

Managing Organizational Risk in Nuclear Command, Control, and Communications (NC3) Modernization

By
Nathan A. Heard

Published: October 15, 2026

Digital modernization is shaped by numerous interacting variables, including how and why organizations make decisions, leadership preferences, technical considerations, and individual user behavior. System vulnerabilities can be introduced or worsen because of a single variable or a combination of factors. How organizations [manage](#) processes, systems, risks, and people play an integral role in preventing, identifying, and mitigating vulnerabilities. Understanding the relationship between organizational risk and technical complexity is essential as the US modernizes its nuclear, command, control, and communications (NC3) architecture. Networked and software-dependent components are vulnerable to cyber exploitation by adversaries. NC3 modernization represents a complex multi-layered cybersecurity challenge. As information security researcher Bruce Schneier [noted](#) in 1999, “complexity is the worst enemy of cybersecurity.” Moreover, no system can be completely “cyber secure.”

Organizational decision-making and leadership preferences play an integral role in how information technology solutions are implemented, from procurement to cybersecurity and everywhere in between. Modernizing the nuclear triad and the NC3 infrastructure relies on a small number of [defense contractors](#) to develop and deliver key technologies. Moving from an analog to a digital environment means third-party software will play an increasingly influential role in NC3 operations. Cybersecurity and risk management researcher Daniel Geer [warned](#) that organizations can become trapped by what he calls the “software monoculture,” meaning organizations assume significant risk when they depend on a narrow set of providers or a single provider for critical systems. Security flaws that originate in one part of an organization could spread to others using the same software, potentially cascading into widespread disruption and prolonged system downtime. Private companies, including defense contractors, could also be exploited first, providing a pathway for threat actors to attack government systems.

Several variables influence decision-making inside military organizations that can introduce system vulnerabilities. Nuclear scholar Scott Sagan [notes](#) that military organizations are rigid, approach issues through a military-centric lens, hold “parochial interests,” and engage in intense internal competition. The [number](#) of military services involved in NC3 modernization has produced disparate program management efforts and disjointed business requirements, which can introduce system vulnerabilities. Risk aversion “within the NC3 community” is another complicating [factor](#), keeping some stakeholders entrenched in legacy systems they perceive to be more secure. Rather than confront modernization risks directly, leaders may make design trade-offs that jeopardize the security of NC3 upgrades and the development of future technologies. Furthermore, leaders with an inadequate understanding of organizational management, cybersecurity, and the cyber-nuclear nexus will undermine trust and contribute to poor decision-making across the enterprise.

The nuclear triad and supporting NC3 infrastructure involve human processes and technical systems working together to manage the inherent complexity. Organizational sociologist Charles Perrow [argued](#) that large organizations, like the military, do not fully understand the solutions they implement to manage complex systems. Perrow identified two structural criteria within complex systems that will eventually lead to accidents: interactive complexity and tight coupling. Interactive complexity involves interrelated systems whose interactions are not fully known. Tightly coupled systems operate under time-dependent requirements and have minimal margin for error. Accident or system exploitation through cyber operations can occur along three [vectors](#): analog-to-digital modernization, ongoing maintenance of legacy analog and digital systems, and the design and implementation of future technologies. Cyber operations could [target](#) tightly coupled processes, potentially precipitating an accident within the NC3 architecture. Offensive operations could disrupt, degrade, or deny critical communication nodes and early warning capabilities. Threat actors may alter or destroy information systems and data used by NC3 stakeholders, including the President. The intersection between normal accidents theory and exploitable system vulnerabilities cannot be understated.

Stakeholders should consider the following options to manage organizational risk effectively. First, create a national center of excellence dedicated to advancing cyber-nuclear scholarship and skills training. Meeting the technical and policy challenges affecting NC3 systems and nuclear deterrence more broadly requires a highly specialized workforce. Cyber capabilities and risks will continue to evolve rapidly as the underlying global security situation becomes increasingly tenuous. Consolidating research and training under a single entity can streamline education delivery and talent acquisition pipelines. The center would be funded and staffed through a partnership among public, private, and military academic institutions, think tanks, and private-sector stakeholders. Second, establish an independent board of civilian experts to oversee US nuclear modernization efforts. A lack of organizational governance threatens the safety, security, and long-term viability of broader efforts to modernize the US nuclear enterprise. Establishing a group of experts independent of Congress and the Department of War (DOW) is essential to ensure accountability and manage organizational impediments. The board would issue reports to Congress and make them available to the public every six months. The board would interface directly with congressional, military, and private-sector stakeholders to remediate issues. It may be worthwhile appointing the authors of the [2023 Strategic Posture Commission](#) report to this board, as they have the expertise to conduct a governance mandate.

Nuclear deterrence is a “zero-failure mission.” Therefore, the systems that enable the US nuclear triad must be resilient to cyber threats. Organizational risk and technical complexity create exploitable system vulnerabilities; coupled with nuclear weapons, this is a dangerous combination. Failing to understand this complexity and address these challenges undermines the credibility of US nuclear deterrence strategy, including extended deterrence commitments. In an era of intensifying Great Power competition against two sophisticated cyber-capable nuclear peers, the United States must remain steadfast in confronting these challenges or risk potentially catastrophic consequences.

Nathan A. Heard is an independent researcher and doctoral student in the Defense and Strategic Studies Program at Missouri State University, focused on deterrence issues and emerging

threats. He holds a master's degree in defense and strategic studies and a graduate certificate in countering weapons of mass destruction from Missouri State. Heard is the author of the graduate thesis "A Novel Deterrence Strategy: Denial Through Space and Cyberspace" (2025) and the article "The Coming Crisis with North Korea" (2026). The views expressed are his own.