U.S. Nuclear Weapons Modernization

Security and Policy Implications of Integrating Digital Technology

NTI
BUILDING A SAFER WORLD

ERIN D. DUMBACHER
PAGE O. STOUTLAND, PH.D

NOVEMBER 2020

NTI is a nonprofit, nonpartisan global security organization focused on reducing nuclear and biological threats imperiling humanity.

The views expressed in this publication do not necessarily reflect those of the NTI Board of Directors or institutions with which they are associated.

Contents

Acknowledgments

The authors are grateful to Nuclear Threat Initiative (NTI) Co-Chair and CEO Ernest J. Moniz, President and COO Joan Rohlfing, and Executive Vice President Deborah Rosenblum for their leadership on the important security issues raised in this report, and we thank the Smith Richardson Foundation for its support of this analysis.

We acknowledge the important guidance we received from members of NTI's Scientific and Technical Advisory Group; members Jill Hruby and James Gosler also served as special consultants on the project, providing indispensable expertise and counsel throughout. At NTI, we thank experts Lynn Rusten, Mark Melamed, and James McKeon for their input on nuclear policy matters. Research and communications support from NTI interns David Bernstein and Melissa Robbins was fundamental to and animated our findings.

We also thank members of NTI's communications team—Carmen MacDougall, Mimi Hall, and Deepika Choudhary, as well as Hillary Coggeshall—for their support in developing this report. We thank Catherine Crary for her diligent work, and we appreciate support from NTI's development team.

In the spring and summer of 2020, a number of U.S. nuclear, defense, and cyber policy expert interviewees participated in our research and offered important insights. We are grateful for their involvement, which was crucial to the success of this project, and reinforce that they are not responsible for, nor do they necessarily endorse, these recommendations.

Finally, the authors acknowledge the essential support of their partners and childcare providers, without whom this work would not have been possible.

Erin D. Dumbacher
Senior Program Officer, Scientific and Technical Affairs, NTI

Page O. Stoutland, Ph.D.
Vice President, Scientific and Technical Affairs, NTI

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.

Policy Context for U.S. Nuclear Modernization

Since developing nuclear weapons in the 1940s, the United States has twice upgraded its nuclear capabilities, first in the 1960s and then in the 1980s, at the height of the Cold War. Many of the weapons and related systems put into service in the 1980s are still in service.

U.S. nuclear deterrence policy seeks to prevent a nuclear attack on the United States or its allies by ensuring that an adversary could not confidently destroy all U.S. nuclear weapons in a first strike, and would therefore be subject to retaliation. This policy is enabled by a diverse nuclear force consisting of land-, air-, and sea-based delivery platforms. Submarines and the nuclear ballistic missiles they carry are recognized as the most survivable leg of the triad, unlikely to be destroyed in a first-strike attack. Ground-based intercontinental ballistic missiles (ICBMs) are the most responsive leg of the triad—able to be launched within minutes—but also the most vulnerable to a first strike.[3]

The U.S. nuclear deterrent is in the process of a recapitalization effort that would take the strategic force from an era of floppy disks to networked systems.

Finally, nuclear-capable bombers are visible and flexible, enabling their use as signals to allies and adversaries.

The U.S. nuclear deterrent is in the process of a recapitalization effort that would take the strategic force from an era of floppy disks to networked systems.[4] Modernization of delivery vehicles will include the following upgrades or replacements:

- The current sea-based leg of the nuclear triad entered service between 1984 and 1997 and consists of 14 Ohio-class submarines carrying Trident D5 ballistic missiles.[5] At least 12 new Columbia-class submarines are expected to enter into service beginning in 2031 to replace the Ohio-class submarines.[6]
- The ground-based leg of the nuclear triad, the Minuteman family of ICBMs, has been in service since 1962; the 440 Minuteman III missiles currently in service were first deployed in 1970.[7] The Ground Based Strategic Deterrent (GBSD) is expected to replace the Minuteman missiles beginning in 2028 with a deployed force of 400.[8]
- Nuclear-capable bombers have been in operation for over 50 years: the B-52H Stratofortress was first deployed in the 1960s, and the B-2A Spirit was deployed in 1994.[9] The B-21 Raider is expected to replace those bombers; at least 100 new B-21s are slated to enter service beginning in the late 2020s.[10]
- Additional modernization programs include a replacement for the air-launched cruise missile (the long-range standoff weapon, slated for production of roughly 1,000 missiles beginning

in 2026), the dual-capable F-35A Joint Strike Fighter, and a guided tail kit for the B61 nuclear bomb to increase the weapon's accuracy.[11]

The communications systems within new or refurbished delivery vehicles are slated to be upgraded, along with the nuclear command, control, and communications systems.

The National Nuclear Security Administration (NNSA) within the U.S. Department of Energy is refurbishing aging nuclear bombs and warheads: the B61 first entered service in 1968 and the W78 and W80 warheads were first deployed in 1979 and 1981, respectively.[12] Table 1 outlines current U.S. nuclear forces and the modernizations planned.

A complex system of command, control, communications, and early-warning technologies permits operators to communicate with commanding officers and detect and manage alerts of incoming attacks.[13] The systems include four airborne command centers built in the 1980s, communications satellites of varying vintage in orbit, ground-based sensors to gather and process incoming satellite data, and an Advanced Extremely High Frequency satellite communications system that permits the National Security Council and the president to communicate with forces "up to and through nuclear war."[14] Plans for modernizing the command, control, and communications, and early-warning system—collectively known as NC3—have yet to be finalized, but many of the existing systems date to 1970s designs and 1980s development.[15] U.S. Strategic Command serves as the "enterprise lead" for the modernization, filling a coordination gap among the military services responsible for the air, space, and ground systems that keep all aspects of the triad connected to one another and to the president.[16]

TABLE 1
Current U.S. Nuclear Forces and Planned Modernizations

	AGING SYSTEM(S)	REPLACEMENT OR RE-FURBISHED SYSTEM(S)
At sea	Ohio-class submarines	Columbia-class submarines
On ground	Minuteman III	Ground Based Strategic Deterrent
In the air	B52 and B2 bombers; Air-launched cruise missile	B21 bombers; Long-Range Standoff cruise missile
Bombs & warheads	B-61, W-76, W-78, W-80	B61 tail kit and refurbishment; warhead life extension programs
Command, control, communications	e.g., Advanced Extremely High Frequency satellites	e.g., Evolved Strategic SATCOM

PART 1

Digital and Advanced Tools in U.S. Nuclear Modernization

An extensive drive to modernize the nuclear weapons enterprise is now underway in the United States. It is a decades-long process that includes refurbishments to bombs and warheads, replacement delivery systems, and a new command and control infrastructure to permit enhanced communication with decision-makers. Whereas these upgrades—the first major nuclear system upgrades undertaken since the 1980s—are intended to ensure a safer, more secure, and more effective deterrent, the modern process of digitizing and automating the nuclear triad and command, control, and communications systems also brings risks.

Nuclear systems long have included some digital and semi-autonomous systems, but the current round of modernization expands the use of digital and automation components into the U.S. nuclear deterrence architecture. Nuclear delivery vehicles, planning systems, and early-warning sensors all will receive new digital and automated tools.[17] As the United States develops, procures, and transitions to new fleets of ballistic missile submarines, strategic bombers, and ICBMs, it is "embarking on the largest, most complex nuclear modernization effort in its history."[18]

Once this effort is completed, the U.S. nuclear triad will rely on digital tools and include limited automation.

Once this effort is completed, the U.S. nuclear triad will rely on digital tools and include limited automation.

Senior Department of Defense officials state that the modernization plans are "sensible … reasonable and affordable" and that the deterrent "must be modernized to remain credible."[19] Without an increase in the size of the nuclear stockpile and with plans to maintain levels of strategic forces compliant with the 2011 New Strategic Arms Reduction Treaty (New START), leaders at the Departments of Defense and Energy aim to modernize in such a way that the effort is a "largely one-for-one replacement of the Cold War-era triad and stockpile."[20] New weapon delivery vehicles such as the Columbia-class ballistic missile submarine, the B-21 strategic bomber, and the GBSD are the centerpieces of this round of U.S. nuclear modernization, yet the broader effort will include upgrades to associated systems. Many of these systems are still in research and development phases and will require extensive testing before they are deployed. Public sources and unclassified interviews with experts reveal that an active, broad, and significant series of software, hardware, and systems engineering development efforts is underway.[21]

A Digital, Partially Automated Triad

With the incorporation of digital components into new systems and in upgrades to existing systems, modernization will result in a different nuclear triad and command and control system from that of the Cold War era. Among a sample of 46 Air Force, Navy, Space Force, and Department of Energy initiatives included in or related to the nuclear modernization drive,[22] 41 are incorporating new or upgraded digital components (Table 2).[23] Notably, almost 9 out of 10 planned nuclear modernization programs involve at least some new digital components or upgrades, and nearly

TABLE 2
Digital and Automation Elements Planned in U.S. Nuclear Modernization

	TOTAL NUCLEAR MODERNIZATION PROGRAMS	DIGITAL COMPONENTS OR UPGRADES	AUTOMATION OR MACHINE LEARNING ADDITIONS
Air Force	25	23 (92%)	4 (16%)
Space Force	6	6 (100%)	2 (33%)
Navy	8	8 (100%)	5 (63%)
Dept. of Energy	7	4 (57%)	0 (0%)
Total	**46**	**41 (89%)**	**11 (24%)**

NOTES: (1) Estimates are based upon publicly available information, primarily budget requests, for fiscal years 2020 and 2021. (2) Many of the nuclear command and control modernization systems are not included as distinct programs in the data reviewed for this study. (3) Given the distinctions between the development processes between DOD and DOE and the practice of sourcing to the national laboratories, the availability of DOE documents is more limited. These factors may affect the quantitative findings.

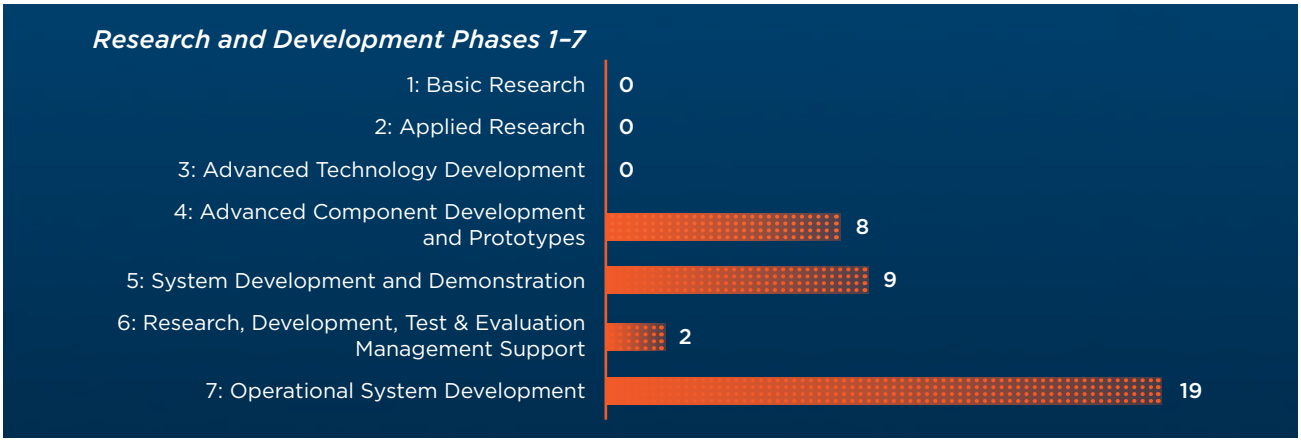
one-quarter involve automated or machine learning systems.[24]

Such refurbishments or upgrades are being introduced to already deployed and operational systems, while other elements of the modernization program are in earlier stages of the acquisition process. Of the 38 Department of Defense programs reviewed still in research and development, the majority are in or nearing operational system development (Figure 1). Department of Defense nuclear modernization programs are in the "Advanced Component Development and Prototypes" phase or beyond, indicating that component technologies are being or have been tested prior to their integration into nuclear weapons systems. This phase will end with the "decision point to enter development of a specific product with an associated budget, suppliers, contract terms, and schedule" and is "generally considered the start of the program of record."[25] The Columbia-class submarine, GBSD ICBM, B-21 bomber, and Long Range Stand Off Weapon all will complete the Advanced Component Development and Prototype phase (Milestone B in the Defense Department acquisitions framework) by the end of 2020 and will undergo operational testing before eventually transitioning to full-rate production.[26] The major modernization initiatives are progressing, but many designs are not yet final.

Of the nuclear modernization programs reviewed for this report—including but not limited to command and control systems—nearly half will be dual-capable (supporting both nuclear and conventional weapons) systems or capabilities.[27] For example, new ground components for early-warning systems will process data from sensors and satellites that were not exclusively designed for detecting nuclear launches.[28] Strategic air-delivery platforms, such as the legacy B-52 and developing B-21 bombers, as well as in-theater dual-capable aircraft, will have the potential to carry both conventional and nuclear payloads.

FIGURE 1

Department of Defense Nuclear Modernization Programs and Progress, n=38



Digital Upgrades to Delivery Vehicles

The strategic bombers, submarines, and intercontinental ballistic and cruise missile fleets will incorporate a host of digital components in the modernization effort. The Air Force plans to add operator-facing and design improvements to the B-52, B-2, and B-1B bombers to upgrade monitors, replace missile warning systems, gain a multi-data-link capability for in-flight retargeting with an automated system to avoid fratricide, and replace navigation and targeting pod functions. These improvements will result in "enhanced targeting capability through weapon hand-off navigational updates for guided nuclear weapons" even when Global Positioning Service data are unavailable as well as a "digital, high-definition video-streaming targeting pod" on new, multifunction display units.[29] The air-launched cruise missile will gain software upgrades and perform analysis to "pro-actively identify components which will degrade system reliability."[30] The replacement system for the Minuteman III ICBMs, the GBSD, will "exploit state-of-the art communications and information transfer techniques" for command and control applications.[31] The Columbia-class submarines will share software with the Virginia-class nuclear-powered attack submarines, but it is not clear which upgrades are planned for the Columbia program. The Virginia-class submarines expect to gain defenses for sonar and combat control programs, a forward compartment with a secret-level local area network, new displays and a fiber optic backbone in the command and control systems, and automated sensors to integrate with the navigation and non-propulsion electronics systems.[32]

Digital Upgrades to the B61-12 Bomb

The B61-12 nuclear bomb is replacing four older variants of the B61 bomb and includes significant digital upgrades. The B61-12 includes a new tail kit assembly that "is designed to be mechanically mated" and connected.[33] Some of the delivery vehicles carrying the B61-12 "will have an analog interface with the B61-12 that is designed to deliver the weapon in a ballistic mode,

with the tail kit in a fixed position," whereas others "will have a digital interface with the B61-12," which will permit use of the new guidance system the tail kit assembly offers.[34] This is the "first-ever digital interface to the B61 family of weapons," according to one of project leaders.[35]

The tail kit has undergone rigorous testing since 2016 and has "demonstrated high degrees of accuracy and reliability in testing to date with no reliability failures."[36] Testing found that "[o]ne system component presents a cybersecurity vulnerability, but mitigation or elimination of the vulnerability appears feasible without a major investment of time or money."[37] Yet the Government Accountability Office (GAO) found that in non-nuclear assemblies there were "problems with an electrical part" incorporated in both the B61-12 and the modified W88 warhead that led to an almost two-year delay and cost increases of up to $700 million for the B61-12 program alone.[38] According to congressional testimony from the NNSA, "[w]hile the problematic components have worked during all system tests," concerns remained that the electrical parts would not function reliably 20 to 30 years from now."[39] This situation demonstrates the potential supply chain risks of relying on commercial off-the-shelf technologies, especially given their quality control in comparison with the rigorous review for all microelectronic systems that are developed at national laboratories.[40] The failure of even minor parts, such as a $5 capacitor, to perform at the same rigorous standard of review or variations in quality from different producers can lead to nearly $1 billion cost overruns. Some experts have criticized the cost of the B61-12.[41]

Department of Energy officials, however, have been explicit that they intend to use lessons learned to improve supply chain management in the future and, ultimately, to reduce spending on nuclear weapons.[42] The B61-12 weapon is expected to be delivered in fiscal year 2022.[43]

Digital Upgrades to Strategic Satellite Systems

Satellite modernization is underway with efforts to upgrade and eventually replace the aging MILSATCOM, Space Based Overhead Persistent Infrared System, and Advanced Extremely High Frequency system as well as the ground systems to receive and analyze data. Satellites and their ground stations will see improved transmission speeds, upgrades to connectivity, better image quality, and wider fields of view. Cryptography upgrades for many systems will enhance their security while user interfaces also will improve, allowing for more complete or custom views of data. Some of these improvements will accelerate the use of algorithms,

SOURCE: United States Air Force

Advanced Extremely High Frequency System

leveraging "large data sets generated by emerging large format focal planes" and will "expand technical intelligence and battlespace awareness processing and data dissemination tools."[44]

Nuclear Command, Control, and Communications: Full-Scale Modernization

It is estimated that the more than 150 existing nuclear command, control, and communications systems (NC3) will need either significant modernization or integration with new assets and delivery vehicles.[45] The Strategic Automated Command and Control System (SACCS), necessary to maintain communication and execute nuclear launch orders in a crisis, was still using floppy disks until late 2019; it now has new hardware and software.[46]

The age of the existing system necessitates replacement, but replacement introduces important cybersecurity questions. The NC3 architecture must maintain uninterrupted communication with all relevant members of the nuclear mission when needed. Legacy systems must be upgraded to connect with new delivery vehicles, sometimes even if the legacy system will be retired before the new delivery vehicles are fully operational. New NC3 systems must reliably connect to both legacy and modernized delivery capabilities.[47]

Modernization efforts also will need to prioritize the resiliency and survivability of all NC3 systems.

The SACCS, first fielded in 1963, permits decision-makers to communicate with nuclear forces and transmits Emergency Action Messages to commanders in the field.[48] The system is currently undergoing a series of upgrades, but it was recently "running on an IBM Series/1 Computer, which is a 1970s computing system," according to the GAO.[49] Recently, the SACCS finally stopped using 1970s-era floppy disks; the system now uses a "highly secure solid state digital storage solution."[50]

For example, the Integrated Broadcast Service, which provides integrated intelligence, surveillance, and reconnaissance information to operators, will become a scalable system to "accommodate growth as the virtual world grows and cyber operations change."[51] The modernized system will increase output to 100 million messages per day, as well as increase the flow, searchability, and storage of information.

The new Joint All Domain Command and Control (JADC2) system will integrate conventional and nuclear information "in an attempt to move data at machine speed and execute joint all domain operations."[52] General Hyten, vice chair of the Joint Chiefs of Staff and former commander of U.S. Strategic Command, has noted that JADC2 and NC3 "are intertwined because, well, NC3 will operate in elements of JADC2."[53] Modernization efforts also will need to prioritize the resiliency and survivability of all NC3 systems, including U.S. space-based NC3 systems, which face growing threats from counterspace weaponry and an increasingly congested orbital environment.[54]

SOURCE: Robert Gauthier/Los Angeles Times via Getty Images

Missile combat crew member at Malmstrom Air Force Base inside the launch control center in 2014

Bringing in Advanced Tools: New Process Automation and Machine Learning Applications

Some automation additions to nuclear systems incorporate conventional process automation approaches; other investments take advantage of the gains machine learning techniques have made in recent years, for example, to analyze early-warning, ballistic missile sensor data rapidly.

In recent budget requests, just over 20 percent of a sample of nuclear modernization programs have included automation or machine learning efforts.[55] Of the surveyed nuclear modernization programs, 11 anticipate incorporating automated components that will process high volumes and sources of data or improve security (see Table 1). Automation or machine learning features will automate backup power switches, streamline acquisition and maintenance efforts, rapidly identify and patch cyber vulnerabilities, advance the speed of planning systems, analyze sensor data for early-warning systems, or improve the targeting accuracy of a gravity bomb. Budget requests cross-referenced with open-source literature reflect decisions and processes from nearly a decade of planning and initiatives to advance the military's use of modern tools, including artificial intelligence (AI).[56]

Targeted applications of automation should be distinguished from lethal autonomous weapons and automation of nuclear launch decisions without human decision-making. Today, nuclear launch decisions in the United States require presidential approval, and this research did not identify any consideration of the U.S. adopting a "Dead Hand," or removing humans from the decision-making loop for launching nuclear weapons.

It is noteworthy that current plans for nuclear modernization do not include systems with the highest degrees of machine control—which are more akin to general AI or autonomy—in which computers make decisions without human intervention. This choice is consistent with the Defense Department's AI ethical principles, which recommend that human beings "exercise appropriate levels of judgment and remain responsible for the development, deployment, use, and outcomes of DoD AI systems," in addition to calling for the department's use of AI systems to be equitable, traceable, reliable, and governable.[57]

It is noteworthy that current plans for nuclear modernization do not include systems with the highest degrees of machine control.

Examples of New Automation or Machine Learning Tools

Automated Power Backups

Automated components are replacing outdated capabilities in legacy systems for targeted purposes. The aging Minuteman III ICBM squadrons, for example, will have an automated switching unit that will replace "software and electronics to measure incoming and standby power characteristics."[58] The current system has become outdated, leading Minuteman III missiles to inadvertently switch between the primary and backup power sources; these incidents "have increased the use and accelerated the wear on" these components.[59] The upgraded automatic switching unit is intended to reduce stress on these critical systems and help maintain reliability should the primary power source be cut. The Defense Department estimates that "all Launch Facilities and Missile Alert Facilities will be impacted by this program at all missile wings."[60] These automated components will process data and perform a single function; failures in these components could stress systems but would not affect launch controls for the missiles.

Acquisition Systems and Problem-Solving

To improve integration of data science across the Navy, the Digital Warfare Office was established in December 2016 and drives "the push to apply AI and machine learning to operations."[61] Projects include an effort to incorporate machine learning to analyze acoustics in the undersea domain, which could allow the United States to accurately locate adversary ballistic missile submarines in crises.[62] Another effort devised a "digital twin" of ship power plants to record all relevant data on power plant performance.[63] Another project enabled the use of sensor data to order necessary F/A-18 Super Hornet parts proactively and predictively for maintenance, reducing repair time by 45 percent and the number of parts ordered per repair by 40 percent.[64] This project parallels efforts to use data analytics and develop algorithms to streamline maintenance operations.[65] Such work demonstrates the targeted role for machine learning and advanced data science and the potential impact on military operations.

The Joint Artificial Intelligence Center (JAIC) "is a focal point of the DoD AI Strategy."[66] The JAIC coordinates predictive maintenance efforts given that "commercially developed AI-based applications have the potential to predict more accurately maintenance needs on equipment." [67] The Air Force has recently increased coordination with the JAIC on condition-based maintenance and enhanced reliability centered maintenance operations.[68] Lt. General John N.T. "Jack" Shanahan (ret.), the first director of the JAIC, called integrating AI into the Department of Defense "a multi-generational problem requiring a multi-generational solution [that] demands the right combination of tactical urgency and strategic patience."[69] Shanahan has stated that AI will not be incorporated into the NC3 architecture: "You will find no stronger proponent of integration of AI capabilities writ large into the Department of Defense…but there is one area where I pause, and it has to do

with nuclear command and control."[70] General Shanahan's comments reaffirm that the United States does not intend to adopt a "Dead Hand" launch system controlled by AI; however, budget requests do include targeted roles for machine learning applications and other automated systems for NC3 systems.

Cyber Defense and Situational Awareness

Cybersecurity upgrades in military systems will incorporate machine learning and automation to rapidly detect and patch cyber vulnerabilities.[71] To address emerging cybersecurity vulnerabilities, unclassified documents propose using automated tools for red-teaming, both to identify vulnerabilities and to teach personnel about the variety of vulnerabilities a cyber system may encounter.[72]

U.S. Navy documents outline automation efforts to enhance the cyber resiliency of NC3 systems. Defensive cyber operations missions will "incorporate Nuclear Command, Control, and Communications Navy (NC3) missions" within environments that allow "for better overall situational awareness and improved speed of response to the most dangerous malicious activity by leveraging the power of machine learning and artificial intelligence to harness existing knowledge more rapidly."[73] Budget documents outline how these efforts will enhance the Navy's nuclear command, control, and communications as well as ballistic missile defense cybersecurity.[74]

Another Navy program, the Continuous Hardening and Monitoring Program "brings together current and historical information from all sources, Navy attack surfaces and network operations" to improve "network and operational system hardening and remediation efforts," according to the former commander of the U.S. Fleet Cyber Command, current Chief of Naval Operations Admiral Michael Gilday.[75]

The program looks at "ways to utilize data analytics, machine learning, and other automation technologies" for enhancing cybersecurity defenses.[76] Rear Admiral Danelle Barrett (ret.), who served as the Navy Cyber Security Division director until November 2019, found that, consistent with many private sector cyber defense practices, "[a]nything that we can do to automate the cybersecurity protection of our network at Internet speed—lightning speed—is what we're interested in."[77]

Nuclear Planning Systems

U.S. Strategic Command operates the Integrated Strategic Planning and Analysis Network (ISPAN) to design comprehensive nuclear attack plans.[78] Automated information system technologies allow ISPAN to develop, process, and display a variety of nuclear targeting plans in regional and global contexts. Public details on the system remain scant, because "[i]t is one of DoD's most complex classified computer systems and the only national force level planning system."[79] Humans seem to remain in the loop, but this semi-automated tool is "right in the decision-making process."[80]

ISPAN is composed of a digital planning system that allows for leaders at the combatant command and strategic levels to jointly coordinate and execute battle plans

and a second system that uses "Machine-to-Machine collaboration" to speed up the joint planning process and to create a comprehensive digital interface displaying all relevant information to execute those plans.[81] The second system also offers "rapid distributed Course of Action (COA) development and global situational awareness supporting both contingency and crisis planners."[82] Initial contract opportunity language called for creation of "an automated 'Courses of Action' suite."[83] However, contracts to automate COAs were never awarded, and efforts have been delayed to January 2021.[84]

The second system within the ISPAN is the Mission Planning and Analysis System (MPAS), "an automated information system to support Global Strike nuclear and conventional target development and weaponeering."[85] Through recent digitization of 1980s technologies, MPAS processes data on strategic effects of various nuclear systems and rapidly outputs an even wider variety of targeting recommendations.[86] The Air Force says these modernization efforts will assist leaders in making informed, decisive, and efficient decisions during crises by displaying the effects of both conventional and nuclear strike options.[87] Meanwhile, the Air Force is rapidly developing ISPAN Increment 5, which will primarily include extensive, ongoing software upgrades to the MPAS nuclear planning system until fiscal year 2024, after which a decision to transition to full deployment must be made.[88]

Early Warning

Next Generation Overhead Persistent Infrared (Next-Gen OPIR) early-warning satellites are rapidly being developed and acquired to replace the legacy Space-Based Infrared System satellite architecture. Next-Gen OPIR satellites will occupy positions in geosynchronous and polar orbits, which will allow them to persistently monitor the earth for signs of ballistic missile launches. The program is fully funded in FY2021 and being rapidly prototyped, with the goal of launching Next-Gen OPIR satellites by 2025 and the complete constellation by 2029.[89]

Automation and machine learning are planned for incorporation into the Future Operationally Resilient Ground Evolution (FORGE) ground system for the program. FORGE "is being designed as an open architecture, meaning it will be able to incorporate data from other sensors" to amplify missile launch detection capabilities.[90] "Essentially, this is a smartphone model," said Dave Wajsgras, president of Raytheon ISS: "We've built an operating system that everyone can build applications for—from Raytheon to the Air Force to universities to small companies. These applications allow the system to process specific types of data."[91]

To handle data analysis, FORGE will use machine learning and algorithm development to rapidly process and transmit early-warning information to relevant parties as well as rely on cloud storage.[92] The Defense Department reports that the automated capability will process data

from a wider variety of sources than legacy systems and allow for more rapid communication across the nuclear mission.[93]

The U.S. Space Force points to the Next-Gen OPIR program as an example of successful rapid acquisition efforts.[94] However, recent GAO reports have "assessed the schedule as highly aggressive and high risk, given concurrent development efforts … and complex integration that includes first-time integration of a new payload and spacecraft, among other significant technical risks." Efforts to upgrade the cybersecurity of the Next-Gen OPIR satellites are limited; program officials report "they plan to generally reuse software from the Space Based Infrared System (SBIRS) GEO programs, ground system, and other programs." It is also possible that the "the future ground system may not be ready when the first GEO satellite is delivered."[95] Despite these warnings, the first two Next-Gen OPIR payloads have passed preliminary design review.[96]

PART 2

Benefits and Risks to Digitizing and Automating

The reason to integrate digital technologies into U.S. nuclear weapons systems is clear: the old systems are outdated or nearing end of life and today's replacements are likely to be digital. Through modernization, the U.S. nuclear weapons systems will benefit from the addition of digital or automated components. At the same time, though, risks abound, and leaders must address them in a timely way. Unfortunately, the cybersecurity and supply chain security practices at the Departments of Defense and Energy lag behind the acquisitions process.

The Need to Modernize

The Barack Obama administration determined that a broad modernization of nuclear weapons systems was necessary to maintain a safe, secure, and effective deterrent. In 2016, then–Secretary of Defense Ashton Carter reasoned that "it's not a choice between replacing these platforms or keeping, it's really a choice between replacing them or losing them."[97] The need to modernize nuclear weapons systems that were last updated in the 1980s is well documented.[98] While upgrades and life extensions have occurred over the years, much of the U.S. nuclear deterrent—including delivery vehicles, command, control, and communications, and the weapons themselves—dates to the 1970s and 1980s. Some elements of U.S. nuclear forces, such as the B-52 bombers, date to the 1950s. From delivery vehicles to command and control networks to early-warning satellites, the platforms, as well as the technologies and systems upon which they rely, are increasingly difficult to reliably maintain.[99]

Although both the Obama and Donald Trump administrations supported modernization of the U.S. nuclear deterrent, the scope of the program is a matter of ongoing debate within the nuclear policy community. Key issues include the expense of the effort, what sorts of upgrades are required, whether the force structure should be modified, and the international security implications of U.S. nuclear force policy and posture. The ramifications of incorporating new digital systems during the modernization process remain on the periphery of analysis and debate.

Track Record for Weapons System Cyber and Supply Chain Security Is Wanting

Experts have documented the need for incorporating the best cybersecurity practices into weapons development; this report will not enumerate the full scope and series of risks, nor the relative difficulty of mitigating and managing them across the defense industrial base.[100] It is important to note, however, that the absence of consistent, well-implemented cybersecurity measures across all weapons system research and development creates acute challenges for the U.S. nuclear mission. Historically, cybersecurity has been an add-on or an afterthought in major defense weapons system design. Program management incentives have not been structured to encourage managers to prioritize the need for mitigating cybersecurity vulnerabilities over time.

The GAO has raised alarm regarding the Defense Department's lack of focus on

combating cyber threats to critical systems. A 2018 GAO report found that the department's weapons systems are increasingly networked and more software reliant than in years past, creating an expansive attack surface.[101] Operations testing revealed mission-critical cyber vulnerabilities even while Defense Department program officers understood the systems to be secure. The GAO declared that the department is "just beginning to grapple with the scale" of the vulnerabilities to critical weapons systems.[102] Similar challenges appear at the Department of Energy/NNSA in securing the supply chain of critical components.[103]

Until recently, there was no lead organization within the Department of Defense responsible for defending the defense industrial base against cyber threats; defense contractors and other firms were trusted to manage their own cybersecurity risks. The result was compromised systems and military readiness at risk.[104] A 2018 MITRE study recommends that "[a]ccountability for integrity and mission readiness [...] be blended across the acquisition, operations, and sustainment communities, with a clear chain of command directly to the Secretary of Defense."[105] Accountability for ensuring that department-wide cybersecurity procedures apply to nuclear modernization programs or surfacing and managing AI safety issues is unclear. The cross-cutting cybersecurity policies meant to defend military assets and systems against cyber or supply chain attacks at the Defense Department are still immature, presenting the possibility that the nuclear weapons modernization could outpace the policy frameworks.

Cybersecurity Initiatives Lag Modernization's Acquisitions Progress

Although the Defense Department has taken actions including revising cybersecurity policies and guidance and has been directed by Congress to address cyber vulnerabilities, these actions are late, according to the GAO.[106] The Air Force has requested nearly $70 million for cyber resiliency of weapon system programs in FY2021, a roughly 80 percent increase from the prior year, with funding for the Cyber Resiliency Office for Weapon Systems, which trains acquisitions workers and provides system security engineering.[107] Additional information system security and information technology development programs work toward protection and defense against cyber risks.[108] The Navy has recently completed congressionally mandated "cyber vulnerability assessments of major Navy weapons systems and cyber vulnerability assessments of critical shore infrastructure."[109] Roughly $42 million went toward vulnerability assessments in fiscal year 2019. Then the secretary of the Navy published the sobering *Cybersecurity Readiness Review* summarizing various cybersecurity risk analyses and recognizing the extensive cultural and institutional challenges to enhancing cyber resiliency in the Navy, particularly as there are "no uniform or effective cybersecurity metrics to quantify the threat, influence resourcing, or operational planning."[110] The Navy is taking numerous steps, both technical and organizational, to mitigate cyber vulnerabilities but acknowledges its efforts' limitations.[111]

There now is a set of policies and guidelines for managing cybersecurity risk in place for major Defense Department weapons development programs.[112] These relatively new structures include delineation of task ownership as well as checklists to be used before granting authorization to connect a digital tool to other weapons platforms or systems. There also are necessary, cross-department initiatives to speed up software development and reform acquisitions processes to accommodate the realities of digital technologies.[113] Experts interviewed by NTI describe the various efforts underway as "necessary, but not sufficient" in the face of cyber threats to high-consequence systems.[114]

The initiatives underway are important and could aid the nuclear mission and modernization efforts, but the GAO has noted that in the race to develop and deploy digital technologies (both software and hardware) for prior, conventional military missions, key information, planning, and decision-making steps were omitted, and the initiatives are not models for high-consequence strategic technology and system developments.[115] Cybersecurity and software development practices remain inconsistent, and critical assessments delay progress.[116]

The approach of chasing and reacting to vulnerabilities has an impact on overall program cost and schedule, and raises concerns about the system's performance over time.

Vulnerability management is a central concern across weapons system development but is not sufficient to confirm that critical systems and their components are free from compromise throughout the development and operations life cycle.[117] Existing approaches to securing weapons systems amount to a set of "whack-a-mole" efforts—as each vulnerability is revealed, it is patched, and so on.[118] The approach of chasing and reacting to vulnerabilities has an impact on overall program cost and schedule, and raises concerns about the system's performance over time.

The retention of a highly skilled and sought-after cybersecurity workforce also is affected by delayed or deficient cybersecurity practices. A 2019 RAND Corporation study cited concerns that "the Air Force simply is not structured in a way that allows for the flexibility that is ideal for cutting-edge cyber operations, or for being proactive (as opposed to reactive) in cyber support and maintenance."[119]

Some experts have called management of digital risks the "fourth pillar" of Defense Department acquisitions, and initiatives are underway to improve the defense acquisitions workforces' understanding of cybersecurity.[120] In early 2020, the Defense Department announced the Cybersecurity Maturity Model Certification Initiative to encourage basic cyber hygiene throughout the department's industrial base. The department's risk-management framework, based on National Institute of Standards and Technology recommendations, is in place, and work has focused on new training and integrating of cybersecurity concerns early in the process.[121]

In just one recent example that demonstrates the severity of the risk, the Defense Department's inspector general found that insufficient and inconsistent security

practices have made ballistic missile defense installations vulnerable to physical and cyber threats, jeopardizing classified technical information.[122] The GAO also continues to find lackluster cyber hygiene practices at the department.[123] As of June 2020, cybersecurity of major defense acquisitions still suffered from "inconsistent software development and practices."[124]

Accountability and Oversight Challenges of a Digital Modernization

Lack of accountability for meeting key milestones is an ongoing challenge for major weapons development programs. Structural issues, including the number of personnel involved in decisions with distinct motivations or incentives—who can slow or stymie programs (but not cancel them)—have come to light as initiatives to accelerate software development have met resistance, according to the Defense Innovation Board: "These oversight actors often have overlapping or unclear roles and authorities, as well as competing interests and incentives."[125] In the drive to bring innovation to the nuclear weapons complex, accountability concerns are similar.

NTI interviewees questioned the level within the departments at which the strategic choices and trade-offs are being made in the modernization effort. Some noted that the Office of the Secretary of Defense and entities such as the Nuclear Weapons Council have recently provided more limited strategic guidance than in previous administrations.[126] Former Secretary of Defense James Mattis assigned U.S. Strategic Command responsibility—the enterprise lead—for nuclear command and control modernization, but a number of Defense Department civilian leaders, as well as the Air Force and Navy, remain responsible for the acquisition and sustainment of NC3 assets.[127]

For delivery systems, individual program managers are responsible and report through the Office of the Undersecretary of Defense for Acquisitions and Sustainment. For warhead and bomb modernization, the Office of Defense Programs at the Energy Department's NNSA is responsible. The Nuclear Weapons Council, with representatives from both Defense and Energy, "is the focal point for interagency activities to sustain and modernize the U.S. nuclear deterrent [and] endorses military requirements, approves trade-offs, and ensures alignment between DoD delivery systems and National Nuclear Security Administration (NNSA) weapons," according to *The Nuclear Matters Handbook 2020*.[128]

Requirements for cybersecurity practices lagged behind some weapons system development, and today, assessments are not yet a permanent, institutionalized part of the acquisitions process.[129] At least four of the 46 nuclear modernization programs reviewed in this study do not describe explicit, unique cybersecurity protocols in public documents; instead, they rely on department-wide cybersecurity resources for weapons systems. The National Institute of Standards and Technology, in its update to the Department of Defense Risk Management Framework, advises that test and evaluation processes for information system security occur prior to awarding development contracts.[130]

Program management offices (PMOs) often have experience and training in warfighting, readiness, and hardware development rather than software and cybersecurity. They face difficult problems that require risk-based calculations with imperfect, evolving information.[131] A recent study on management challenges for nuclear modernization in the Air Force raised the prospect that leaders send signals to decision-makers and program managers that certain requests, such as those for more resources or workforce expertise, are off limits. Managers' fears of being "laughed out of the room" could hold back constructive feedback in the Air Force's nuclear modernization work, according to a RAND report.[132]

Congress has an important oversight role to play, with help from the expertise of the GAO, the Congressional Budget Office, and the Congressional Research Service, among others. The GAO's program evaluation already warns of cybersecurity risks to nuclear development programs. The 2020 bipartisan Cyberspace Solarium Commission report, as one example, outlined necessary cybersecurity actions for the nuclear command and control system.[133] The Senate version of the fiscal year 2021 National Defense Authorization Act, passed in June 2020, includes recommendations from the commission directing the secretary of defense to ensure "cyber resiliency of nuclear command and control system." [134] (The NDAA for FY 2021 has yet to become law.) Congressional oversight of the design and development of the new and replacement systems is expanding. In addition, interviewees described internal controls from the Office of the Secretary of Defense as limited.

Although the benefits of successfully integrating automation and AI technologies into military and nuclear systems are many, there also are certain risks that must be considered.

Machine Learning Applications Add Complexity to Nuclear Modernization

Ambitions are high for including some applications of AI into nuclear systems. Some experts posit that AI can reduce the risks of nuclear war by creating early-warning systems that are more reliable than ever before, leading to a reduced likelihood of accident or malfunction, and therefore a decreased chance of escalation during a crisis. Machine learning algorithms could make situational predictions to help leaders and military commanders with decision-making.[135] Machine learning also could defend against cyberattacks on critical systems; U.S. Cyber Command is currently strengthening defensive cyber capabilities and developing "intelligent information systems for analyzing cyberintrusion based on cloud computing, big-data analysis, and other technologies."[136]

Although the benefits of successfully integrating automation and AI technologies into military and nuclear systems are many, there also are certain risks that must be considered. Machine learning, a form of AI, is still a "fragile" technology, sometimes performing in unexpected ways outside of a narrow set of conditions. Furthermore,

incorporating machine learning technologies into weapons systems leaves them potentially vulnerable to so-called adversarial attacks.

Machine learning tools "learn" by being exposed to data. Once "trained," the algorithms can predict future results on the basis of the data provided. Examples can be as simple as linear regression techniques, in which a linear relationship is assumed between a variable *x* and result *y*. More complex applications, such as image classification (e.g., identifying that a photo of a cat is indeed a cat), require more complex algorithms, such as the use of neural networks.

The applications of machine learning have dramatically expanded in recent years as a result of increased computing power and, most importantly, greatly enhanced availability of data that can be used to train the system. While of great utility for many applications, machine learning techniques suffers from a number of shortcomings that are especially of importance for high-consequence applications (e.g., self-driving cars, autonomous weapons).

For example, small perturbations in the data can lead to misclassification and/or unexpected results. Furthermore, systems developed in one environment may not be reliable in another. Algorithms can also be fooled by sophisticated adversaries who purposely input data designed to cause the machine learning-based system to make a mistake. Finally, the features of the data (e.g., of an image) that are most heavily represented in the algorithm are not always well known or intuitive. As a result, it's sometimes not clear how a machine learning system makes its decisions—particularly important for high-consequence applications.

According to the National Security Commission on Artificial Intelligence, as of 2020 the Defense Department must still "strengthen AI Test and Evaluation, Verification and Validation capabilities by developing an AI testing framework, creating tools to stand up new AI testbeds, and using partnered laboratories to test market and market-ready AI solutions."[137] Among other initiatives, the JAIC is currently working to develop a cloud-based tool providing "the development, test, and runtime environment and the collaboration, tools, reusable assets, and data that military services need to build, refine, test, and field AI applications."[138] As Richard Danzig has written, the necessary consideration for the U.S. national security community is "to be maximally thoughtful and creative about new technologies at the time of their design and deployment."[139]

It's sometimes not clear how a machine learning system makes its decisions—particularly important for high-consequence applications.

The risks of integrating AI tools into weapons systems are amplified when applied to nuclear weapons systems and missions.[140] Whereas AI in decision-support functions could make early-warning data more reliable in general, a false alarm,

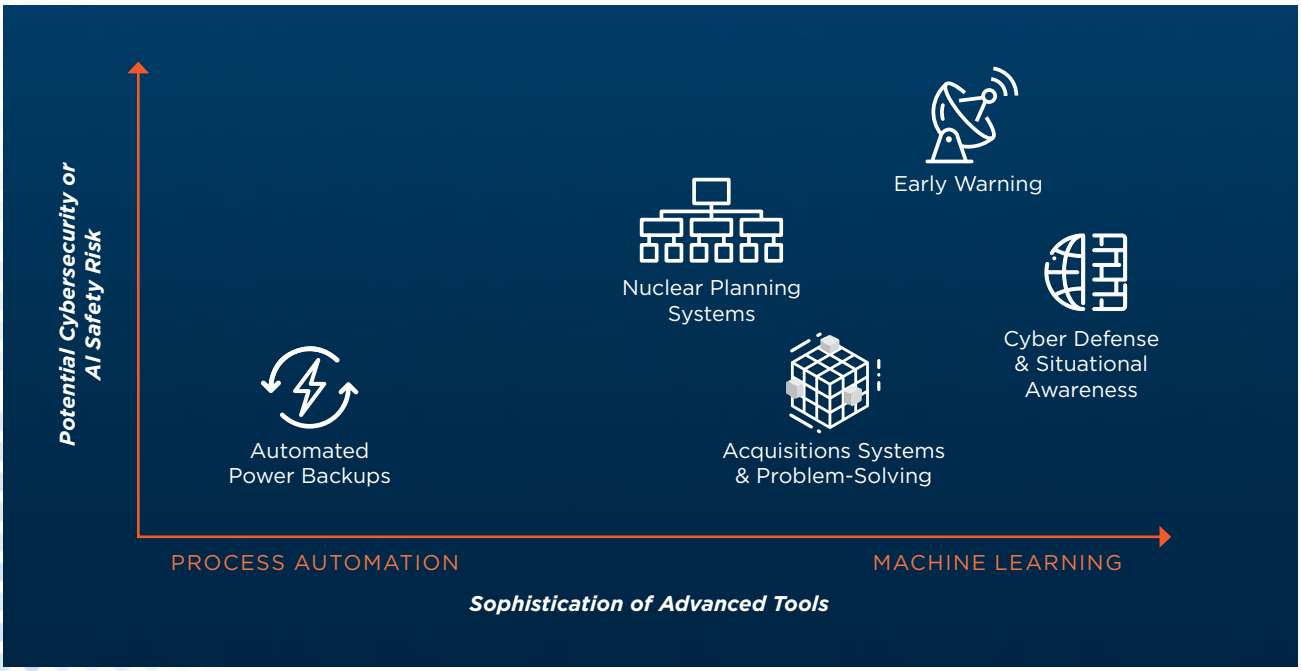
coupled with an inability to understand why it occurred, could be catastrophic.

As outlined in Part 1, roughly one-fifth of programs reviewed are likely to gain advanced automation or machine learning tools. Many are relatively traditional and low-risk automation upgrades; others take advantage of the growing capabilities machine learning techniques offer. In one case, the Minuteman III is gaining an automated switching tool to turn on backup power—a relatively low-risk, straightforward function. Machine learning can be used to rapidly characterize images, and applying this technology to early-warning sensor data analysis to remove the partially manual analysis processes can yield effectiveness gains. For example, the Next-Gen OPIR satellite constellation will communicate with the forthcoming FORGE system to analyze its input data. FORGE is expected to use machine learning algorithms to rapidly process early-warning information. Proponents link FORGE with increasing decision time for the president in case of an attack, a potential risk-reduction measure.

Simple risk calculations are difficult to apply to nuclear weapons concerns where other factors must be considered, such as the geopolitical implications of an accident or the likelihood that an adversary could compromise a nuclear weapon system. The current and potential future risks of incorporating digital and emerging technologies into the U.S. nuclear deterrent are hard to quantify, but clearly some applications are higher risk than others. As shown in figure 2, automated power backups are likely to be relatively low risk, whereas the inclusion

FIGURE 2

Risks Associated With Automation and Machine Learning Upgrades to U.S. Nuclear Weapons Systems, Illustration



of more advanced machine learning tools in early-warning and cyber defense systems could introduce additional risks.

In considering inclusion of a new digital system, program managers and leaders must weigh a number of factors. For example: Do the functional gains from a new tool—being able to ingest information more rapidly and from a wider variety of sources, as the early-warning ground system FORGE intends, for example—outweigh the risks of adding machine learning tools to an important function? How can these risks be mitigated or managed? At what point are additional layers of support, governance, and review required?

Additional Challenges: Balancing Integration with Entanglement

A key advantage of digital and information technologies in national security is the interoperability and integration opportunities digital tools offer: bringing together data streams to provide decision-makers and operators with additional context, improved situational awareness, or streamlined information flows, all of which can improve outcomes. At the same time, the transition to digital tools within NC3 and nuclear delivery platforms can accelerate "entanglement" risks, in which an attack on conventional capabilities could be interpreted as an attack on a nuclear system. The addition of digital tools in the nuclear enterprise is not the only factor prompting additional integration of conventional and nuclear command and control; initiatives that modernize or replace antiquated NC3 systems facilitate integration and potential entanglement.

Plans to develop the JADC2 and other integration have stoked fears about the entanglement of nuclear and conventional command and control systems. Because U.S., Chinese, and Russian NC3 assets all serve both conventional and nuclear missions, the targeting of any of them in a conventional conflict could be interpreted as an attack on a nuclear system.[141] The plans come amid advocacy for broader joint operational concepts for deterring and defeating aggression.[142]

Technical necessity and efforts to reduce costs are likely to drive more military systems to be dual use, improving situational awareness but also potentially complicating crisis management and increasing pathways to nuclear escalation.[143] Outside of the nuclear mission, there is growing interest in a "hybrid commercial-military network" that would allow the Defense Department to use commercial satellite services. The U.S. Strategic Command has sought to use non-military, commercial systems, yet it warns of the current and forthcoming difficulties of "certifying those systems as fail-proof."[144] Practical limitations, such as legacy satellite communications terminals across the military that are incompatible with commercial data feeds, may slow use of commercial networks.[145] Military and commercial integration on satellite payloads, however, could increase the resiliency of U.S. space assets and decrease the likelihood that even a dedicated counter-space mission could destroy U.S. early-warning capabilities.[146]

Nuclear-weapons states sometimes have made the deliberate choice to field dual-capable systems for strategic as well as efficiency purposes—the obfuscation between the missions can be intentional and serve as a feature as well as a risk of a military posture. Some degree of nuclear and conventional entanglement may prove inevitable for cost and efficiency reasons, but the implications of dual-use systems require careful, intentional consideration.[147]

RECOMMENDATIONS

Confidence through Managing Trade-offs

The implications of balancing the benefits with the risks of modernization are clear—effective nuclear deterrence requires confidence that nuclear forces always be ready if needed but never be used if not properly authorized. By taking advantage of the benefits provided by modern technologies, while ensuring that the risks are managed, the United States will be able to increase confidence that nuclear forces are ready while reducing the risk of miscalculation and accidental or unauthorized use.

The following three recommendations outline ways that leaders in the Office of the Secretary of Defense and at the NNSA, military commanders, contractors, national laboratory scientists and engineers, and those in oversight roles can more effectively weigh the risks and benefits of incorporating digital technologies into U.S. nuclear modernization programs consistent with the policy that for as long as nuclear weapons exist, the U.S. nuclear deterrent will be safe, secure, and effective.

RECOMMENDATION 1

Prioritize Digital Security and Reliability alongside Cost, Schedule, and Performance

Leaders and managers in the Departments of Defense and Energy as well as congressional overseers should prioritize digital security and reliability in addition to the conventional cost, schedule, and performance objectives for nuclear modernization efforts. Digital systems should meet clearly established security and reliability thresholds before joining the nuclear enterprise.

Schedule or performance requirements may nonetheless need to shift in favor of digital security and reliability.

Balancing the budgets, schedules, quality, security, and reliability of nuclear modernization programs can be challenging, especially given that some systems already have exceeded their life expectancy, and delaying target dates for a replacement system may not be a realistic option. In such cases, sufficient resources should be allocated to ensure confidence in the new systems. In other cases, schedule or performance requirements may nonetheless need to shift in favor of digital security and reliability.

The administration and Congress should agree on minimum thresholds for security and reliability of systems slated to join the U.S. nuclear weapons system. The standards should accommodate risks that include, but are not limited to:

- intrusion, including exploitation of vulnerabilities;
- accessibility issues amid a range of peacetime and crisis conditions, including jamming and denial of service;
- information corruption, spoofing, or poisoning;
- explainability, especially of the embedded logic of automated or machine learning applications; and
- system engineering or programmatic problems as a result of integrating new tools into the existing or the broader U.S. nuclear weapons enterprise.

Within the already complex defense acquisitions process with its milestone checkpoints, the undersecretaries of

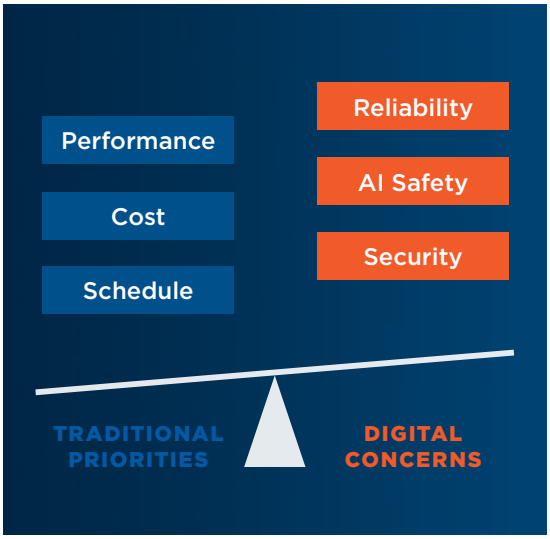
Defense for Research and Engineering and for Acquisition and Sustainment should require that digital security and reliability metrics be met at all acquisitions process milestones. Before a system becomes operational, third-party, independent tests should confirm that essential security and reliability thresholds are met. Ongoing testing will be needed to maintain confidence that the digital systems connected to the world's most catastrophic weapons are reliable and secure.

Oversight and programmatic efforts should, whenever possible, emphasize the importance of digital reliability early and throughout the program's development lifecycle.[148] The risks are "worthy of a high degree of oversight" and "attention in the design process," according to a former senior defense official.[149] For some aspects of the modernization effort, requirements already are in place and decisions made now will reduce the flexibility for addressing significant digital reliability concerns later. The Defense Science Board has recommended an assessment to evaluate the confidence in "the mission assurance of the nuclear deterrent against a top tier cyber threat."[150] High levels of cybersecurity should be confirmed when a system is operational, not only during research and development. Leaders must evaluate the full spectrum of risks on a continual basis—cybersecurity is not purely an operational concern nor a vulnerability-patching task.

Ongoing testing will be needed to maintain confidence that the digital systems connected to the world's most catastrophic weapons are reliable and secure.

FIGURE 6

Balancing Traditional Priorities and Digital Concerns, Illustrative



RECOMMENDATION 2

Establish Tailored Test and Evaluation Controls

Building on the established milestone approval and technology readiness assessments of major defense acquisitions, tailored test and evaluation and controls should be established to confirm digital systems' readiness for use in U.S. nuclear weapons systems.[151] Existing directives and practices for testing and evaluation and verification and validation are insufficient for reviewing digital systems to be integrated into nuclear weapons systems.

Although sound development principles can minimize the potential vulnerabilities to cyberattacks and automation can help, designing completely secure software and hardware is a significant challenge.[152] Similarly, fundamental challenges remain to adequately testing machine learning tools' performance amid diverse and dynamic

conditions.[153] In addition, training data must be representative of actual conditions, and the consequences of such errors, which range from the trivial to the catastrophic, must be considered. In the case of early-warning or other applications relevant to nuclear decision-making, just as in other machine learning applications, there is a potential for bias or other dataset limitations that could lead to poor outcomes.

The history of using machine learning applications in the private sector "suggests that it's very hard to think of all of [the potential errors] in advance," according to an analysis by the JASON science advisory group.[154] Department of Defense directives outline developmental and operational testing and evaluation/validation and verification steps for autonomous and semi-autonomous systems,[155] but the JASON report cautions that the Department's testing of AI systems "needs to go beyond checking that requirements are satisfied … to probe outside the boundary of expected behavior to try to uncover unexpected weaknesses."[156]

Given the implications of a digital system failure or compromise within nuclear or related systems, an additional layer of testing, evaluation, verification, and validation tailored to the unique properties of digital systems is necessary for the nuclear enterprise.[157] If the high requirements for inclusion in the nuclear enterprise are unmet, an alternative approach must be seriously considered.

If the high requirements for inclusion in the nuclear enterprise are unmet, an alternative approach must be seriously considered.

RECOMMENDATION 3

Consider the Implications of Digitization for U.S. Nuclear Policy and Posture

Nuclear policies cannot be stagnant amid a modernization program that brings significant changes to the U.S. nuclear deterrent. The U.S. nuclear modernization effort must address cyber threats and issues of AI safety, even if it complicates the already challenging task of rebuilding the nuclear triad and command and control systems. The U.S. nuclear policy community must continually consider the implications for U.S. nuclear strategy, policy, and posture of introducing digitization and partial automation into the U.S. nuclear deterrent.

For decades, nuclear weapons operations have led governments "to strike a balance between competing purposes" including "significant choices … on matters of strategic doctrine, organizational procedure, weapons engineering, communications design, financial allocation, personnel training, the disposition of authority, and the formation of political commitments."[158] The warheads, bombs, and delivery vehicles, and the accompanying command, control, and communications systems around them have always had inherent limitations and capabilities that informed policy options. Although technology should not determine policy, policymakers need to recognize the implications of technological change. Specifically, the implications of a digital and partially automated U.S. nuclear weapons system must be considered and understood to ensure that deterrence, and confidence in it, is not weakened.

To prepare for and mitigate the new risks digital and advanced tools can bring to U.S. nuclear weapons and systems, leaders, engineers, and operators should consider how to shift operations and policies to improve and prioritize the safety, security, and effectiveness of U.S. nuclear forces and systems. For example: If early-warning sensor analysis applies machine learning tools and digital interpretations of raw radar data, at what point in the analysis or alert process could or should a human verify the information?[159] If additional information sources are available for decision-makers, how will this information be presented and managed in a crisis? As modernization advances, changes to nuclear operations may be required to maintain confidence in the weapons systems.

In addition to updating nuclear operations to fit the new technologies, consideration should be given to whether new technologies call for a change in policies. For instance, some NTI interviewees brought up policy and force posture changes such as eliminating "hair-trigger" alert postures or eliminating the ICBM leg of the triad entirely. Others argued that the ICBM leg may be less sensitive to cybersecurity risks than the bomber or submarine legs and therefore is an important hedge against threats to command and control systems.

Anticipating the future implications of technological change is difficult given the expected life span of the modernized nuclear forces, which could extend to the 2080s. Nor are these challenges unique to the United States; they will be faced to some degree by other states with nuclear weapons that are or will in the future be modernizing their systems and adding digital components. Questions the United States (and potentially other states with nuclear weapons) should be considering include:

The implications of a digital and partially automated U.S. nuclear weapons system must be considered and understood to ensure that deterrence, and confidence in it, is not weakened.

- How do cyber threats to nuclear weapons systems affect strategic stability, and what can be done to mitigate them?[160]
- Are new declaratory policies, transparency, or confidence-building measures needed in light of greater digitization and integration of conventional and nuclear systems to mitigate the risks to strategic stability that could arise?
- Should concerns about current or future cyber and/or AI safety risks to nuclear early-warning or other systems lead to consideration of changes to nuclear postures to mitigate some of the risks?
- How might digital systems affect future policy options (e.g., the use of self-destruct mechanisms)?
- Will digital upgrades enable greater accuracy of delivery systems and warheads and therefore have implications for future nuclear force requirements?
- What are the operational and planning implications, if any, of greater digitization and automation for extended deterrence and U.S. allied commitments?

Considering these questions and more is vital to maintaining a safe, secure, and effective nuclear deterrent and to maintaining strategic stability with other nuclear weapons states. The introduction of modern technologies into the nuclear modernization effort creates both opportunities and risks with critical, if not yet fully understood, implications for U.S. national and international security.

About the Authors

Erin D. Dumbacher is a senior program officer for scientific and technical affairs at the Nuclear Threat Initiative, focusing on emerging technology and nuclear security.

Prior to joining NTI, Dumbacher was a director at CEB (now Gartner), a research and advisory firm, where she led management, operations, and technology transition research. She previously held research and strategy positions at Atlantic Media. Dumbacher has also worked on the Cyber and National Security team at the U.S. Office of Management and Budget and in the office of U.S. Congressman Cramer of Alabama's 5th District.

Dumbacher holds a master's degree in conflict management and international economics from the Johns Hopkins University School of Advanced International Studies (SAIS) and a bachelor's in international affairs from the George Washington University. In 2010, she received a Fulbright Fellowship to study technology and international relations in Estonia.

Page Stoutland, Ph.D, is NTI's vice president for scientific and technical affairs. He joined NTI in 2010 and is responsible for its scientific and technically related projects designed to strengthen nuclear security and reduce risks around the world. Prior to joining NTI, Stoutland spent 10 years at Lawrence Livermore National Laboratory, where he held a number of senior positions.

Earlier in his career, he held positions within the U.S. Department of Energy and at Los Alamos National Laboratory. Stoutland holds a bachelor's degree from St. Olaf College in Northfield, Minnesota, and a doctorate in chemistry from the University of California, Berkeley. After completing his doctorate, he spent two years at Stanford University as a National Institutes of Health postdoctoral fellow.

Appendix

Methodology

Data sources for this project include publicly available literature and in-depth interviews conducted by the authors and NTI staff. This report does not draw on any classified sources.

Top sources include research products from the legislative branch, including the Congressional Research Service, the Congressional Budget Office, and the Government Accountability Office. From the executive branch, NTI reviewed relevant budget documents, program overviews, and public statements. To support the case studies, NTI reviewed requests for proposals, trade studies, and public statements from defense contractors. In particular, NTI derived information on digital and automation upgrades planned as part of the nuclear modernization effort from Air Force, Navy, and Space Force RDT&E (research, development, testing, and evaluation) budget requests and the Department of Energy's National Nuclear Security Administration (NNSA) budget requests.

NTI conducted 17 in-depth interviews with national security, defense, cyber, and nuclear technology experts, by phone or video conference, during the spring and summer of 2020, making clear in each conversation that the project was based solely on unclassified information.

Sample of Nuclear Modernization Programs

NTI derived information on program elements relevant to nuclear modernization programs from Defense Department and NNSA budget requests, including information regarding plans for digital and/or automated systems and any explicit cybersecurity or autonomy protocols governing these systems. It gathered data from the FY20 and FY 2021 budget requests and justifications. NTI recorded budget activity numbers, denoting the progress of a program within the research, development, test and evaluation process for each program element relevant to the nuclear modernization drive, as well as phases in the nuclear weapons life cycles for warheads. The full data set is available from the authors upon request.

Endnotes

1 For example, the Nuclear Posture Review is a mandatory review to clarify U.S. nuclear policy, force posture, and strategy for the next five or ten years. (See authorizing legislation: *National Defense Authorization Act for Fiscal Year 2008*, Public Law 110-181, *U.S. Statutes at Large* 122 (2008), Sec. 1070.)

2 Peter D. Feaver, "Command and Control in Emerging Nuclear Nations." *International Security* 17, no. 3 (Winter 1992–1993): 160-87, accessed July 27, 2020, doi: 10.2307/2539133.

3 Office of the Secretary of Defense, *Nuclear Posture Review Report*, Washington, DC: U.S. Department of Defense, 2018), 45, media.defense.gov/2018/Feb/02/2001872886/-1/-1/1/2018-NUCLEAR-POSTURE-REVIEW-FINAL-REPORT.PDF.

4 Max Kutner, "Reminder: U.S. Nuclear System Runs on Early Computers and 8-Inch Floppy Disks," Newsweek, August 9, 2017, www.newsweek.com/trump-nuclear-bombs-north-korea-floppy-disks-648874.

5 "Fleet Ballistic Missile Submarines-SSBN," U.S. Navy Fact File, January 29, 2019, https://www.navy.mil/Resources/Fact-Files/Display-FactFiles/Article/2169580/fleet-ballistic-missile-submarines-ssbn/; U.S. Library of Congress, Congressional Research Service, *Navy Columbia (SSBN-826) Class Ballistic Missile Submarine Program: Background and Issues for Congress*, by Ronald O'Rourke, R41129, (April 12, 2019), fas.org/sgp/crs/weapons/R41129.pdf.

6 Kingston Reif with Alicia Sanders-Zakre, *U.S. Nuclear Excess: Understanding the Costs, Risks, and Alternatives*, (Arms Control Association, April 2019), www.usnuclearexcess.org/wp-content/uploads/2019/05/Report_NuclearExcess2019_update0410.pdf; U.S. Library of Congress, Congressional Research Service, *Navy Columbia (SSBN-826) Class Ballistic Missile Submarine Program*.

7 "Minuteman III," Missile Threat, Center for Strategic and International Studies Missile Defense Project, September 19, 2016, missilethreat.csis.org/missile/minuteman-iii/.

8 Reif with Sanders-Zakre, *U.S. Nuclear Excess: Understanding the Costs, Risks, and Alternatives*"

9 Hans M. Kristensen and Matt Korda, "United States Nuclear Forces, 2019." *Bulletin of the Atomic Scientists* 75 no. 3 (April 2019), 122–34, thebulletin.org/2019/04/united-states-nuclear-forces-2019/.

10 Reif with Sanders-Zakre, *U.S. Nuclear Excess*.

11 Reif with Sanders-Zakre, *U.S. Nuclear Excess*; "AGM-86 Air-Launched Cruise Missile (ALCM)," Missile Threat, Center for Strategic and International Studies Missile Defense Project, November 29, 2016, missilethreat.csis.org/missile/alcm/; Zachary Keck, "Why the B-61-12 Bomb Is the Most Dangerous Nuclear Weapon in America's Arsenal," *The National Interest*, October 9, 2018, nationalinterest.org/blog/buzz/why-b-61-12-bomb-most-dangerous-nuclear-weapon-americas-arsenal-32976.

12 "B61-12 Life Extension Program," U.S. Department of Energy, National Nuclear Security Administration, www.energy.gov/sites/prod/files/2018/12/f58/B61-12%20LEP%20factsheet.pdf; "The W80 Warhead: Intermediate Yield Strategic Cruise Missile Warhead," the Nuclear Weapon Archive, August 29, 2007, nuclearweaponarchive.org/Usa/Weapons/W80.html; and "The W-78 Warhead: Intermediate Yield Strategic ICBM MIRV Warhead," the Nuclear Weapon Archive, September 1, 2001, nuclearweaponarchive.org/Usa/Weapons/W78.html.

13 U.S. Congressional Budget Office, *Projected Costs of U.S. Nuclear Forces, 2019 to 2028*, January 2019, www.cbo.gov/publication/54914.

14 "Advanced Extremely High Frequency System," U.S. Air Force Space Command Fact Sheet, March 22, 2017, www.afspc.af.mil/About-Us/Fact-Sheets/Display/Article/249024/advanced-extremely-high-frequency-system/.

15 Sandra Erwin, "Satellites, Command-and-Control Systems Taking a Bigger Bite of Nuclear Modernization Budget," *Space News*, January 24, 2019, spacenews.com/satellites-command-and-control-systems-taking-a-bigger-bite-of-nuclear-modernization-budget/.

16 Sandra Erwin, "U.S. STRATCOM to Take Over Responsibility for Nuclear Command, Control and Communications," *Space News*, July 23, 2018, spacenews.com/u-s-stratcom-to-take-over-responsibility-for-nuclear-command-control-and-communications/.

17 The focus of this report is on the nuclear delivery vehicles, command, control, and communications systems, bombs, and warheads that constitute the U.S. nuclear triad and related systems. It does not focus on other, important components of the nuclear modernization such as nuclear weapons laboratory facility upgrades, operational technology, digitization of manufacturing or component fabrication processes, and other supporting tools and activities. Initiatives at the Departments of Defense and Energy are underway to address cybersecurity risks of facilities, operational technology, and digital or advanced tools used throughout the industrial base.

18 Office of the Deputy Assistant Secretary of Defense for Nuclear Matters, *Nuclear Matters Handbook 2020* (Washington, DC: U.S. Department of Defense, 2020), 7, www.acq.osd.mil/ncbdp/nm/nmhb/docs/NMHB2020.pdf.

19 "Department of Defense Background Briefing on Nuclear Deterrence and Modernization," transcript of senior Defense officials' briefing, February 21, 2020, www.defense.gov/Newsroom/Transcripts/Transcript/Article/2090986/department-of-defense-background-briefing-on-nuclear-deterrence-and-modernizati/; and "Nuclear Modernization: Ensuring a Safe, Secure, Reliable, and Credible U.S. Nuclear Deterrent," U.S. Department of Defense, media.defense.gov/2019/Apr/01/2002108024/-1/-1/1/NUCLEAR-MODERNIZATION-FIVE-KEY-TAKEAWAYS.PDF.

20 "Department of Defense Background Briefing on Nuclear Deterrence and Modernization."

21 The authors are aware that many details about the nuclear modernization plans and systems are classified. For a full discussion about the research methods, the availability of public information on these topics, and the rationale for the open-source survey, please see the appendix.

22 "Initiatives included in or related to the nuclear modernization drive" refers to upgrades to and acquisition of new components of the nuclear delivery triad, bombs and warheads, and command, control, and communications systems.

23 Data from FY2020 RDT&E budget justifications, updated with FY21. See the methodology section, in Appendix.

24 See full methodology section, in the appendix, for details. These data rely predominately on RDT&E budget requests of fiscal years 2020 and 2021, presenting a snapshot of the overall modernization effort.

25 Office of the Under Secretary of Defense for Acquisition and Sustainment, *Acquisition Policy Transformation Handbook* (Washington, DC: U.S. Department of Defense, January 15, 2020), www.acq.osd.mil/ae/assets/docs/DoD%205000%20Series%20Handbook%20(15Jan2020).pdf.

26 For Columbia-class submarine: U.S. Library of Congress, Congressional Research Service, *Navy Columbia (SSBN-826) Class Ballistic Missile Submarine Program*; for GBSD: "Air Force Reviews Preliminary Design for Future ICBM," Air Force Nuclear Weapons Center, May 15, 2020, www.afnwc.af.mil/News/Article/2188140/air-force-reviews-preliminary-design-for-future-icbm/; for

B-21 bomber: U.S. Library of Congress, Congressional Research Service, *Air Force B-21 Raider Long-Range Strike Bomber*, by Jeremiah Gertler,. R44463 (November 13, 2019), 6, https://fas.org/sgp/crs/weapons/R44463.pdf.

27 Refer to the methodology section and table in the appendix.

28 Infra "Early Warning" case in point.

29 U.S. Department of Defense, Fiscal Year (FY) 2020 Budget Estimates, *Research, Development, Test & Evaluation, Air Force, Vol. III, Part 1*, "PE 0101127F: B-2 Squadrons" (March 2019), 3A-230, www.saffm.hq.af.mil/Portals/84/documents/FY20/RDTE/FY20_PB_RDTE_Vol-IIIa.pdf?ver=2019-03-18-153510-997; and U.S. Department of Defense, Fiscal Year (FY) 2020 Budget Estimates, *Research, Development, Test & Evaluation, Air Force, Vol. III, Part 1*, "PE 0101126F: B-1B Squadrons" (March 2019), 3A-217, www.saffm.hq.af.mil/Portals/84/documents/FY20/RDTE/FY20_PB_RDTE_Vol-IIIa.pdf?ver=2019-03-18-153510-997.

30 U.S. Department of Defense, Fiscal Year (FY) 2020 Budget Estimates, *Research, Development, Test & Evaluation, Air Force, Vol. III, Part 1*, "PE 0101122F: Air-Launched Cruise Missile (ALCM)" (March 2019), 3A-209, www.saffm.hq.af.mil/Portals/84/documents/FY20/RDTE/FY20_PB_RDTE_Vol-IIIa.pdf?ver=2019-03-18-153510-997.

31 U.S. Department of Defense, Fiscal Year (FY) 2020 Budget Estimates, *Research, Development, Test & Evaluation, Air Force, Vol. II*, "PE 0603851F: Intercontinental Ballistic Missile," (March 2019), 2-70, www.saffm.hq.af.mil/Portals/84/documents/FY20/RDTE/FY20_PB_RDTE_Vol-II.PDF?ver=2019-03-18-153506-683.

32 U.S. Library of Congress, Congressional Research Service, *Navy Columbia (SSBN-826) Class Ballistic Missile Submarine Program*; and U.S. Department of Defense, Fiscal Year (FY) 2020 Budget Estimates, *Research, Development, Test & Evaluation, Navy, Budget Activity 5*, "PE 0604558N: New Design SSN" (March 2019), 3-991, www.secnav.navy.mil/fmc/fmb/Documents/20pres/RDTEN_BA5_Book.pdf.

33 "B61 Mod 12 Life Extension Program Tail Kit Assembly," FY18 Air Force Programs, Office of the Director, Operational Test and Evaluation, 173–4, www.dote.osd.mil/Portals/97/pub/reports/FY2018/af/2018b61.pdf?ver=2019-08-21-155843-557.

34 U.S. Government Accountability Office, *B61-12 Nuclear Bomb: Cost Estimate for Life Extension Incorporated Best Practices, and Steps Being Taken to Manage Remaining Program Risks*, GAO-18-456 (Washington, DC, May 2018), 14, www.gao.gov/assets/700/692202.pdf.

35 Leah Bryant, "Nuclear Bomb Tail Kit Reaches Major Milestone for Production Phase," Air Force Nuclear Weapons Center, December 7, 2018, www.af.mil/News/Article-Display/Article/1707698/nuclear-bomb-tail-kit-reaches-major-milestone-for-production-phase/.

36 "B61 Mod 12 Life Extension Program Tail Kit Assembly."

37 "B61 Mod 12 Life Extension Program Tail Kit Assembly."

38 Allison B. Bawden, Director, Natural Resources and Environment, National Nuclear Security Administration, *Nuclear Weapons: NNSA's Modernization Efforts Would Benefit from a Portfolio Management Approach* (testimony before the Subcommittee on Strategic Forces, Committee on Armed Services, U.S. House of Representatives), GAO-20-443T (Washington, DC: March 3, 2020), 4, www.gao.gov/assets/710/705058.pdf; U.S. Department of Energy, National Nuclear Security Administration, *Fiscal Year 2020: Stockpile Stewardship and Management Plan* (report to Congress) (Washington, DC, July 2019), 2-40–41, fas.org/nuke/guide/usa/ssmp-2020.pdf.

39 Charles P Verdon, Deputy Administrator for Defense Programs, National Nuclear Security Administration, *Status of the B61-12 Life Extension and W88 Alteration 370 Programs* (testimony before the Subcommittee on Strategic Forces, Committee on Armed Services, U.S.

House of Representatives), September 25, 2019, www.congress.gov/116/meeting/house/109998/witnesses/HHRG-116-AS29-Wstate-VerdonC-20190925.pdf.

40 U.S. Government Accountability Office, *Nuclear Weapons: NNSA Needs to Incorporate Additional Management Controls Over Its Microelectronics Activities*, GAO-20-357 (Washington, DC, June 9, 2020), 8–10, www.gao.gov/products/GAO-20-357.

41 For example, see Hans Kristensen and Robert Norris,"The B61 Family of Nuclear Bombs," *Bulletin of the Atomic Scientists* 70 no. 3 (2014), 83, www.tandfonline.com/doi/pdf/10.1177/0096340214531546.

42 Aaron Mehta, "How a $5 Part Used to Modernize Nuclear Warheads Could Cost $850 Million to Fix," *Defense News*, September 25, 2019, www.defensenews.com/smr/nuclear-arsenal/2019/09/25/nuclear-warhead-programs-need-850m-fix-heres-how-the-government-plans-to-cover-it/.

43 U.S. Department of Energy, *National Nuclear Security Administration FY 2021 Congressional Budget Request*, Volume 1, (Washington, DC, February 2020), 120, www.energy.gov/sites/prod/files/2020/03/f72/doe-fy2021-budget-volume-1_2.pdf; and "B61-12 Life Extension Program," National Nuclear Security Administration, June 2020, www.energy.gov/sites/prod/files/2020/06/f76/B61-12-20200622.pdf.

44 U.S. Department of Defense, Fiscal Year (FY) 2020 Budget Estimates, *Research, Development, Test & Evaluation, Air Force, Vol. II*, "PE 1206441F: Space Based Infrared System (SBIRS) High EMD" (March 2019), 2-983, and "PE 1206442F: Next Generation OPIR," 2-995, www.saffm.hq.af.mil/Portals/84/documents/FY20/RDTE/FY20_PB_RDTE_Vol-II.PDF?ver=2019-03-18-153506-683.

45 Jeffrey Larsen, *Nuclear Command, Control, and Communications: US Country Profile*, Tech4GS Special Reports, August 22, 2019, 5, https://nautilus.org/napsnet/napsnet-special-reports/nuclear-command-control-and-communications-us-country-profile/; some sources list higher estimates, of up to 240 NC3 systems. See also Philip Reiner, Alexa Wehsener, and M. Nina Miller, "When Machine Learning Comes to Nuclear Communication Systems," C4ISRNET, April 30, 2020, https://www.c4isrnet.com/thought-leadership/2020/04/30/when-machine-learning-comes-to-nuclear-communication-systems/.

46 Valerie Insinna, "The US Nuclear Forces' Dr. Strangelove-Era Messaging System Finally Got Rid of Its Floppy Disks," C4ISRNET, October 17, 2019, www.c4isrnet.com/air/2019/10/17/the-us-nuclear-forces-dr-strangelove-era-messaging-system-finally-got-rid-of-its-floppy-disks/; see also U.S. Department of Defense, Fiscal Year (FY) 2020 Budget Estimates, *Research, Development, Test & Evaluation, Air Force, Vol. III, Part 1*, "PE 0101316F: Worldwide Joint Strategic Communications" (March 2019), 30-307, https://www.saffm.hq.af.mil/Portals/84/documents/FY20/RDTE/FY20_PB_RDTE_Vol-IIIa.pdf?ver=2019-03-18-153510-997.

47 David Deptula and William LaPlante, with Robert Haddick, *Modernizing U.S. Nuclear Command, Control, and Communications* (Arlington, VA: Mitchell Institute for Aerospace Studies, February 2019), 5, http://docs.wixstatic.com/ugd/a2dd91_ed45cfd71de2457eba3bcce4d0657196.pdf.

48 "Strategic Automated Command Control System," Federation of American Scientists, January 10, 1999, fas.org/nuke/guide/usa/c3i/saccs.htm.

49 U.S. Government Accountability Office, *Information Technology: Federal Agencies Need to Address Aging Legacy Systems*, GAO-16-468 (Washington, DC, 2016), 60, www.gao.gov/assets/680/677436.pdf.

50 Insinna, "The US Nuclear Forces' Dr. Strangelove-era Messaging System Finally Got Rid of its Floppy Disks."

51 U.S. Department of Defense, Fiscal Year (FY) 2020 Budget Estimates, *Research, Development, Test & Evaluation, Air Force, Vol. III, Part 2*, "PE 1203179F: Integrated Broadcast Service (IBS)"

(March 2019), 3B-837, www.saffm.hq.af.mil/Portals/84/documents/FY20/RDTE/FY20_PB_RDTE_Vol-IIIb.pdf?ver=2019-03-18-153459-043.

52 U.S. Library of Congress, Congressional Research Service, *Defense Capabilities: Joint All Domain Command and Control*, by John R. Hoehn, IF11493 (April 6, 2020), https://crsreports.congress.gov/product/pdf/IF/IF11493/2; and Sherrill Lingel, Jeff Hagen, Eric Hastings, Mary Lee, Matthew Sargent, Matthew Walsh, Li Ang Zhang, and David Blancett, *Joint All-Domain Command and Control for Modern Warfare: An Analytic Framework for Identifying and Developing Artificial Intelligence Applications* (Santa Monica, CA: RAND Corporation, 2020), www.rand.org/pubs/research_reports/RR4408z1.html; and Morgan Dwyer, "Making the Most of the Air Force's Investment in Joint All Domain Command and Control," Center for Strategic and International Studies, March 6, 2020, www.csis.org/analysis/making-most-air-forces-investment-joint-all-domain-command-and-control.

53 Colin Clark, "Nuclear C3 Goes All Domain: Gen Hyten," Breaking Defense, February 20, 2020, breakingdefense.com/2020/02/nuclear-c3-goes-all-domain-gen-hyten/.

54 Deptula and LaPlante, with Haddick, *Modernizing U.S. Nuclear Command, Control, and Communications*.

55 In this report, the term "process automation" refers to business or robotic process automation in which the tool performs "if, then, else" functions using information technology, reducing the burden of repetitive or time-sensitive tasks for operators. (See Gartner glossary, business process automation and robotic process automation: www.gartner.com/en/glossary.) "Machine learning" in this report refers to software development that includes "systems that can learn and then teaches them what to do" either through direct human supervision or machine guidance; "machines learn by finding statistical relationships in past data." (See Vincent Boulanin, Lora Saalman, Petr Topychkanov, Fei Su, and Moa Peldán Carlsson, *Artificial Intelligence, Strategic Stability, and Nuclear Risk*, (Stockholm International Peace Research Institute, June 2020), 9, www.sipri.org/sites/default/files/2020-06/artificial_intelligence_strategic_stability_and_nuclear_risk.pdf.)

56 Bob Work, "Remarks by Deputy Secretary Work on Third Offset Strategy" (speech, Brussels, Belgium, April 28, 2016), www.defense.gov/Newsroom/Speeches/Speech/Article/753482/remarks-by-d%20eputy-secretary-work-on-third-offset-strategy/.

57 Defense Innovation Board, *AI Principles: Recommendations on the Ethical Use of Artificial Intelligence by the Department of Defense*, October 31, 2019, media.defense.gov/2019/Oct/31/2002204458/-1/-1/0/DIB_AI_PRINCIPLES_PRIMARY_DOCUMENT.PDF.

58 U.S. Department of Defense, Fiscal Year (FY) 2020 Budget Estimates, *Research, Development, Test & Evaluation, Air Force, Vol. III, Part 1*, "PE 0101213F: Minuteman Squadrons" (March 2019), 3A-227, www.saffm.hq.af.mil/Portals/84/documents/FY21/RDTE_/FY21%20Air%20Force%20Research%20Development%20Test%20and%20Evaluation%20Vol%20IIIa.pdf?ver=2020-02-11-083556-403.

59 U.S. Department of Defense, Fiscal Year (FY) 2020 Budget Estimates, *Research, Development, Test & Evaluation, Air Force, Vol. III, Part 1*, "PE 0101213F: Minuteman Squadrons" (March 2019), 3A-227, www.saffm.hq.af.mil/Portals/84/documents/FY21/RDTE_/FY21%20Air%20Force%20Research%20Development%20Test%20and%20Evaluation%20Vol%20IIIa.pdf?ver=2020-02-11-083556-403.

60 U.S. Department of Defense, Fiscal Year (FY) 2021 Budget Estimates, *Research, Development, Test & Evaluation, Air Force, Vol. 1*, "M30MLG: MM III Modifications" (February 2020), 1-114, www.saffm.hq.af.mil/Portals/84/documents/FY21/PROCUREMENT_/FY21%20Air%20Force%20Missile%20Procurement_1.pdf?ver=2020-02-10-145322-973.

61 Office of the Deputy Chief of Naval Operations for Information Warfare, "Why the Navy Needs a Digital Warfare Office," *CHIPS*, January–March 2018, www.doncio.navy.mil/chips/ArticleDetails.aspx?ID=9895 and Sam LaGrone, "VCNO Moran: Navy Must Do More to Harness Data to Help

Win Future Fights," USNI News, January 16, 2019, news.usni.org/2019/01/16/vcno-moran-navy-must-harness-data-better-help-win-future-fights.

62 U.S. Department of Defense, Fiscal Year (FY) 2020 Budget Estimates, *Research, Development, Test & Evaluation, Navy,Vol. 2*, "PE 0604027N: Digital Warfare" (February 2020), 2-1055, secnav.navy.mil/fmc/fmb/Documents/20pres/RDTEN_BA4_Book.pdf.

63 Megan Eckstein, "Navy Digital Warfare Office Proving Data Analytics Can Help Address Nagging Operational Problems," USNI News, October 4, 2017, news.usni.org/2017/10/04/navy-digital-warfare-office-proving-data-analytics-can-help-address-nagging-operational-problems.

64 U.S. Department of the Navy, *Agility and Accountability, Business Operations Plan Fiscal Years 2019–2021*, Version 1.2 (Washington, DC: Department of the Navy, October 2018), 34, https://www.documentcloud.org/documents/5018847-Dept-of-the-Navy-Business-Operations-Plan-FY2019.html.

65 U.S. Department of Defense, Fiscal Year (FY) 2021 Budget Estimates, *Research, Development, Test & Evaluation, Navy ,Vol.3* "PE 0605013N: Information Technology Development," (February 2020), 3-1536, www.secnav.navy.mil/fmc/fmb/Documents/21pres/RDTEN_BA5_Book.pdf; and Department of Defense, *Condition Based Maintenance Plus DoD Guidebook* (Washington, DC: Department of Defense, May 2008), www.dau.edu/guidebooks/Shared%20Documents/Condition%20Based%20Maintenance%20Plus%20(CBM+)%20Guidebook.pdf.

66 U.S. Department of Defense, *Summary of the 2018 Department of Defense Artificial Intelligence Strategy: Harnessing AI to Advance our Security and Prosperity*, 9, media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/SUMMARY-OF-DOD-AI-STRATEGY.PDF

67 U.S. Department of Defense, *Summary of the 2018 Department of Defense Artificial Intelligence Strategy*, 11.

68 Theresa Hitchens, "Air Force Expands AI-Based Predictive Maintenance," Breaking Defense, July 9, 2020, breakingdefense.com/2020/07/air-force-expands-ai-based-predictive-maintenance/.

69 Jack Shanahan, "Lt. Gen. Jack Shanahan Media Briefing on A.I.-Related Initiatives within the Department of Defense," August 30, 2019, www.defense.gov/Newsroom/Transcripts/Transcript/Article/1949362/lt-gen-jack-shanahan-media-briefing-on-ai-related-initiatives-within-the-depart/.

70 Quoted in Sydney J. Freedberg Jr., "No AI for Nuclear Command & Control: JAIC's Shanahan," Breaking Defense, September 25, 2019, breakingdefense.com/2019/09/no-ai-for-nuclear-command-control-jaics-shanahan/.

71 U.S. Library of Congress, Congressional Research Service *Artificial Intelligence and National Security*, by Kelley M. Saylor, R5178 (November 10, 2020), 11, fas.org/sgp/crs/natsec/R45178.pdf.

72 Funding requests from the Navy specify that cybersecurity upgrades will involve automated efforts, whereas Air Force requests do not highlight the same role for machine learning and automated systems. U.S. Department of the Navy, *Cybersecurity Readiness Review*, (Washington, DC, March 2019), 17, 42, 47,: www.wsj.com/public/resources/documents/CyberSecurityReview_03-2019.pdf?mod=article_inline.)

73 U.S. Department of Defense, Fiscal Year (FY) 2021 Budget Estimates *Research, Development, Test, and Evaluation, Navy, Vol. 5*, "PE 0303140N: Information Sys Security Program" (February 2020) 5-1111, www.secnav.navy.mil/fmc/fmb/Documents/21pres/RDTEN_BA7-8_Book.pdf; and Michael M. Gilday, Commander, U.S. Fleet Cyber Command, statement before the Subcommittee on Cybersecurity, Committee on Armed Services, U.S. Senate, May 23, 2017, 6, www.armed-services.senate.gov/imo/media/doc/Gilday_05-23-17.pdf.

74 U.S. U.S. Department of Defense, Fiscal Year (FY) 2021 Budget Estimates, *Research, Development, Test & Evaluation, Navy, Vol. 5* "PE 0303140N: Information Sys Security Program"

(Washington, DC: Department of the Navy, 2020) 5-1107, www.secnav.navy.mil/fmc/fmb/Documents/21pres/RDTEN_BA7-8_Book.pdf.

75 Michael M. Gilday, Commander, U.S. Fleet Cyber Command, statement before the Subcommittee on Cybersecurity, Committee on Armed Services, U.S. Senate, March 13, 2018, 5, www.armed-services.senate.gov/imo/media/doc/Gilday_03-13-18.pdf.

76 Gilday, statement before the Subcommittee on Cybersecurty, May 23, 2017, 5.

77 Robert K. Ackerman, "U.S. Navy Programs Shore up Cybersecurity," *SIGNAL*, October 1, 2018, www.afcea.org/content/us-navy-programs-shore-cybersecurity.

78 "Integrated Strategic Planning and Analysis Network (ISPAN)," Air Force Programs, www.dote.osd.mil/Portals/97/pub/reports/FY2012/af/2012ispan.pdf?ver=2019-08-22-111755-567; and U.S. Department of Defense, Major Automated Information System Annual Report 2016, *Integrated Strategic Planning and Analysis Network Increment 5*, apps.dtic.mil/sti/pdfs/AD1019821.pdf.

79 U.S. Department of Defense, Fiscal Year (FY) 2021 Budget Estimates, *Research, Development, Test & Evaluation, Air Force, Vol. III, Part 1*, "PE 0101324F: Integrated Strategic Planning & Analysis Network," (February 2020), 3a-275, www.saffm.hq.af.mil/Portals/84/documents/FY21/RDTE_/FY21%20Air%20Force%20Research%20Development%20Test%20and%20Evaluation%20Vol%20IIIa.pdf?ver=2020-02-11-083556-403.

80 NTI interview, May 6, 2020.

81 "Integrated Strategic Planning and Analysis Network (ISPAN); U.S. Department of Defense, *Major Automated Information System Annual Report 2016, Integrated Strategic Planning and Analysis Network Increment 5*; and Bryan Bartles, "GAP CIE Brief to the NDIA Capabilities for Senior Decision Makers Panel," Slide 5, March 6, 2018, ndiastorage.blob.core.usgovcloudapi.net/ndia/2018/cyber/Bartels.pdf

82 U.S. Department of Defense, Fiscal Year (FY) 2021 Budget Estimates, *Other Procurement, Air Force, Vol. 1*, "833560: Integrated Strat Plan & Analy Network (ISPAN)" (February 2020), 1-185, www.saffm.hq.af.mil/Portals/84/documents/FY21/PROCUREMENT_/FY21%20Air%20Force%20Other%20Procurement_1.pdf?ver=2020-02-10-145335-880.

83 "Federal Contract Opportunity: Global Adaptive Planning Collaborative Information Environment 2.0 (GC2.0)" FA8730-SS-GAPCIE, January 4, 2019, https://govtribe.com/opportunity/federal-contract-opportunity/global-adaptive-planning-collaborative-information-environment-2-dot-0-gc2-dot-0-fa873019r0009.

84 "Global Adaptive Planning Collaborative Information Environment 2.0 (GC2.0)" FedBizOpps Daily, FBO #6363 Modification, April 27, 2019, http://www.fbodaily.com/archive/2019/04-April/27-Apr-2019/FBO-05293569.htm.

85 U.S. Department of Defense, Fiscal Year (FY) 2021 Budget Estimate, *Budget Estimates Fiscal Year 2021: Other Procurement*, *Air Force, Vol. 1*, "833560: Integrated Strat Plan & Analy Network (ISPAN)."

86 Patty Welsh, "Battle Management Working to Improve Nuclear Scenario Planning," Air Force News, October 26, 2014, www.af.mil/News/Article-Display/Article/526335/battle-management-working-to-improve-nuclear-scenario-planning/

87 U.S. Department of Defense, *Major Automated Information System Annual Report 2016*, *Integrated Strategic Planning and Analysis Network Increment 5*.

88 U.S. Department of Defense, Fiscal Year (FY) 2021 Budget Estimate, *Budget Estimates Fiscal Year 2021: Research, Development, Test & Evaluation, Air Force*, *Volume III, Part 1*, "PE 0101324F: Integrated Strategic Planning & Analysis Network (February 2020), 3A-276, www.saffm.hq.af.mil/Portals/84/documents/FY21/RDTE_/FY21%20Air%20Force%20Research%20Development%20Test%20and%20Evaluation%20Vol%20IIIa.pdf?ver=2020-02-11-083556-403.

89 Theresa Hitchens, "2021 Budget Will Fully Fund Next-Gen OPIR, Says Roper," Breaking Defense, February 24, 2020, breakingdefense.com/2020/02/2021-budget-will-finally-fully-fund-next-gen-opir-says-roper/.

90 Nathan Strout, "The Air Force's New System to Process Missile Warning Data," C4ISRNET, January 28, 2020, www.c4isrnet.com/battlefield-tech/space/2020/01/29/the-air-forces-new-system-to-process-missile-warning-data/.

91 Theresa Hitchens, "Raytheon Nabs Contract for Missile Warning Ground System," Breaking Defense, January 28, 2020, breakingdefense.com/2020/01/raytheon-nabs-contract-for-missile-warning-ground-system/.

92 Kris Osborn, "This Is the Pentagon's Plan to Improve Its Missile Threat System," *The National Interest*, June 3, 2020, nationalinterest.org/blog/buzz/pentagons-plan-improve-its-missile-threat-system-159961; and Kris Osborn, "The U.S. Military Wants to Give President Trump More Time to Respond to a Nuclear Attack," *The National Interest*, July 13, 2020, nationalinterest.org/blog/buzz/us-military-wants-give-president-trump-more-time-respond-nuclear-attack-164667.

93 David Liapis, "Improving Lives, Maximizing Taxpayer Dollars with Dual-Use Space Capabilities," Air Force Space Command, September 12, 2019, www.afspc.af.mil/News/Article-Display/Article/1959289/improving-lives-maximizing-taxpayer-dollars-with-dual-use-space-capabilities/.

94 "Next Generation Overhead Persistent Infrared GEO Satellites Embracing Rapid Acquisitions with Successful System Requirements Reviews," Air Force Space Command, June 6, 2019, www.afspc.af.mil/News/Article-Display/Article/1870883/next-generation-overhead-persistent-infrared-geo-satellites-embracing-rapid-acq/.

95 U.S. Government Accountability Office, *Defense Acquisitions Annual Assessment: Drive to Deliver Capabilities Faster Increases Importance of Program Knowledge and Consistent Data for Oversight*, GAO-20-439 (Washington, DC, June 2020), 194, www.gao.gov/assets/710/707359.pdf.

96 Nathan Strout, "Infrared Sensors for the Space Force's Future Missile-Warning Satellites Pass Key Milestone," C4ISRNET, May 26, 2020, www.c4isrnet.com/battlefield-tech/space/2020/05/26/infrared-sensors-for-the-space-forces-next-generation-missile-warning-satellites-pass-key-milestone/.

97 Ashton Carter, "Remarks by Secretary Carter to troops at Minot Air Force Base, North Dakota," September 26, 2016, Department of Defense, www.defense.gov/Newsroom/Transcripts/Transcript/Article/956079/remarks-by-secretary-carter-to-troops-at-minot-air-force-base-north-dakota/

98 Office of the Deputy Assistant Secretary of Defense for Nuclear Matters, "The U.S. Nuclear Deterrent: Past, Present, and Future," in *Nuclear Matters Handbook*; Keir A. Lieber and Daryl G. Press, "Obama's Nuclear Upgrade," *Foreign Affairs*, July 6, 2011, www.foreignaffairs.com/articles/2011-07-06/obamas-nuclear-upgrade; and Keir A. Lieber and Daryl G. Press, "The Nukes We Need," *Foreign Affairs*, November/December 2009, www.foreignaffairs.com/articles/2009-11-01/nukes-we-need.

99 Deptula and LaPlante, with Haddick, *Modernizing U.S. Nuclear Command, Control, and Communications*.

100 See Defense Science Board, *Resilient Military Systems and the Advanced Cyber Threat*, (Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, January 2013), dsb.cto.mil/reports/2010s/ResilientMilitarySystemsCyberThreat.pdf; Government Accountability Office, *Weapon Systems Cybersecurity: DOD Just Beginning to Grapple with Scale of Vulnerabilities*, GAO-19-128 (Washington, DC, October 2018), www.gao.gov/assets/700/694913.pdf; Chris Nissen, John Gronager, Robert Metzger, and Harvey Rishikof, *Deliver Uncompromised: A Strategy for Supply Chain Security and Resilience in Response to the Changing Character of War* (MITRE Center for Technology and National Security, August 2018), 13, www.mitre.org/sites/default/files/publications/pr-18-2417-deliver-uncompromised-MITRE-study-26AUG2019.pdf; and Morgan Dwyer, "Does the Defense Department's New Approach to Industrial Base Cybersecurity Create More Problems than It Solves?" Center for Strategic and International Studies, December 18, 2019, csis.org/analysis/does-defense-departments-new-approach-industrial-base-cybersecurity-create-more-problems-it, among others.

101 "Attack surface" is the boundary of a system or environment that an attacker could "enter, cause an effect on, or extract data from," according to the National Institute of Standards and Technology's Computer Research Center, csrc.nist.gov/glossary/term/attack_surface.

102 U.S. Government Accountability Office, *Weapon Systems Cybersecurity: DOD Just Beginning to Grapple with Scale of Vulnerabilities*.

103 See, for example, U.S. Government Accountability Office, *Nuclear Weapons: NNSA Needs to Incorporate Additional Management Controls Over Its Microelectronics Activities*, GAO-20-357, Washington, DC, June 2020, www.gao.gov/assets/710/707424.pdf; and U.S. Government Accountability Office, *Weapon Systems Cybersecurity: DOD Just Beginning to Grapple with Scale of Vulnerabilities*.

104 The Office of the Under Secretary of Defense for Acquisition and Sustainment has launched the Cybersecurity Maturity Model Certification effort to ensure controlled, unclassified information is secure in the defense industrial base. Source of analysis: Nissen, Gronager, Metzger, and Rishikof, *Deliver Uncompromised*.

105 Nissen, Gronager, Metzger, and Rishikof, *Deliver Uncompromised*.

106 See U.S. Government Accountability Office, *Weapons Systems Cybersecurity:, DOD Just Beginning to Grapple with Scale of Vulnerabilities*.

107 U.S. Department of Defense, Budget Estimates Fiscal Year (FY) 2021, *Research, Development, Test & Evaluation, Air Force, Vol. II*, "PE 0604414F: Cyber Resiliency of Weapon Systems-ACS" (February 2020), 2-195–211, www.saffm.hq.af.mil/Portals/84/documents/FY21/RDTE_/FY21%20Air%20Force%20Research%20Development%20Test%20and%20Evaluation%20Vol%20II.pdf?ver=2020-02-12-145218-377.

108 U.S. Department of Defense, Fiscal Year (FY) 2021 Budget Estimates, *Research, Development, Test & Evaluation, Navy ,Vol 5*, "PE 0303140N: Information Sys Security Program" (February 2020) 5-1101–38, www.secnav.navy.mil/fmc/fmb/Documents/21pres/RDTEN_BA7-8_Book.pdf; U.S. Department of Defense, Fiscal Year (FY) 2021 Budget Estimates, *Research, Development, Test & Evaluation, Navy ,Vol 3*, "PE 0605013N: Information Technology Development" (February 2020) 3-1389–542, www.secnav.navy.mil/fmc/fmb/Documents/19pres/RDTEN_BA5_Book.pdf; and U.S. Department of Defense, Fiscal Year (FY) 2021 Budget Estimates, *Operation and Maintenance, Air Force, Vol. 1* "Cyberspace Activities" (February 2020) 206–218, www.saffm.hq.af.mil/Portals/84/documents/FY21/OM_/ACTIVE/FY21%20Air%20Force%20Operation%20and%20Maintenance%20Vol%20I.pdf?ver=2020-02-10-154101-027.

109 U.S. Department of Defense, Budget Estimates Fiscal Year (FY) 2021: *Research, Development, Test, and Evaluation, Navy, Vol, 4* "PE 0606942N: Assessments & Evals Cyber Vulnerabilities" (February 2020) 4-297, https://www.secnav.navy.mil/fmc/fmb/Documents/21pres/RDTEN_BA6_book.pdf.

110 U.S. Department of the Navy, *Cybersecurity Readiness Review*, 40.

111 Dan Gouré, "Navy Must Work To Secure Its Platforms, Networks And Installations From Cyber Attack" RealClearDefense, November 14, 2019, www.realcleardefense.com/articles/2019/11/14/navy_must_work_to_secure_its_platforms_networks_and_installations_from_cyber_attack_114851.html.

112 For example, Office of the Undersecretary of Defense for Acquisition, Technology, and Logistics, *DoD Program Manager's Guidebook for Integrating the Cybersecurity Risk Management Framework (RMF) into the System Acquisition Lifecycle*, September 2015, v. 1.0, www.dau.edu/tools/Lists/DAUTools/Attachments/37/DoD%20-%20Guidebook,%20Cybersecurity%20Risk%20Management%20Framework,%20v1.08,%20Sep%202015.pdf; and U.S. Department of the Air Force, *Risk Management Framework (RMF) for Air Force Information Technology* (Air Force Instruction 17-101), February 6, 2020, static.e-publishing.af.mil/production/1/saf_cn/publication/afi17-101/afi17-101.pdf.

113 See Defense Innovation Board recommendations, innovation.defense.gov/Recommendations/, accessed August 2020.

114 NTI interviews, multiple. See methodology for further details on the in-depth interviews conducted as part of this research.

115 U.S. Government Accountability Office, *Defense Acquisitions Annual Assessment*, GAO-20-439, June 2020.

116 U.S. Government Accountability Office, *Defense Acquisitions Annual Assessment*, GAO-20-439, June 2020.

117 Vulnerability management includes the organizational concerns of implementing controls and risk management for defending against cyberattacks. See also the U.S. Computer Emergency Response Team Guide: *Vulnerability Management, CRR Supplemental Resources Guide, Vol. 4* v. 1.1, us-cert.cisa.gov/sites/default/files/c3vp/crr_resources_guides/CRR_Resource_Guide-VM.pdf.

118 NTI interview, June 17, 2020.

119 Chaitra M. Hardison, Leslie Adrienne Payne, John A. Hamm, Angela Clague, Jacqueline Torres, David Schulker, and John S. Crown, *Attracting, Recruiting, and Retaining Successful Cyberspace Operations Officers: Cyber Workforce Interview Findings* (Santa Monica, CA: RAND Corporation, 2019), 59, www.rand.org/pubs/research_reports/RR2618.html.

120 See: Wesley Hallman, "Cybersecurity: Front and Center Industry," *National Defense*, June 19, 2019, www.nationaldefensemagazine.org/articles/2019/6/19/ndia-perspective-cybersecurity---front-and-center-for-industry.

121 For a recent example, see Andrew J. Konicki, "The Race to Implement Artificial Intelligence: Changing practices in order to catch up with our adversaries," *Marine Corps Gazette*, February 2020, WE3743, mca-marines.org/wp-content/uploads/The-Race-to-Implement-Artificial-Intelligence.pdf: "[T]oo many of those in the acquisition workforce see [the program development lifecycle map] as *the* means to delivering a product rather than as a framework."

122 U.S. Department of Defense Inspector General, *Security Controls at DoD Facilities for Protecting Ballistic Missile Defense System Technical Information*, Report No. DODIG-2019-034 (December 10, 2018), media.defense.gov/2018/Dec/14/2002072642/-1/-1/1/DODIG-2019-034.PDF.

123 See U.S. Government Accountability Office, *CYBERSECURITY DOD Needs to Take Decisive Actions to Improve Cyber Hygiene*, GAO-20-241 (Washington, DC, April 2020), www.gao.gov/assets/710/705886.pdf.

124 U.S. Government Accountability Office, *Defense Acquisitions Annual Assessment*, GAO-20-439, June 2020.

125 Defense Innovation Board, *Software is Never Done: Refactoring the Acquisition Code for Competitive Advantage*, March 21, 2019, media.defense.gov/2019/Mar/26/2002105909/-1/-1/0/SWAP.REPORT_MAIN.BODY.3.21.19.PDF.

126 NTI interview, June 11, 2020.

127 Sandra Erwin, "U.S. STRATCOM to Take Over Responsibility for Nuclear Command, Control and Communications," *Space News*, July 23, 2018, spacenews.com/u-s-stratcom-to-take-over-responsibility-for-nuclear-command-control-and-communications/.

128 Office of the Deputy Assistant Secretary of Defense for Nuclear Matters, "Nuclear Weapons Council" in *Nuclear Matters Handbook 2020*, 85; U.S. Government Accountability Office, "Nuclear Weapons Council," www.gao.gov/products/GAO-15-446. According to the GAO in 2015, "[t]he Council does not have an up-to-date agreement that reflects the processes it uses to carry out its responsibilities."

129 Morgan Dwyer, "Prioritizing Weapon System Cybersecurity in a Post-Pandemic Defense Department," Center for Strategic and International Studies, May 13, 2020, www.csis.org/analysis/prioritizing-weapon-system-cybersecurity-post-pandemic-defense-department.

130 National Institute of Standards and Technology, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, NIST Special Publication 800-37 Revision 2, December 2018, 64, nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf.

131 NTI interview, June 17, 2020.

132 Don Snyder, Sherrill Lingel, George Nacouzi, Brian Dolan, Jake McKeon, John Speed Meyers, Kurt Klein, and Thomas Hamilton, *Managing Nuclear Modernization Challenges for the U.S. Air Force: A Mission-Centric Approach* (Santa Monica, CA: RAND Corporation, 2019), www.rand.org/pubs/research_reports/RR3178.html.

133 *Cyberspace Solarium Commission Report*, (Washington, DC, March 2020), www.solarium.gov/; *Cyberspace Solarium Commission Legislative Proposals* (Washington, DC, July 2020), www.solarium.gov/; and Joshua Rovner, "Did the Cyberspace Solarium Commission Live Up To Its Name?" *War on the Rocks*, March 19, 2020, warontherocks.com/2020/03/did-the-cyberspace-solarium-commission-live-up-to-its-name/.

134 *National Defense Authorization Act for Fiscal Year 2021*, S.4049, 116th Congress, Sec. 1629. "Ensuring cyber resiliency of nuclear command and control system" 898–900, www.congress.gov/bill/116th-congress/senate-bill/4049.

135 Edward Geist, and Andrew J. Lohn, *How Might Artificial Intelligence Affect the Risk of Nuclear War* (Santa Monica, CA: RAND Corporation, 2018), 21, www.rand.org/content/dam/rand/pubs/perspectives/PE200/PE296/RAND_PE296.pdf.

136 China Arms Control and Disarmament Association, *Artificial Intelligence and Its Military Implications*, Stanley Center for Peace and Security, July 2019, stanleycenter.org/wp-content/uploads/2020/05/ArtificialIntelligence-ItsMilitaryImplications-China.pdf.

137 National Security Commission on Artificial Intelligence, *Second Quarter Recommendations (Quarterly Series No. 2)*, 2020, drive.google.com/file/d/1hgiA38FcyFcVQOJhsycz0Ami4Q6VLVEU/view.

138 "The JAIC Story," Joint Artificial Intelligence Center, https://www.ai.mil/about.html; and "Developing the Joint Common Foundation: Meet: Denise Hodge, Information Systems Security Manager," *AI in Defense*, Joint Artificial Intelligence Center, March 25, 2020, www.ai.mil/blog_03_25_20-developing_the_jcf_dhodges.html.

139 Richard Danzig, *Technology Roulette: Managing Loss of Control as Many Militaries Pursue Technological Superiority*, Center for a New American Security, June 2018, 17, s3.amazonaws.com/files.cnas.org/documents/CNASReport-Technology-Roulette-DoSproof2v2.pdf?mtime=20180628072101.

140 Paul Scharre, "Autonomous Weapons and Stability," (Ph.D diss., King's College London, March 2020), 11, kclpure.kcl.ac.uk/portal/files/129451536/2020_Scharre_Paul_1575997_ethesis.pdf.

141 In October 2020, the U.S. Army and Air Force agreed to collaborate and establish the Combined Joint All-Domain Command and Control (CJADC2), according to a press release: Joe Lacdan, "Army, Air Force Form Partnership, Lay Foundation for CJADC2 Interoperability," October 2, 2020, www.af.mil/News/Article-Display/Article/2369626/army-air-force-form-partnership-lay-foundation-for-cjadc2-interoperability/. See also James M. 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 (summer 2018), 56–99; Rebecca Hersman, Eric Brewer, and Suzanne Claeys, "NC3: Challenges Facing the Future System," *CSIS Briefs*, July 9, 2020 www.csis.org/analysis/nc3-challenges-facing-future-system ;and Clark, "Nuclear C3 Goes All Domain: Gen Hyten."

142 Michèle Flournoy and Gabrielle Chefitz, *Sharpening the U.S. Military's Edge: Critical Steps for the Next Administration*, Center for a New American Security, July 13, 2020, www.cnas.org/publications/commentary/sharpening-the-u-s-militarys-edge-critical-steps-for-the-next-administration.

143 Rebecca Hersman, Reja Younis, Bryce Farabaugh, Bethany Goldblum, and Andrew Reddie, *Under the Nuclear Shadow: Situational Awareness Technology and Crisis Decisionmaking*, Center for Strategic and International Studies, March 18, 2020, 33–38, www.csis.org/analysis/under-nuclear-shadow-situational-awareness-technology-and-crisis-decisionmaking.

144 Rachel S. Cohen, "Hyten: Future NC3 Network to Use Commercial Systems," *Air Force Magazine*, April 11, 2019, www.airforcemag.com/hyten-future-nc3-network-to-use-commercial-systems/.

145 Sandra Erwin, "Satcom Conumdrum [*sic*]: Air Force Contemplating Right Mix of Commercial, Military Satellites," *SpaceNews*, May 6, 2019, spacenews.com/satcom-conumdrum-air-force-contemplating-right-mix-of-commercial-military-satellites/.

146 Refer to appendix on DARPA Blackjack Program.

147 Ralph Thiele, *Artificial Intelligence—A Key Enabler of Hybrid Warfare*, COI Strategy & Defence, March 2020, www.hybridcoe.fi/wp-content/uploads/2020/03/WP-6_2020_rgb.pdf.

148 See Charles Pickar, "Informing DoD Program Planning through the Examination of the Causes of Delays in Acquisition Using Acquisition Data" (Paper presented at the 15th Annual Acquisition Research Symposium, Monterrey, CA, March 2020), www.researchgate.net/publication/339782829_INFORMING_DOD_PROGRAM_PLANNING_THROUGH_THE_EXAMINATION_OF_THE_CAUSES_OF_DELAYS_IN_ACQUISITION_USING_ACQUISITION_DATA.

149 NTI interview, June 3, 2020.

150 Assessments should be conducted with regularity, include technical expertise and deep analysis, and have an accountability mechanism that, for example, calls on individuals to certify the results. Section 2.4, "Certify Cyber Resilience of U.S. Nuclear Systems," in Defense Science Board, *Task Force on Cyber Deterrence*, Department of Defense, February 2017 dsb.cto.mil/reports/2010s/DSB-CyberDeterrenceReport_02-28-17_Final.pdf.

151 "DoD Financial Management Regulation Volume 2B, Chapter 5, RDT&E Appropriations Chart" and "DoD Defense Acquisition Guidebook Technology Readiness Level Chart," Defense Acquisition University, www.dau.edu/cop/stm/DAU%20Sponsored%20Documents/FMR-TRL%20map.pdf.

152 See the Defense Innovation Board's "Software Acquisition and Practices (SWAP) Study," including Primary Recommendation B2, "Automated Testing and Evaluation": *Software Is Never Done: Refactoring the Acquisition Code for Competitive Advantage*, Defense Innovation Board, May 3, 2019, media.defense.gov/2019/Apr/30/2002124828/-1/-1/0/SOFTWAREISNEVERDONE_REFACTORINGTHEACQUISITIONCODEFORCOMPETITIVEADVANTAGE_FINAL.SWAP.REPORT.PDF.

153 Michèle A. Flournoy, Avril Haines, and Gabrielle Chefitz, *Building Trust through Testing: Adapting DOD's Test & Evaluation, Validation & Verification (TEVV) Enterprise for Machine Learning Systems, including Deep Learning Systems*, WestExec Advisors, October 2020, cset.georgetown.edu/wp-content/uploads/Building-Trust-Through-Testing.pdf.

154 JASON Defense Advisory Panel, *Perspectives on Research in Artificial Intelligence and Artificial General Intelligence Relevant to DoD*, JSR-16-Task-003, The Mitre Corporation, January 2017, 54, fas.org/irp/agency/dod/jason/ai-dod.pdf.

155 U.S. Department of Defense Directive 3000.09, November 21, 2012, "Autonomy in Weapons Systems," Enclosures 2 and 3, November 21, 2012, www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/300009p.pdf.

156 JASON, *Perspectives on Research in Artificial Intelligence and Artificial General Intelligence Relevant to DoD*.

157 The 2018 Department of Defense Artificial Intelligence Strategy seeks to "pioneer approaches for AI test, evaluation, verification, and validation"; there are no higher consequence undertakings toward which this ambition should apply than the nuclear modernization drive. See *Summary of the 2018 Department of Defense Artificial Intelligence Strategy: Harnessing AI to Enhance Our Security and Prosperity*, February 12, 2019, media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/SUMMARY-OF-DOD-AI-STRATEGY.PDF.

158 John D. Steinbruner, "Choices and Trade-offs" in *Managing Nuclear Operations*, ed. Ashton B. Carter, John D. Steinbruner, and Charles A. Zraket (Washington, DC: Brookings Institution Press, 1987), 535.

159 This is a hypothetical example that is consistent with the Department of Defense's principles for ethical use of artificial intelligence. See "DoD Adopts Ethical Principles for Artificial Intelligence" press release, February 24, 2020, www.defense.gov/Newsroom/Releases/Release/Article/2091996/dod-adopts-ethical-principles-for-artificial-intelligence/.

160 This use of "strategic stability" is among the more narrow definitions of the phrase, as discussed by James M. Acton in "Reclaiming Strategic Stability," in *Strategic Stability: Contending Interpretations*, ed. Elbridge A. Colby and Michael S. Gerson (Carlisle, PA: Strategic Studies Institute and U.S. Army War College Press, 2013), 117.

Nuclear Threat Initiative

1776 Eye Street, NW, Suite 600

Washington, DC 20006

www.nti.org

Facebook.com/nti.org @NTI_WMD @NTI_WMD