmakers respond to attacks on each system. For these reasons, we favor the more neutral phrase *non-dedicated systems for NC2*.

Risk of Inadvertent Escalation

The extended use of non-dedicated systems for NC2 can lead to inadvertent escalation by triggering regrettable reactions by both adversarial and U.S. leaders.

The use of non-dedicated systems for NC2 could perversely incentivize adversaries to attack those systems in two ways. First, although a variety of redundant and diverse systems that can support NC2 can increase U.S. mission assurance, it also lowers the stakes for an adversary to attack individual systems. Because the consequences of destroying or disabling individual systems would be lower, so, too, are the disincentives that restrain an adversary from attacking them. Second, extensive use of non-dedicated systems for NC2 without nuclear hardening—relying instead on other means for survivability—could incentivize an adversary to escalate to limited nuclear use to defeat U.S. conventional forces.[7]

The use of non-dedicated systems for NC2 could also contribute to inadvertent escalation by U.S. president, commanders, or their advisers. Attacks on command and control systems could cause degradation of command and control, leading to decisions to escalate in order to avoid defeat. Such inadvertent escalation on the U.S. decisionmaking side could arise from two sources. The first source is *intent ambiguity*—i.e., when the intended target of attacks on command and control systems is unclear. If attacks on non-dedicated systems begin to erode NC2 capabilities, is that the intent of the adversary, or is it an unintended consequence of intended degradation of conventional command and control? The second source of inadvertent escalation is U.S. decisionmakers being caught *by surprise by the impact of attacks* on non-dedicated systems. If the patterns of capability loss are unexpected, a president and their advisers might choose to escalate prematurely in order to avoid greater losses in NC2 capabilities.

Another factor that could lead to inadvertent escalation affects both adversaries and U.S. leaders: the diminished ability to send and receive signals of resolve and restraint. In general, the more segregated the systems are for nuclear and conventional command and control, the more opportunities exist for all sides to send clear signals; the more commingled, the fewer the opportunities to send clear signals via command and control. The loss of signaling abilities can increase escalation risks.

Finally, it is vital to remember that escalation management also requires a willing, rational, and capable partner. Both sides must choose to exercise restraint in the targeting of the other's command and control capabilities. Both sides must also be able to perform attack characterization and assessment and control their forces.[8] Paradoxically, when U.S. planning for survivable capabilities allowing for protracted, limited nuclear conflict was at its height during the Cold war, military planners in the Soviet Union appear to have rejected the notion that controlled, limited strategic nuclear operations was possible.[9] In the present day, the United States

Above all, command and control must serve the needs of commanders at all phases of war, and those commanders must have and retain confidence in command and control capabilities even when systems are degraded under attack.

confronts two potential challengers—Russia and China—that emphasize escalation management.[10] This circumstance suggests that ensuring survivability of mission-essential functions to enable escalation management should be a priority for the Department of the Air Force (DAF) as it weighs what the future NC2 architecture should look like.

Pathways to Manage Risk of Inadvertent Escalation

Thus far, we have argued that the use of non-dedicated systems for NC2 was extensive during the Cold War and that some use of non-dedicated systems today is unavoidable. Therefore, there are some risks of inadvertent escalation and reduction in opportunities to send clear, unambiguous signals. But even if systems could be perfectly segregated between nuclear and conventional roles, the challenges of verification would preclude reducing the risks of inadvertent escalation to zero. Fortunately, these risks are not intrinsic to the use of non-dedicated systems: Risks emerge from how systems are implemented; therefore, inadvertent escalation can be managed. What are promising pathways to manage these risks?

The key issues faced in implementation of the system-of-systems for command and control are (1) the extent of the use of non-dedicated systems (i.e., the number of systems), (2) which systems are non-dedicated, and (3) how those systems are structured to support specific command and control functions.

Above all, command and control must serve the needs of commanders at all phases of war, and those commanders must have and retain confidence in command and control capabilities even when systems are degraded under attack.[11] Choices for using or not using non-dedicated systems for NC2 can increase or decrease robustness of command and control and the confidence of commanders in it. Robustness of command and control arises from a portfolio of methods, such as the following:

- defending systems (through hardening, active defense, and deterrence)
- complicating adversary targeting (through proliferating systems, making systems hard to find—e.g., by mobility or deception—and leveraging mutual stakes from attacking systems)
- resiliency measures (through redundancy and diversity of systems, architecture of the system of systems, the ability to rapidly reconstitute systems, and the ability to adapt processes).

This portfolio of methods must work satisfactorily against all types of threats and hazards, which range from day-to-day threats (such as hostile insiders and cyber operations) to nuclear weapon effects. Hardening against the latter is necessary to operate, de-escalate, and terminate in trans- and post-nuclear phases of war. But survivability of systems to nuclear weapon effects is generally costly, which can limit the number of hardened systems.

The system-of-systems supporting command and control must be designed to meet all these needs. Pathways to achieve these sufficiently to mitigate inadvertent escalation risks include the following:

- Design command and control to ensure that needs at every level of military activity—from day-to-day readiness through crisis/gray conflict, conventional war, regional conventional war with potential or limited nuclear use, to general nuclear war—are met to the satisfaction of the relevant leaders and commanders,
- Monitor the mission assurance of command and control functions under all foreseeable threats and hazards.
- Assess how command and control capabilities would degrade when under attack.
- Communicate the expected degradation to relevant leaders.

If these implementation challenges are sufficiently addressed, the additional robustness would make the impact of an attack on any specific system less consequential and thereby reduce inadvertent escalation.

The greater the number of systems that are dedicated for NC2, the more opportunities exist for signaling and the lower the chances of signaling ambiguity. Because strategic signaling is a national-level activity, decisions must be made about whether to pay the expense to expand signaling opportunities, to accept the risk of reducing signaling opportunities, or to design the system of systems for command and control in a way that masks signaling even during escalation. Furthermore, these decisions must be made with the consultation of authorities above the service level. The pathways to reduce signaling-related risks include the following:

- Assess signaling opportunities presented by non-dedicated design architectures for command and control for both the United States and its adversaries.
- Choose the extent of non-dedicated system use. These choices should be
  - informed by signaling opportunities
  - made in consultation with above-service-level authorities who would send and receive strategic signaling.

Notes

[1] This report includes and builds on arguments made in Snyder et al., 2023. Also see Hoehn, 2021; and Deptula and LaPlante, 2019.

[2] See Acton, 2018; Hersman, et al., 2020; Colby 2016.

[3] Most prominently, see Acton, 2018.

[4] Acton, 2018, pp. 57–58.

[5] See, for example, Hersman et al., 2020, for this claim. For an extended discussion of the historical record, see Chapter 2 of Snyder et al., 2023.

[6] Ball, 1981, pp. 17–25.

[7] These escalation risks come to the fore during a crisis or conflict; neither concern seems compelling while general deterrence persists.

[8] Ball, 1983, pp. 201–202.

[9] Hines, Mishulovich, and Shulle, 1995, p. 24.

[10] Kaufman and Hartnett, 2016; Kofman, Fink, and Edmonds, 2020.

[11] Department of Defense, 2018, p. i; Department of Defense, 2010, p. xiv.

References

Acton, James M., "Escalation Through Entanglement: How the Vulnerability of Command-and-Control Systems Raises the Risks of an Inadvertent Nuclear War," *International Security*, Vol. 43, No. 1, Summer 2018, pp. 56–99.

Ball, Desmond, "Can Nuclear War Be Controlled?" *Adelphi Papers*, London: International Institute for Strategic Studies, Vol. 21, No. 169, 1981.

Ball, Desmond, "Soviet Strategic Planning and the Control of Nuclear War," *The Soviet and Post-Soviet Review*, Vol. 10, No. 1, January 1983, pp. 201–217.

Colby, Elbridge, *From Sanctuary to Battlefield: A Framework for a U.S. Defense and Deterrence Strategy for Space*, Washington, D.C.: Center for a New American Security, January 2016.

Department of Defense, *Nuclear Posture Review Report*, Washington, D.C., April 2010.

Department of Defense, *Nuclear Posture Review*, Washington, D.C., February 2018.

Deptula, David A., and LaPlante, William A., with Robert Haddick, *Modernizing U.S. Nuclear Command, Control, and Communications*, Arlington, Va.: Mitchell Institute for Aerospace Studies, Air Force Association, February 2019.

Hersman, Rebecca, Reja Younis, Bryce Farabaugh, Bethany Goldblum, and Andrew Reddie, *Under the Nuclear Shadow: Situational Awareness, Technology, and Crisis Decisionmaking*, Washington, D.C.: Center for Strategic & International Studies, March 2020.

Hines, John, Ellis M. Mishulovich, and John F. Shulle, *Soviet Intentions 1965–1985*, Vol. 2, *Soviet Post–Cold War Testimonial Evidence*, McLean, Va.: BDM Federal, Inc., 1995.

Hoehn, John R., *Joint All-Domain Command and Control: Background and Issues for Congress*, Washington, D.C.: Congressional Research Service, R46725, August 12, 2021.

Kaufman, Alison A., and Daniel M. Hartnett, *Managing Conflict: Examining Recent PLA Writings on Escalation Control*, Alexandria, Va.: Center for Naval Analysis, DRM-2015-U-009963-Final3, February 2016.

Kofman, Michael, Anya Fink, and Jeffrey Edmonds, *Russian Strategy for Escalation Management: Evolution of Key Concepts*, Alexandria, Va.: Center for Naval Analysis, DRM-2019-U-022455-1Rev, April 2020.

Snyder, Don, Alexis A. Blanc, Edward Geist, James Williams, Cortney Weinbaum, Myron Hura, Jennifer Brookes, Brian Dolan, Sarah MacConduibh, Tim McDonald, and Matthew Sargent, *On the Use of Non-Dedicated Systems for Nuclear Command and Control: Considerations for the Department of the Air Force*, Santa Monica, Calif.: RAND Corporation, RR-A976-1, 2023, Not available to the general public.

Acknowledgments

We thank Major General Andrew (Andy) Gebara and Major General Jason Armagost for sponsoring this research. Brigadier General Mark (Zulu) Pye, Colonel Craig Ramsey, and Michael (Swede) Tichenor provided critical support to the work at various stages of the project. We had a number of constructive discussions with individuals in and out of government regarding the usage of non-dedicated systems for the command and control of nuclear forces. These conversations were stimulating and refined our thinking. We especially thank the MITRE Corporation for many helpful discussions.

At RAND, we thank Lieutenant General (retired) Robert (Bob) Elder, Jr. and Jim Quinlivan for many enlightening discussions, and Walter Nelson for tracking down archival materials.

For access to a number of documents helpful in our research, we thank the Defense Threat Reduction Agency for access to the Defense Threat Reduction Information Analysis Center Scientific and Technical Information Archival and Retrieval System. We also thank the National Archives and Records Administration, in particular Sarah Waitz, for access to Senate and House hearing transcripts.

That we received help and insights from those acknowledged above should not be taken to imply that they concur with the views expressed in this report. We alone are responsible for the content, including any errors or oversights.

About This Report

The objective of this project was to evaluate the benefits and potential downsides of the use of non-dedicated systems for the command and control of nuclear operations. The research reported here was commissioned by Air Force Global Strike Command and conducted within the Force Modernization and Employment Program of RAND Project AIR FORCE as part of a fiscal year 2021 project, "Nuclear Command and Control over Assured Communications."

RAND Project AIR FORCE

RAND Project AIR FORCE (PAF), a division of the RAND Corporation, is the Department of the Air Force's (DAF's) federally funded research and development center for studies and analyses, supporting both the United States Air Force and the United States Space Force. PAF provides the DAF with independent analyses of policy alternatives affecting the development, employment, combat readiness, and support of current and future air, space, and cyber forces. Research is conducted in four programs: Strategy and Doctrine; Force Modernization and Employment; Resource Management; and Workforce, Development, and Health. The research reported here was prepared under contract FA7014-16-D-1000.

Additional information about PAF is available on our website: www.rand.org/paf/

This report documents work originally shared with the DAF on September 10, 2021. The draft reports, issued on September 30, 2021 and March 18, 2022, were reviewed by formal peer reviewers and DAF subject-matter experts.

www.rand.org

RR-A976-3