Executive Summary

An expansive, complex undertaking to modernize the United States' nuclear bombs and warheads, their delivery systems, and the command, control, and communications infrastructure around them is underway. It is a project that carries the potential for great benefits through an increase in digital systems and automation, as well as the addition of machine learning tools into the U.S. nuclear triad and the supporting nuclear weapons complex. But it also is one that carries significant risks, including some that are not fully understood. If it does not take the time to protect the new systems integrated with some of the deadliest weapons on earth from cyberattack, the U.S. government will be dangerously outpaced in its ability to deter aggressors.

Given the stakes, why take on new risks at all? The reason to integrate digital technologies into U.S. nuclear weapons systems is clear: this is the first significant upgrade of U.S. nuclear weapons systems in nearly 40 years, and the old systems need replacing. The most efficient way to update the full nuclear triad of bombers, submarines, and ground-based missiles, as well as the bombs, warheads, and command, control, and communications network, is to use today's technology, including digital tools. From digital displays on bomber aircraft to advanced early-warning sensors and machine-learning-enabled nuclear options planning tools, this U.S. nuclear weapons recapitalization, like past modernizations, will be a product of its time.

Once the process is complete, the modernized U.S. nuclear triad will rely on more digital components and will include limited automation. Machine learning applications will provide some essential functions relevant to nuclear decision-making, and analog systems at or beyond their expected end of life will largely be replaced.

In the recent past, the Departments of Defense and Energy have struggled to respond to cybersecurity and supply chain threats to major weapons development programs. In many cases, efforts to address cybersecurity have lagged behind the acquisitions process, creating challenges for protecting against vulnerabilities in new or modified weapons systems. In addition, outside pressures often place a premium on meeting ambitious cost and schedule commitments, sometimes at the expense of performance and reliability, even in the face of evolving cybersecurity risks and challenges presented by new tools such as machine learning. Risks to all digital and machine learning systems are myriad: attacker intrusions, lack of access to critical systems amid a crisis, interference with physical security systems that protect nuclear weapons, and inaccurate data and information, among others. All

these risks, if not addressed, could undermine confidence in a nuclear weapon or related system.

Integrating new technologies with old is a perpetual engineering challenge, but for the U.S. nuclear deterrent, it is one with implications that go far beyond the significant risks posed by cyber threats and digital malfunctions. Effective nuclear deterrence requires confidence that nuclear forces will always be ready if needed but never be used without proper authorization.

If the new digital systems integrated into U.S. nuclear weapons are not protected from escalating cyber threats, or if added automation cannot be trusted, the high confidence U.S. leaders (as well as adversaries) place in nuclear weapons systems will erode, undermining nuclear deterrence and, potentially, strategic stability.

Given the multiple risks associated with today's nuclear modernization program, NTI drew on open-source information, including budget requests, official statements, and press reports, to determine how digital systems and automation are included in the nuclear weapons enterprise modernization and to develop recommendations for military and civilian leaders in the Departments of Defense and Energy, as well as those in oversight roles in the executive branch and Congress.

It is crucial—now, before it becomes an even more difficult task to secure the modern systems, and before they are deployed or operational—that the technical risks posed by new technologies be recognized and mitigated. To ensure that as long as the United States has nuclear weapons, they continue to be safe, secure, and effective, it is important that as U.S. nuclear policies evolve, they take into account the benefits and risks of digital and advanced tools to the modernized nuclear deterrent.

Recommendations

This report provides three recommendations:

1. **Prioritize digital security and reliability alongside cost, schedule, and performance.** In addition to these essential, traditional objectives for developing weapons, program managers must focus on ensuring that digital systems perform as needed, including in the presence of a determined adversary, enabling confidence in the deterrent. Digital systems should meet clearly established security and reliability thresholds before joining the nuclear enterprise.

RECOMMENDATIONS

1. Prioritize **digital security and reliability** alongside cost, schedule, and performance.
2. Establish **tailored test and evaluation controls.**
3. Consider the **implications of digitization for U.S. nuclear policy and posture.**

2. **Establish tailored test and evaluation controls.** Digital systems present new testing and evaluation challenges, and procedures must be in place to confirm that a system is ready for operational use. This is especially critical for high-consequence systems, first and foremost the nuclear deterrent.

3. **Consider the implications of digitization for U.S. nuclear policy and posture.** U.S. nuclear deterrence policies are updated on a regular basis[1] to accommodate the current geopolitical situation and other factors. As modernization proceeds in the coming decades, U.S. nuclear policies, strategy, and force posture must take into account the implications of a digitized deterrent.

About this Report

This report explores the risks and benefits related to the modernization of U.S. nuclear weapons systems and addresses implications for the national security community to consider as the process moves forward. The report is divided into three parts:

- Part 1, drawing only on publicly available information, explores the scale and scope of the digitization and automation of the U.S. nuclear modernization drive.
- Part 2 addresses the need to balance the new technology's risks against its benefits.
- Part 3 offers recommendations for managing the implications of adding digital, automation, or machine learning tools to U.S. nuclear weapons and related systems.

This report does not comment on specific systems or the technical merits or limitations of bringing these new tools into the nuclear weapons complex. It is clear that modernizing nuclear weapons brings new burdens and opportunities related to maintaining the "always/never" commitment to launch only on a president's legal order.[2] Only through ongoing management of trade-offs—including cost, schedule, and cybersecurity concerns, among others—can a modern U.S. nuclear weapons system be safe, secure, and effective in the 21st century.