CNA

April 2023

Artificial Intelligence in Nuclear Operations

CHALLENGES, OPPORTUNITIES, AND IMPACTS

Tim McDonnell, Mary Chesnut, Tim Ditter, Anya Fink, Larry Lewis

with contributions by Annaleah Westerhaug

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

IRM-2023-U-035284-Final

Abstract

The US, Russia, and China have all recognized the revolutionary promise of artificial intelligence (AI). It is likely, as each seeks areas of advantage through AI, that they will explore nuclear applications of AI. Consequently, the US State Department's Bureau of Arms Control, Verification, and Compliance (AVC) asked CNA to conduct research and analysis that would sharpen its understanding of how AI could affect nuclear risks and how AVC could reduce those risks and capture security-enhancing benefits. This report characterizes how all three competitors are using AI in nuclear operations; how they might do so in the future; and how their uses of AI could increase, decrease, or otherwise affect nuclear risks. It also recommends ways the US government might mitigate the risks of AI-enabled nuclear operations and capturing possible risk-reducing benefits.

This document contains the best opinion of CNA at the time of issue. The views, opinions, and findings contained in this report should not be construed as representing the official position of the Department of State.

DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

Public Release 4/14/2023

This work was created in the performance of Department of State Contract No. 19AQMM21P1807.

Topical Report No. 03.

Reporting Period: October 2021 – February 2022

Reporting Date: April, 2023

Cover image: An Air Force officer operates a terminal for the Semi-Automatic Ground Environment, the world's first networked computer system. Beginning in the late 1950s, it aggregated data from hundreds of radars to coordinate the defense of North America against nuclear-armed Soviet bombers. Photo credit: MIT Lincoln Lab.

Approved by: **April 2023**

Nilanthi Samaranayake

Nilanthi Samaranayake, Research Program Director
Strategy and Policy Analysis
Strategy, Policy, Plans, and Programs Division

This document may contain materials protected by the Fair Use guidelines of Section 107 of the Copyright Act, for research purposes only. Any such content is copyrighted and not owned by CNA. All rights and credits go directly to content's rightful owner.

Request additional copies of this document through inquiries@cna.org.

© 2023 CNA Corporation

Executive Summary

The US, the Russian Federation, and the People's Republic of China (PRC) have all recognized the revolutionary promise of artificial intelligence (AI), with machines completing complex tasks and matching or exceeding human performance. In parallel, all three competitors are modernizing their nuclear forces. It is likely, as each seeks areas of advantage through AI, that they will explore nuclear applications. AI applications—in both nuclear operations and AI-enabled military capabilities more broadly—could increase or decrease nuclear risk.

Research questions

Against this background, the US State Department's Bureau of Arms Control, Verification, and Compliance (AVC) asked CNA to conduct research and analysis that would sharpen its understanding of how AI could impact nuclear risks. To that end, CNA addressed three questions:

1. How are the US, Russia, and PRC using AI to enable their respective nuclear operations today?
2. How might US, Russian, and PRC enabled nuclear postures interact—especially during crises or conflict—in the circa 2035 timeframe? In what specific ways might AI increase or decrease nuclear risk?
3. What steps can the US government take to mitigate AI-driven nuclear risks and/or capture any risk-reducing benefits of AI-enabled nuclear operations?

Project contributions

This project makes two basic contributions. The first is a deep exploration of the many complicated ways that AI could influence nuclear risk that goes beyond what can be found in prior research on the topic. Building on that exploration, the second contribution is a set of recommendations that will help the US government mitigate the risks and capture the risk-reducing benefits of AI-enabled nuclear operations.

Findings

Departing from the observation that AI-enabled nuclear operations could have both positive and negative effects on overall nuclear risk, we identified mechanisms by which AI-enabled nuclear operations could increase or reduce nuclear risk, as well as mechanisms by which AI could have a significant but uncertain impacts on nuclear risk. These mechanisms account for not only the technical characteristics of AI, but also for the interface between humans and AI, the ways that AI can alter the behavior of human operators, and the ways AI might shape leaders' decisions about nuclear use in crisis or war—specifically, the following:

- AI could increase nuclear risks as a result of three categories of challenges.
  - **AI technical challenges** include the performance of specific AI systems, complex and unpredictable interactions among AI systems operating in a system of systems, shortcomings in AI training data, poor alignment between AI tools and tasks, and adversary action against AI systems.
  - **Human-factors challenges** include human trust in AI, unskilled use of AI by operators, skill degradation, and decision-time compression.
  - **Risks from leader calculus** center on the difficulty of assessing how AI could affect the military balance—which in turn shapes leaders' choices.
- There are opportunities for AI to mitigate nuclear risks in four areas:
  - Nuclear weapons surety
  - Survivability and resilience of nuclear forces
  - Leadership decision-time expansion
  - Crisis and conflict de-escalation
- AI could also have significant effects on nuclear risk if used to improve capabilities in five areas. However, whether these improved capabilities reduce or decrease nuclear risk would depend on the details of exactly how AI was used, by which actors, and to what ends. The five areas are as follows:
  - Operations and maintenance of nuclear forces
  - Performance of non-nuclear forces
  - Performance of nuclear forces
  - Analysis, planning, and decision support
  - Active air and missile defense

Recommendations

Based on these findings we identified three sets of steps that can promote the desirable nuclear risk-reducing benefits of AI-enabled nuclear operations and mitigate risks. These steps are nested, reflecting the fact that AI applications in the nuclear niche will be shaped by military applications more broadly, as well as in the non-military AI ecosystem. Specifically, we propose the following:

- ***Focused risk mitigation for AI applications in nuclear operations.*** Because of the unique context and characteristics of nuclear operations and the high stakes involved, some risk mitigation steps should focus specifically on AI applications in nuclear operations.
- ***Applied efforts on risk mitigation of AI applications in military operations.*** The US military, like many militaries around the world, is seeking to apply AI to many functions involving conventional warfare. These general military applications will share many of the same challenges as applications to nuclear operations. This reflects an opportunity for parts of the military and government responsible for nuclear operations to work with the US military as a whole to reduce risks from military applications of AI overall.
- ***Basic research and practical solutions for fundamental sources of AI-related risks.*** Given the relative newness of modern AI techniques and a focus on commercial applications versus fundamental understanding and safety, there are many aspects of AI risks that are still not well understood. The US government can work with a wide array of partners—other governments, industry, and academia—to better understand these risks and to seek collective solutions to mitigate them. Such fundamental research would help reduce the risks of using AI in a wide range of fields, including nuclear operations.

This page intentionally left blank.

Contents

Introduction

Project background

The US and its great power competitors have recognized the revolutionary promise of artificial intelligence (AI), with machines completing complex tasks and matching or exceeding human performance. For the US, AI is now a key element of its national security strategy. But the US is not alone in recognizing the criticality of AI to national security. Russian Federation President Vladimir Putin once remarked that "the one who becomes the leader in this sphere [artificial intelligence] will be the ruler of the world."[1] Similarly, People's Republic of China (PRC) Paramount Leader Xi Jinping has argued that China must "ensure that our country marches in the front ranks where it comes to theoretical research in this important area of AI and occupies the high ground in critical and AI core technologies." In 2017, China's central government released the Next-Generation Artificial Intelligence Development Plan, which explicitly seeks to "promote all kinds of AI technology to become quickly embedded in the field of national defense innovation."[2]

At the same time that peer competitors' leaders are extolling the importance of AI, the US, Russia, and China are modernizing their nuclear forces. It is likely, as each seeks areas of advantage through AI, that they will explore nuclear applications. The integration of AI into the great powers' increasingly sophisticated nuclear forces could change nuclear operations in all three countries in subtle and profound ways. Some AI applications—both within nuclear operations and AI-enabled military capabilities more broadly—could increase the likelihood or the speed at which conventional conflict could become nuclear. On the other hand, AI technologies could also increase safety and reduce the potential for human error across the nuclear arsenals of all three nations.[3]

[1] Radina Gigova, "Who Vladimir Putin Thinks Will Rule the World," CNN, Sep. 2, 2017, https://www.cnn.com/2017/09/01/world/putin-artificial-intelligence-will-rule-world.

[2] Likewise, China has developed a plan to "build on China's first-mover advantage in the development of AI to accelerate the construction of an innovative nation and global power." Next-Generation AI Development Plan, State Council of the PRC, July 20, 2017, https://na-production.s3.amazonaws.com/documents/translation-fulltext-8.1.17.pdf.

[3] Many of our findings and recommendations are likely germane to nuclear risks involving other states, such as North Korea, Iran, India, and Pakistan. However, we chose to focus our risk analysis and mitigation efforts in this project on the three countries that have the greatest potential to apply AI to their already robust and growing nuclear forces.

Research questions

Against this background, the US State Department's Bureau of Arms Control, Verification, and Compliance (AVC) asked CNA to conduct research and analysis that would sharpen its understanding of how AI could impact nuclear risks. To that end, CNA addressed three questions:

1. How are the US, Russia, and PRC using AI to enable their respective nuclear operations today?
2. How might US, Russian, and PRC–enabled nuclear postures interact—especially during crises or conflict—in the circa 2035 timeframe? In what specific ways might AI increase or decrease nuclear risk?
3. What steps can the US government take to mitigate AI-driven nuclear risks and/or capture any risk-reducing benefits of AI-enabled nuclear operations?

Approach and methodology

To answer these questions, CNA assembled a task organized team with expertise in nuclear operations, AI, and US, Russian, and PRC nuclear capabilities. Collectively, the team brought four analytic assumptions to the table going into the project:

- First, the United States prefers to avoid employment of nuclear weapons by any country at any scale. This assumption is rooted in long-standing US policies of deterring nuclear attack and reducing the salience of nuclear weapons in international politics.
- Second, the most likely paths to nuclear employment run through a major conventional war.
- Third, the risk of a botched attempt to employ nuclear weapons under extreme circumstances warrants treatment alongside the more commonly discussed risks of accidental, unauthorized, or inadvertent nuclear escalation because that outcome—like nuclear escalation—is something the US government would want to avoid.
- Fourth, because both AI and nuclear operations are so technically complex, in any attempt to understand how AI could shape future nuclear risks, the details—things like how countries attempt to apply AI in their nuclear operations, how successful they are, and how they perceive the AI-enabled nuclear capabilities of their rivals—will really matter. This meant that we had to engage deeply with these details as we carried out our research.

These assumptions informed the team's approach to the project, which we carried out in five basic steps:

1. We began with a detailed literature review covering the fields of AI and nuclear operations.
2. Next, we augmented this literature review with additional research to develop an AI implementation matrix (AIIM) that captures how the US, Russia, and the PRC are currently using or have used AI to enable their nuclear operations.
3. Subsequently, we built on this baseline analysis to devise a circa 2035 AI-enabled nuclear order of battle (OOB) for the US, Russia, and China. Our goal with this OOB was to provide a basis for discussion about how future AI-enabled nuclear postures could interact in crisis or conflict.
4. We convened two day-long workshops that included experts in both AI and nuclear issues from academia, think tanks, and government to explore how future AI-enabled nuclear postures could interact.
5. Finally, we compiled and analyzed the results of these workshops alongside existing literature on such topics as deterrence, escalation, and AI and emerging technologies more broadly to explicate the different mechanisms by which AI could shape future nuclear risks and how the US government could mitigate those risks and capture possible risk-reducing benefits of AI-enabled nuclear operations.

Additional details on the approach and methodology can be found in Appendix A: Approach and Methodology.

Roadmap

This report begins with an overview of existing literature on AI and nuclear risks. The sections that follow describe the role of automation and AI in US, Russian, and PRC nuclear operations. The report then proceeds with a discussion of nuclear risks and a crosswalk between ways in which AI-enabled technologies as applied to nuclear operations could increase, reduce, or have an uncertain impact on nuclear risks. We close with a series of three nested recommendations for mitigating the risks of AI-enabled nuclear operations and capturing possible risk-reducing benefits via focused risk mitigation in the AI-nuclear space, applied risk mitigation efforts for AI in military operations more broadly, and basic research on fundamental sources of AI-related risks.

Literature on AI and Nuclear Risks

In recent years, scholars and practitioners have debated the potential implications of AI-enabled technologies, autonomy, and other emerging and disruptive technologies for the practice of nuclear deterrence and for strategic arms control. Initial concerns in the literature that AI's only effect would be the prospect of an increase in escalation potential and nuclear risks have gradually given way to perspectives that AI presents both risks and opportunities, and that its effects on strategic stability could be either destabilizing or stabilizing. In turn, the reduction of destabilizing effects and the increase in stabilizing ones may be possible through governance and focused risk reduction. This literature review is not exhaustive, but it does provide an overview of key arguments.

Initial research and writing on AI and nuclear deterrence focused primarily on the increase in nuclear risks from first-strike instability and escalation of a conventional conflict. For example, Geist and Lohn, Davis, T4GS, Horowitz, Scharre, and others have written about the dangers stemming from perceptions of an imbalance in strategic capabilities (e.g., intelligence, surveillance, and reconnaissance (ISR) and defensive and offensive capabilities) and concerns about risk of a surprise attack; the issues of data reliability, adversarial hacking, and data manipulation compounded by the speed and lethality of AI; and challenges with decision-making given the expectations of speed and potential (over)reliance on data analytics and automation.[4] Horowitz, Scharre, and Velez-Green have argued that "the potential deployment of uninhabited, autonomous nuclear delivery platforms and vehicles could raise the prospect for accidents and miscalculation" while "the need to fight at machine speed and the cognitive risk introduced by automation bias could increase the risk of unintended escalation."[5]

[4] See, for example, Edward Geist and Andrew J. Lohn, *How Might Artificial Intelligence Affect the Risk of Nuclear War?* RAND Perspective, 2018, https://www.rand.org/content/dam/rand/pubs/perspectives/PE200/PE296/RAND_PE296.pdf; Zachary S. Davis, *Artificial Intelligence on the Battlefield: An Initial Survey of Potential Implications for Deterrence, Stability, and Strategic Surprise,* Lawrence Livermore National Laboratory/Center for Global Security Research, Mar. 2019, https://cgsr.llnl.gov/content/assets/docs/CGSR-AI_BattlefieldWEB.pdf; T4GS, "AI and the Military: Forever Altering Strategic Stability," T4GS Reports, Feb. 13, 2019, http://www.tech4gs.org/ai-and-human-decision-making.html; Michael C. Horowitz, "When Speed Kills: Lethal Autonomous Weapon Systems, Deterrence and Stability," *Journal of Strategic Studies* 42, no. 6 (2019), https://doi.org/10.1080/01402390.2019.1621174; Paul Scharre, "Military Applications of Artificial Intelligence: Potential Risks to International Peace and Security," in *The Militarization of Artificial Intelligence,* Stanley Center for Peace and Security, Aug. 2019, https://stanleycenter.org/publications/militarization-of-artificial-intelligence/; Vincent Boulanin, Lora Saalman, Petr Topychnakov, Fei Su, and Moa Peldan Carlsson, *Artificial Intelligence, Strategic Stability and Nuclear Risk,* SIPRI, June 2020, https://www.sipri.org/publications/2020/other-publications/artificial-intelligence-strategic-stability-and-nuclear-risk.

[5] Michael C. Horowitz, Paul Scharre, and Alexander Velez-Green, "A Stable Nuclear Future? The Impact of Autonomous Systems and Artificial Intelligence," Dec. 2019, available at https://arxiv.org/pdf/1912.05291.

Fitzpatrick has offered a scenario of a malevolent third-party interference into situational awareness and warning systems.[6]

Perhaps the most central focus has been on the role of AI in nuclear command, control, and communications (NC3) systems, along with the debate about whether a "dead hand"–type system could be stabilizing. In this regard, Lowther and McGiffin have argued that the US should develop an AI-based NC3 system that could "overcome the attack-time compression challenge" and "accelerate wartime decision-making."[7] O'Brien has countered that such AI as a decision-maker (as opposed to a decision aid) would be a "recipe for disaster," pointing to the "entanglement" problem, where sensors and key nodes could be destroyed early in a conflict, thus potentially limiting the data available to the AI-enabled system.[8] Sankaran posits that a more useful system would be one that could "argue in the face of overwhelming fear of an impending attack that a nuclear launch isn't happening."[9]

Some observers have noted the ripple effect of the AI-nuclear nexus on international security dynamics. A 2019 workshop by the Stanley Center for Peace and Security, Stimson Center, and the UN Office for Disarmament Affairs (UNODA) discussed the potential challenges of an arms race in AI, concluding that "characteristics of arms racing—high rates of investment, a lack of transparency, mutual suspicion and fear, and a perceived incentive to deploy first—heighten the risk of avoidable or accidental conflict."[10] Russian analyst Vadim Kozyulin has also pointed out that a global imbalance in military technologies could lead to AI "have-nots" responding with asymmetric approaches.[11]

More recent writings have focused on the opportunities, limits, and risks of the AI-nuclear nexus. Cox and Williams have argued the positives of integrating AI into ISR platforms and that

---

[6] Mark Fitzpatrick, "Artificial Intelligence and Nuclear Command and Control," *Survival* 61, no. 3 (2019), https://doi.org/10.1080/00396338.2019.1614782.

[7] Adam Lowther and Curtis McGiffin, "America Needs a 'Dead Hand'," War on the Rocks, Aug. 16, 2019, https://warontherocks.com/2019/08/america-needs-a-dead-hand/.

[8] Luke O'Brien, "Whither Skynet? An American 'Dead Hand' Should Remain a Dead Issue," War on the Rocks, Sep. 11, 2019, https://warontherocks.com/2019/09/whither-skynet-an-american-dead-hand-should-remain-a-dead-issue/.

[9] Jaganath Sankaran, "A Different Use for Artificial Intelligence in Nuclear Weapons Command and Control," War on the Rocks, Apr. 25, 2019, https://warontherocks.com/2019/04/a-different-use-for-artificial-intelligence-in-nuclear-weapons-command-and-control/.

[10] Melanie W. Sisson, "Multistakeholder Perspectives on the Potential Benefits, Risks, and Governance Operations for Military Applications of Artificial Intelligence," in *The Militarization of Artificial Intelligence,* Stanley Center for Peace and Security, Aug. 2019, https://stanleycenter.org/publications/militarization-of-artificial-intelligence/.

[11] Vadim Kozyulin, "Militarization of AI—A Russian Perspective," in *The Militarization of Artificial Intelligence,* Stanley Center for Peace and Security, Aug. 2019, https://stanleycenter.org/publications/militarization-of-artificial-intelligence/.

its use "as part of the analytical tool kit for early warning and detection could improve target identification, prevent false positives or close calls, and increase understanding of [the] adversary" and improve the effectiveness of wargaming and defense planning by potentially reducing human biases.[12] Favarro and Schwarz have written about the potential of human augmentation to compress the decision timeline, potentially raising risks but, at the same time, potentially minimizing the risk of accidents.[13] Johnson posits that "AI is unlikely to have a material impact" on NC3 and that, in addition to improving accuracy and navigation of conventional and nuclear systems, it could buttress their resilience against countermeasures and improve the survivability of unmanned systems, potentially reducing states' "fear of a nuclear decapitation."[14] Vaynman has looked at the role of AI in improving the processing of information gathered via satellites for monitoring and verification and finds that "while AI has the potential to improve unilateral monitoring in important ways, the benefits may also be somewhat overstated" because of brittleness, unclear accuracy, and failures.[15]

Some observers have focused on the uncertainty and complexity brought about by emerging and disruptive technologies, including AI, for conventional and nuclear operations. Gottemoeller has written about the "standstill conundrum," where "the survivability associated with secure second-strike retaliatory forces will become uncertain because their concealment will be impossible."[16] Hersman has focused on "wormhole escalation" dynamics, where nuclear dangers may arise as unintended consequences of actions with (seemingly) low escalatory risk.[17] Durkalec et al. have written about the complex interactions of emerging and disruptive technologies that could positively or negatively affect "a decision-maker's ability to

[12] Jessica Cox and Heather Williams, "The Unavoidable Technology: How Artificial Intelligence Can Strengthen Nuclear Stability," *The Washington Quarterly*, 44, no. 1 (2021), https://doi.org/10.1080/0163660X.2021.1893019.

[13] Marina Favarro and Elke Schwarz, "Human Augmentation and Nuclear Risk: The Value of a Few Seconds," *Arms Control Today*, Mar. 2022, https://www.armscontrol.org/act/2022-03/features/human-augmentation-nuclear-risk-value-few-seconds.

[14] James Johnson, "AI, Autonomy, and the Risk of Nuclear War," War on the Rocks, July 29, 2022, https://warontherocks.com/2022/07/ai-autonomy-and-the-risk-of-nuclear-war/.

[15] Jane Vaynman, "Better Monitoring and Better Spying: The Implications of Emerging Technology for Arms Control," *Texas National Security Review* 4, no. 4 (Fall 2021), http://dx.doi.org/10.26153/tsw/17496.

[16] Rose Gottemoeller, "The Standstill Conundrum: The Advent of Second-Strike Vulnerability and Options to Address It," *Texas National Security Review* 4, no. 4 (Fall 2021), http://dx.doi.org/10.26153/tsw/17496.

[17] Rebecca Hersman, "Wormhole Escalation in the New Nuclear Age," *Texas National Security Review,* Summer 2020, http://dx.doi.org/10.26153/tsw/10220.

assess the situation, deliberate about the optimal course of action, and control one's forces and execute preplanned operations."[18]

With so much of the focus on risks in the AI-nuclear nexus, there are the questions of governance and risk reduction. On multilateral governance, some authors have noted that the central challenge of governance is "uncertainty—about the ways AI will be applied, about whether current international law adequately captures the problems that use of AI might generate, and about the proper venues through which to advance the development of governance approaches for military applications of AI."[19] Nevertheless, some have proposed risk reduction measures such as an agreement on strict human control over nuclear launch decisions ("human-in-the-loop"); limits or bans on certain AI-enabled systems in nuclear operations or autonomous nuclear systems; and norm promotion, dialogues, and codes of conduct and other confidence and security-building measures (CSBMs) and transparency initiatives.[20]

This project builds on existing literature and advances it by offering insights into how specific AI applications could raise or lower specific kinds of nuclear risk. In so doing, we draw on deep knowledge of nuclear strategy, operations, and risk, and the (likely) strengths and weaknesses of AI as an enabler of nuclear operations to generate useful recommendations that move beyond generalities.

---

[18] Jacek Durkalec, Anna Peczeli, and Brian Radzinsky, *Nuclear Decision-Making, Complexity, and Emerging and Disruptive Technologies: A Comprehensive Assessment,* European Leadership Network, Feb. 2022, https://www.europeanleadershipnetwork.org/report/nuclear-decision-making-complexity-and-emerging-and-disruptive-technologies-a-comprehensive-assessment/.

[19] See *The Militarization of Artificial Intelligence,* Stanley Center for Peace and Security, Aug. 2019, https://stanleycenter.org/publications/militarization-of-artificial-intelligence/.

[20] Jessica Cox and Heather Williams, "The Unavoidable Technology: How Artificial Intelligence Can Strengthen Nuclear Stability," *The Washington Quarterly* 44, no. 1 (2021), https://doi.org/10.1080/0163660X.2021.1893019; Boulanin et al., *Artificial Intelligence, Strategic Stability and Nuclear Risk*; Michael C. Horowitz and Paul Scharre, *AI and International Stability: Risks and Confidence-Building Measures,* Center for a New American Security, Jan. 2021, https://www.cnas.org/publications/reports/ai-and-international-stability-risks-and-confidence-building-measures; James Johnson, "Inadvertent escalation in the age of intelligent machines: A new model for nuclear risk in the digital age," *European Journal of International Security* 7, no. 3 (2022), https://doi.org/10.1017/eis.2021.23.

AI in US, Russian, and PRC Nuclear Operations

To understand how specific AI applications could shape future nuclear risk, we had to first understand how the US, Russia, and PRC use, or might someday use, AI to enable their nuclear operations. We developed this understanding in two steps:

- First, we developed an AI implementation matrix (AIIM), which draws on open-source research conducted in English, Russian, and Mandarin to document the steps that the US, Russia, and the PRC have taken to date to use AI to enable their nuclear operations. The AIIM captures past and current uses of AI—as the term has evolved over time—as well as ongoing efforts to explore or pursue new applications. The AIIM is reproduced in Appendix B: AI Implementation Matrix.
- Second, we developed a notional circa 2035 AI-enabled nuclear order of battle for all three countries. This table builds on the research that went into the AIIM to illustrate what kinds of AI-enabled nuclear forces the US, Russia, and China *might* field a dozen years into the future. The notional circa 2035 AI-enabled nuclear OOB is reproduced in Appendix C: Notional Circa 2035 AI-Enabled Nuclear Order of Battle.

We used both the AIIM and the notional circa 2035 AI-enabled nuclear OOB to structure the discussion in a series of workshops. These workshops brought together experts on both AI and nuclear operations to generate detailed hypotheses on how different uses of AI by each great power could influence nuclear risk in a hypothetical future conflict.

This section summarizes both tables, providing an overview of how each country has approached the use of AI in nuclear operations to date, as well as their national proclivities—the drivers of their decision-making—with regard to using AI for nuclear operations in the future.

AI in US nuclear operations

The US has used computers to automate certain aspects of nuclear operations that otherwise would require human effort since the late 1950s. An early example was the Semi-Automatic Ground Environment system for US defense against nuclear-armed bomber attack, which used the world's first computer network to correlate radar tracks for incoming enemy aircraft and to cue fighter interceptors and missiles. Formerly, the work of generating an air picture and assigning specific interceptors to specific targets would have required a great deal of rapidly executed human labor. The Semi-Automatic Ground Environment was an early example of US use of "artificial intelligence" (by 1950s standards) to support nuclear operations.[21]

More broadly, the thrust of the United States' early efforts to use AI (as the definition evolved) for nuclear operations was to ensure that the US could either retaliate following an enemy nuclear attack or rapidly preempt such an attack before it was launched. As enemy weapons' travel time collapsed from hours (during the bomber age) to minutes (during the missile era), the US increasingly turned to computer-enabled automation to preempt or respond to attack.

To a large extent, these goals have persisted to the present. Common AI applications for the US seek to increase the time available for leadership decision-making and improve counterforce capabilities—the ability to destroy enemy nuclear forces before they can be used against the US or allies. Examples of AI applications that expand leadership decision time could include using AI to provide "earlier" early warning and speed the dissemination of orders. Examples of AI applications that improve counterforce could include using AI to identify and track mobile targets or to improve weapons' ability to penetrate to their targets autonomously following authorized launch.

The United States' use of AI to enable its nuclear forces takes place within the broader context of decision-making about military uses of AI. In general, the US is far more transparent about military uses of AI than either China or Russia. For example, the US Department of Defense (DOD) publishes AI strategy documents capturing its guidelines for the ethical uses of AI and autonomy in weapons systems.[22]

Finally, it is probably most significant that when DOD officials speak explicitly on AI applications for nuclear operations, their public statements evince a cautious approach. For example, the Air Force reportedly explored the possibility of making its B-21 Raider next-generation bomber optionally manned. However, then head of Air Force Global Strike Command General Robin Rand stated in 2016 that for nuclear missions, "I like the man in the loop; the pilot, the woman in the loop, very much."[23] Similarly, the former head of DOD's Joint

[21] "Semi-Automatic Ground Environment Air Defense System," MIT Lincoln Lab, https://www.ll.mit.edu/about/history/sage-semi-automatic-ground-environment-air-defense-system

[22] US Department of Defense, *Summary of the 2018 Department of Defense Artificial Intelligence Strategy: Harnessing AI to Advance Our Security and Prosperity,* 2019, p. 11, https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/SUMMARY-OF-DOD-AI-STRATEGY.PDF; C. Todd Lopez, "DOD Adopts 5 Principles of Artificial Intelligence Ethics," US Department of Defense, Feb. 25, 2020, https://www.defense.gov/News/News-Stories/Article/Article/2094085/dod-adopts-5-principles-of-artificial-intelligence-ethics/; US Department of Defense, "DOD Announces Update to DOD Directive 3000.09 'Autonomy in Weapon Systems.'" Jan. 25, 2023, https://www.defense.gov/News/Releases/Release/Article/3278076/dod-announces-update-to-dod-directive-300009-autonomy-in-weapon-systems/.

[23] "Air Force Wants to Keep 'Man in the Loop' with B-21 Raider," Military.com, Sep. 19, 2016, https://www.military.com/defensetech/2016/09/19/air-force-wants-to-keep-man-in-the-loop-with-b-21-raider.

AI Center (JAIC), Lieutenant General Jack Shanahan, has been similarly cautious about AI in nuclear operations, stating, "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."[24]

Looking ahead, the goals that seem most likely to animate US uses of AI in nuclear operations could include:

- Enhancing the effectiveness of counterforce strikes by improving target identification, weaponeering, delivery system reliability, penetration capability and accuracy, and battle damage assessment (BDA)
- Increasing pre-attack warning time by improving or accelerating intelligence collection and analysis, sensor data fusion, and warning message dissemination
- Improving the effectiveness of active defenses
- Accelerating the dissemination of orders from the President of the United States (POTUS) to executing units

AI in Russian nuclear operations

Like the United States, the Soviet Union and Russia have either studied or employed automation technologies since the early nuclear age. Key areas included early warning, missile defense, and command and control (C2) systems.

More recently, heralding a call from Russia's President Vladimir Putin, the Russian Ministry of Defense (MOD) has focused on developing AI-enabled and autonomous systems that can more or less independently accomplish various parts of the kill chain for conventional and dual-capable systems.

The MOD's interest in AI-enabled and autonomous technologies is driven by General Staff analyses that these capabilities will be extensively utilized in future warfare by leading powers and, more specific to nuclear operations, concerns that Russia's second-strike capability and critical targets will become more vulnerable with improvements in US strategic capabilities.[25] These analyses and concerns have led to the Russian military's development of AI/autonomous technologies to be utilized in early warning, command, control, communications, computers,

[24] Sydney Freeberg Jr., "No AI for Nuclear Command and Control: JAIC's Shanahan," Breaking Defense, Sep. 25, 2019, https://breakingdefense.com/2019/09/no-ai-for-nuclear-command-control-jaics-shanahan/.

[25] Jeffrey Edmonds, Samuel Bendett, Anya Fink, Mary Chestnut, Dmitry Gorenburg et al., *Artificial Intelligence and Autonomy in Russia,* CNA, May 2021, https://www.cna.org/CNA_files/centers/CNA/sppp/rsp/russia-ai/Russia-Artificial-Intelligence-Autonomy-Putin-Military.pdf.

and ISR (C4ISR) and air and missile defense systems, as well as boutique strike systems announced by President Putin in a 2018 speech.

Russian military thinkers are very aware of the hype surrounding AI versus the technical capabilities of current systems. They are also very conscious about the potential risks of employing AI-enabled and autonomous systems, ranging from these systems being used as attack vectors by adversaries to errors in the systems' design (resulting in damage to own systems).[26] While Russian military writings adamantly maintain that humans should be in the loop, particularly when it comes to nuclear operations, questions remain about the functioning of Russia's "Perimetr" retaliatory system that reportedly allows for some automated operations.[27]

Prior to the war in Ukraine, Russian officials stated, in the now-halted bilateral Strategic Stability Dialogue with the United States, that they were interested in discussing a "security equation" (or a "stability equation").[28] Russia's Chief of the General Staff, General Valery Gerasimov, stated in December 2021 that he understood the "security equation" as "encompass[ing] all types of offensive and defensive weapons impacting strategic stability, as well as new spheres of combat—cyberspace, space, and artificial intelligence."[29] Potential Russian concerns revolve around the employment of AI and autonomy as an enabler of US strategic capabilities. They include elements of AI/autonomy in the US global/regional missile defense architecture, ISR infrastructure in space that could enable improved tracking of Russian mobile intercontinental ballistic missiles (ICBMs), swarms of unmanned vehicles that could destroy C2 and defensive systems, and unmanned reusable space platforms.[30] As one

---

[26] A.V. Stepanov, "Issues of safety in employing AI in military systems (Вопросы безопасности применения искусственного интеллекта в системах военного назначения)," *Voennaya Mysl'* 4 (2021); V. Burenok, "AI: problems and solutions (Искусственный интеллект: проблемы и пути решения)," *Arsenal Otechestva* 1, no. 33 (2018), https://arsenal-otechestva.ru/article/1010-iskusstvennyj-intellekt-problemy-i-puti-resheniya.

[27] Petr Topychkanov, "Autonomy in Russian nuclear forces," in Vincent Boulanin, ed., *The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk*, vol. 1: *Euro-Atlantic Perspectives,* SIPRI, 2019, The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk, Volume I, Euro-Atlantic perspectives | SIPRI.

[28] Elena Chernenko, "The state is stably strategic" (Состояние стабильно стратегическое) *Kommersant*, July 27, 2021, https://www.kommersant.ru/doc/4918323.

[29] "Theses of the speech of the head of the General Staff of the RF at the briefing with defense attaches of foreign states" (Тезисы выступления начальника Генерального штаба ВС РФ на брифинге перед военными атташе иностранных государств), Russian Federation MOD website, Dec. 9, 2021, https://function.mil.ru/files/morf/%D0%A2%D0%B5%D0%B7%D0%B8%D1%81%D1%8B.pdf.

[30] Vadim Kozyulin, "Militarization of AI," in *The Militarization of Artificial Intelligence,* p. 27. Also see Col. D.V. Galkin, Col. P.A. Polyandra, and Col. A.V. Stepanov, "The state and perspectives of the use of AI in military affairs" (Состояние и перспективы использования искусственного интеллекта в военном деле)," *Voennaya Mysl,* Jan. 2021, pp. 113–124.

Russian military thinker posited, the development and deployment of autonomous robotic systems could also have dramatic implications for antisubmarine warfare.[31]

Looking ahead, the goals that seem most likely to animate Russia's uses of AI in nuclear operations could include the following:

- Increasing decision time by speeding early warning data collection, correlation, and aggregation from land, air, undersea, and space-based sensors
- Improving decision-making through information collection and analysis to aid in C2
- Pursuing air and missile defense systems to monitor, detect, and respond to attack, including with hypersonic weapons
- Improving the effectiveness of strike capabilities, including guidance systems for new, dual-capable boutique weapons

AI in PRC nuclear operations

The PRC prioritizes the development of advanced technology such as AI at the highest levels of government. In 2017, the PRC State Council released a plan outlining a three-phase strategic approach to become the world leader in AI by 2030 through investment and development of the PRC's AI sectors. The development of AI across civilian and national defense sectors is also key for the PRC to realize its goal of fully modernizing the People's Liberation Army (PLA) by 2035 and to "fully transform into a world-class military by the mid-21st century."[32]

PLA plans call for its transformation to be dominated largely by AI and autonomy, which the PLA calls "intelligent warfare."[33] PLA writers regard AI and autonomy not only as the future of warfare, but also appear to regard these technologies as an opportunity to offset the US military's technological superiority.[34] PLA sources describe conducting intelligent warfare

[31] A.A. Kokoshin, "Development prospects of the military technosphere and the future of wars and noncombat use of military force," Vestnik AVN, 2/2019.

[32] "China's National Defense in the New Era," State Council Information Office, July 24, 2019.

[33] For more detail on the PLA's concept of intelligent warfare, see Kevin Pollpeter and Amanda Kerrigan, "The PLA and Intelligent Warfare: A Preliminary Analysis," CNA, Oct. 2021, CRM-2021-U-030806-Final.

[34] Chen Dongheng, "Chen Dongheng: Exert Great Effort to Promote Military Intelligentization" (Chen Dongheng: Dali tuijin junshi zhinenghua; 陈东恒：大力推进军事智能化), Study Times (Xuexi Shibao; 学习时报), Dec. 27, 2017, http://www.71.cn/2017/1227/979861.shtml.

using "remote, precise, miniaturized and large-scale unmanned attacks" and through "intelligent swarms and cognitive control warfare."[35]

PRC academic sources generically describe the use of AI for increasing levels of detection, targeting, and striking military targets. These applications of AI are often discussed as a vulnerability for the PRC if other nations advance their own AI-enabled nuclear operations systems and the PRC does not respond with its own advances in AI applications.[36]

Yet very little is written in authoritative PLA and PRC sources on the PRC's adoption of AI into its own nuclear operations. Given the PRC leadership's apparent enthusiasm for AI, the leadership's tight control over PRC nuclear forces, and the PLA's overall drive to avoid being left behind by the US in AI development, it seems likely that the PRC will at least consider a wide range of nuclear applications for AI. However, the PRC generally lacks transparency on its nuclear weapons program, and a great deal of uncertainty remains for its plans to adopt AI into nuclear operations.

Looking ahead, the goals that seem most likely to animate the PRC's uses of AI in nuclear operations could include the following:

- Not being left behind as other countries adopt AI into their own NC3 systems
- Using AI to modernize the PRC military and "intelligentize" warfare
- Improving decision-making speed and overall C2 support
- Increasing targeting precision, including for hypersonic weapons
- Improving nuclear effects modeling and simulation

[35] You Guangrong (游光荣), "Artificial Intelligence Will Profoundly Change the Face of Warfare," (人工智能将深刻改变战争面貌), PLA Daily, Oct. 17, 2018, http://www.81.cn/jfjbmap/content/2018-10/17/content_218050.htm.

[36] Ryan Fedasiuk, "Chinese Perspectives on AI and Future Military Capabilities," Center for Security and Emerging Technology, Aug. 2020.

Nuclear Risks

To help understand ways that AI-enabled nuclear operations could increase or decrease nuclear risk, we had to define the term *nuclear risk*. We do so in this section, then lay out a typology of nuclear risk that draws on the academic literature on nuclear deterrence, strategy, and operations.

Nuclear risk defined

For this project on AI-enabled nuclear operations and nuclear risk, we define nuclear risk in two ways:

1. Risk of nuclear mission failure—that is, that an attempt to employ nuclear weapons in war would fail. This could undermine the would-be attacker's deterrent threats. Its ability to continue deterring (or extending deterrence) would be called into question, its strategy for ending the war might shift, and its opponent might be emboldened to escalate in response.
2. Escalatory risks—the risk that a conventional war could become nuclear, and the risk that a limited nuclear war could expand in geographic scope or destructiveness. This category encompasses two broad escalatory pathways: accidental or unauthorized nuclear use, and leadership decision escalation.

We acknowledge that there are other categories of nuclear risk, including arms racing, nuclear terrorism, and nuclear proliferation. However, we do not address these because they intersect with AI only obliquely.

Nuclear mission failure

Nuclear mission failure refers to attempted but unsuccessful combat employment of nuclear weapons. It could occur for any number of reasons, including technical failure of C2 systems, delivery systems, or weapons; failure in nuclear release processes and procedures; and successful enemy defenses.

Nuclear mission failure is a concern for two basic reasons. First, because (presumably) no national leader would order the use of nuclear weapons for trivial or ancillary missions. Therefore, almost by definition, much would be riding on the successful execution of a nuclear mission. Second, and relatedly, because failure of a nuclear mission would reveal to the intended target that its opponent has the desire to deal a devastating nuclear blow, but not the capability. The revelation of extreme hostile intent coupled with weakness in execution would generate strong incentives for the would-be victim to launch its own nuclear forces to disarm the would-be attacker—lest it have more luck next time.

From an AI perspective, this nuclear risk is linked with factors such as with the way AI systems, systems of AI systems, and human-AI teams function.

Escalatory risks

Accidental or unauthorized escalation

Accidental or unauthorized escalation refers to nuclear release or nuclear detonation caused by failure of the technical or procedural system(s) intended to prevent these occurrences.

Nuclear weapons are typically enmeshed in complex, tightly coupled systems. These systems—for maintenance, C3; safety, surety, and other functions—collectively represent military organizations' best attempt to resolve the "always/never dilemma:" nuclear forces must always carry out assigned missions in response to orders from national leader(s) with nuclear release authority, but they must never be employed or accidentally detonated under any other circumstances.[37] Yet because of their complexity and the often unintended impacts they can have on one another due to their tight coupling, systems of systems intended to resolve the always/never dilemma and prevent accidental or unauthorized escalation can make this outcome more likely.

Though no cases of accidental or unauthorized escalation have yet occurred, the list of near misses in both US and Russian history is uncomfortably long.[38]

From an AI perspective, the risk of accidental or unauthorized escalation is—like the risk of nuclear mission failure—linked with factors such as with the ways AI systems, systems of AI systems, and human-AI teams function.

Leadership decision escalation

Leadership decision escalation is our umbrella term for what the nuclear strategy literature terms inadvertent escalation entanglement, asymmetric escalation, and rational escalation. Inadvertent escalation and entanglement are the product of underinformed decisions by leaders to employ nuclear weapons—for example, as a result of a false belief that their

[37] Peter Feaver, *Guarding the Guardians: Civilian Control of Nuclear Weapons in the United States*, Ithaca, NY: Cornell University Press, 1992.

[38] Scott Sagan, *The Limits of Safety: Organizations, Accidents, and Nuclear Weapons,* Princeton, NJ: Princeton University Press, 1993; Eric Schlosser, *Command and Control: Nuclear Weapons, the Damascus Accident, and the Illusion of Safety*, New York: Penguin Books, 2014. It is unknown whether the PRC has had similar near-misses.

adversary is targeting their ability to C2 their nuclear forces during a conventional war.[39] Asymmetric escalation and rational escalation are the product of reasoned decisions taken by responsible leaders to employ nuclear weapons because doing so is the best (or least bad) available option.[40]

From an AI perspective, these escalation pathways are similar in that they are the result of leaders' decisions—based on good and bad information, perceptions, and misperceptions—under stressful crisis or wartime circumstances. Many AI applications are relevant to this category of escalation because they bear on the volume and quality of information leaders have and on their decision-making processes.

---

39 Barry Posen, *Inadvertent Escalation: Conventional War and Nuclear Risks*, Ithaca, NY: Cornell University Press, 1992; Caitlin Talmadge, "Would China Go Nuclear? Assessing the Risk of Chinese Nuclear Escalation in a Conventional War with the United States," *International Security* 41, no. 4 (2017): 50–92; James Acton, "Escalation Through Entanglement: How the Vulnerability of Nuclear Command and Control Systems Raises the Risks of an Inadvertent Nuclear War," *International Security* 43, no. 1 (2018): 56–99.

40 Brad Roberts, *The Case for US Nuclear Weapons in the 21st Century*, Stanford, CA: Stanford University Press, 2016; Herman Kahn, *On Escalation: Metaphors and Scenarios,* New York: Penguin Books, 1965.

Connecting AI to Nuclear Risks

Building on the typology of nuclear risk developed above, in this section, we explore how various kinds of AI applications could influence different categories of nuclear risk. To do this, we compiled insights from past CNA work, a review of existing literature on AI, nuclear operations and strategy, and ideas generated during two workshops involving experts in AI and nuclear operations.

Briefly, we found that AI-enabled nuclear operations have the potential to both raise and lower the risk of nuclear escalation in different ways and, to different degrees, across all nuclear risk pathways that we discussed. Details such as the character of the training data used, how humans interact with AI systems, how AI support shapes human behavior, and what tasks AI is (or is not) used for can all have an outsize effect on nuclear risk—for better or worse.[41] Correspondingly, we divide this section into three parts:

- How could AI increase nuclear risks?
- How could AI reduce nuclear risks?
- How could AI have an uncertain effect on nuclear risks?

[41] This project is informed by lessons from the evolution of offense-defense theory—a now largely abandoned research paradigm in international relations. The driving idea was that the risk of war varied over time based on whether the dominant military technologies of the day were better suited to offensive or defensive warfare. When offensive technologies were dominant, war was more likely. Efforts to refine offense-defense theory collapsed because of the inability to form a consensus on whether (1) specific technologies or (2) a given era's overall set of dominant military technologies favored offense or defense. For example, barbed wire is clearly useful for defense. However, it could also abet the offense by solidifying attackers' hold on captured territory, or when wrapped around a baseball bat. Against this background, the organization of this discussion reflects our assessment that AI is likely to increase nuclear risks in some ways and decrease it in others—and that its effects will be hugely dependent on the details of how exactly AI is used in nuclear operations. For more on offense-defense theory, see Sean Lynn-Jones, "Offense-Defense Theory and Its Critics," *Security Studies* 4 (Summer 1995): 660–691; Stephen Van Evera, "Offense, Defense, and the Causes of War," *International Security* 22, no. 4 (1998): 5–43; Charles Glaser and Chaim Kaufmann, "What Is the Offense-Defense Balance and Can We Measure It?" *International Security* 22, no. 4 (1998): 44–82; James Davis Jr., Bernard Finel, Stacie Goddard, Stephen Van Evera, Charles Glaser, and Chaim Kaufmann, "Correspondence: Taking Offense at Offense Defense Theory," *International Security* 23, no. 3 (1999): 179–206; Keir Lieber, "Grasping the Technological Peace: The Offense-Defense Balance and International Security," *International Security* 25, no. 1 (2000): 71–104; and Karen Ruth Adams, "Attack and Conquer? International Anarchy and the Offense-Defense-Deterrence Balance," *International Security* 28, no. 3 (2003/2004): 45–83.

How could AI increase nuclear risks?

We have identified three categories of AI challenges that could lead to increased nuclear risk in future AI-enabled nuclear operations: AI technical challenges, human factors, and leadership decision-making.

Each category of challenges is distinct but may be interconnected. For example, an AI technical challenge such as a badly performing AI system could undermine the overall performance of a system of systems critical to nuclear operations. This in turn could affect human factors, such as human trust in AI. Thus, these challenges could be mutually reinforcing, though each connects to nuclear risk in different ways. We discuss these three types of AI challenges below, tracing out the different mechanisms by which they could drive increases in the different categories of nuclear risk.

AI technical challenges

The use of AI applications in nuclear operations carries some risks that are associated with the intrinsic characteristics of AI. We identified five significant risk mechanisms: performance of specific AI systems, AI machine-machine interactions, AI training data, alignment between AI tools and tasks, and adversarial actions against AI systems.

Performance of specific AI systems

The performance of individual AI systems used for nuclear operations could drive nuclear risk by contributing to increased risk of mission failure, accidental/unauthorized use, and leadership decision escalation.

- Failure or malfunction of an AI system performing a critical function could lead to nuclear mission failure. For example, if a missile uses AI to route itself dynamically around enemy defenses, but the AI guidance system does not work properly, the result could be nuclear mission failure.
- Failure or malfunction of an AI system for weapon safety, security, or surety could lead to either mission failure or accidental/unauthorized nuclear use. For example, if a weapon storage facility's AI-enabled biometric access control malfunctioned, authorized personnel could be prevented from accessing weapons and carrying out valid orders. On the other hand, another type of malfunction of this same AI-enabled biometric access control could grant unauthorized personnel access to a secure weapons storage facility. This could increase the risk of accidental or unauthorized nuclear use.
- Failure or malfunction of a decision-support AI could also increase the risk of leadership decision escalation. For example, a decision-support AI could be designed

and trained to replicate or augment the functioning of a leader's staff. It might aggregate, sort, or present data; flag patterns; or, at higher levels of sophistication, develop options or answer questions. Faults in this category of AI systems could drive leaders to make underinformed decisions to escalate by providing them with insufficient, misleading, or false information. For example, loss of communications between a headquarters and a number of early-warning sensors could be the result of a technical issue or an attack. If an AI designed and trained for early warning erroneously flagged a communications loss as a likely attack, a leader might choose to escalate.

AI machine-machine interactions

The overall performance of an AI-enabled nuclear force could increase nuclear risk as a result of interactions among complex, tightly coupled AI-enabled systems. Commonly known as "machine-machine interactions," these could produce unanticipated or emergent outcomes resulting in increased risk of mission failure, accidental/unauthorized use, or leadership decision escalation.[42]

- Interactions among the components of a complex, tightly coupled system of AI-enabled systems being used for nuclear operations could increase the risk of nuclear mission failure. Individual AI systems sometimes fail or perform in unexpected ways. At a broader level, it is possible to imagine that if an individual AI system fails or performs in unanticipated ways, and then interfaces with one or more other AI systems, the result could be a cascade of unexpected and undesirable outcomes. For example, if an AI designed to aggregate pattern-of-life data on enemy air defenses malfunctioned, but its outputs fed into a bomber's route planning AI, the result could be nuclear mission failure. The use of AI systems could introduces pathways to mission failure that do not exist without AI.
- Similarly, interactions among AI-enabled nuclear operations systems could lead to accidental or unauthorized nuclear use. For example, a state might use an AI to support continuity of nuclear C2. An AI system might grant nuclear launch authority to the highest living member of the nuclear chain of command who could still communicate with deployed forces. If this system malfunctioned, and if the state also had an AI-enabled system to automate nuclear launch-order dissemination, the result could be unauthorized nuclear use with little time to stop the order.
- Interactions among different early-warning AIs could also result in leadership decisions to escalate due to misperception. For example, if an AI designed to recognize

[42] See, for example, Sagan, *The Limits of Safety*; Perrow, *Normal Accidents*; Charles Perrow, *Normal Accidents: Living with High-Risk Technologies*, Princeton, NJ: Princeton University Press, 1999.

changes in the pattern of adversary nuclear force movements (mis)attributed outsize importance to routine or predictable fluctuations in the underlying data, and its outputs contributed to an AI designed to aggregate information and provide leaders with strategic early warning, the result could support an underinformed leadership decision to use nuclear weapons.

AI training data

Poor-quality or inappropriate AI training data could increase the risk of nuclear mission failure and nuclear escalation. The central issue is that AI systems used in nuclear operations will be intended for use in competition, crisis, and war. However, because crises and wars are rare (and typically sui generis), the bulk of data available for training AIs will reflect only the competition environment. Thus, AIs used in nuclear operations may not be trained properly for all of the circumstances in which they will be expected to perform.

- AI systems that rely on training data from competition may contribute to nuclear mission failure. For example, a missile guidance AI designed to ensure that the weapon reaches its target might be trained on data reflecting the enemy's peacetime defenses as well as its anticipated wartime defenses. If the enemy's actual wartime defensive systems and tactics do not align with either the peacetime or anticipated wartime defense training data, the AI could be unable to recognize the divergence and incapable of adapting to the new situation. As a result, the enemy's surprising or innovative defenses could succeed, causing nuclear mission failure.
- AI trained on data from competition could contribute to leadership decision escalation as well. This is particularly the case for AI early-warning and decision-support systems. The basic logic is that a given action can mean very different things and warrant very different responses in peacetime, crisis, and war. For example, a decision-support AI could be trained to recognize that a massive cyberattack could warrant a nuclear response. However, in the context of a major war with thousands of casualties on both sides, a cyberattack (as opposed to a kinetic strike) could actually be a step toward de-escalation. An AI trained on peacetime data might fail to recognize this, inappropriately recommending a nuclear response. To the extent leaders relied on AI decision support, this could increase the risk of an underinformed leadership decision to escalate.

Alignment between AI tools and tasks

AI systems can be powerful, but they are not always the best solution. Contemporary AI systems are intrinsically narrow and brittle: while some highly structured tasks are a perfect fit for AI (such as image recognition), other tasks are too complex or cannot be distilled into a form that AI can solve.[43] Trying to force such an AI application to a nonoptimal task can lead to unreliable, inaccurate, or otherwise suboptimal results. If this were done within nuclear operations, a poor alignment between AI tools and the tasks they are intended to perform could increase the risk of nuclear mission failure, accidental or unauthorized nuclear use, or leadership decision escalation.

Adversary action against AI systems

Using AI for nuclear operations could open attack vectors that do not exist for non–AI-enabled nuclear operations. Adversary exploitation of these new attack vectors could increase the risk of nuclear mission failure, accidental or unauthorized nuclear use, and leadership decision escalation.

- Adversary manipulation of AI training data could cause AI systems to malfunction or operate in unexpected ways. For example, adversary manipulation of training data for a weapon system could cause nuclear mission failure. Manipulation of training data for safety/security/surety could permit accidental or unauthorized nuclear use. Adversary manipulation of training data for decision-support or early-warning systems could plausibly induce leadership decision escalation.

Human-factors challenges

Even though they can rely on advanced technologies, nuclear operations are ultimately a human endeavor. They involve human decisions. They require specific skills and expertise. They turn on perception of threats and contexts. They require effective communication. When humans interact with AI systems, these interactions can create risks of their own, apart from those involved in the performance of the AI system itself. Here, we identify four significant human-factors risks associated with the use of AI in nuclear operations: human trust in AI, skill in use of AI, effect on human skills, and decision time compression.

Human trust in AI

Human trust in AI systems can increase nuclear risks whenever humans place too much or too little trust in them. This is especially the case for AI systems used in a wide variety of applications, ranging from simple automation or data aggregation to more sophisticated analysis and decision support.

- AI systems used for automation or routine functions like pattern recognition or data aggregation can contribute to nuclear mission failure if humans place too much or too little trust in them. For example, if humans mistrust a correctly aggregated common

[43] Note that while this is the case in contemporary AI systems, the general aim of AI researchers is to develop more flexible, broadly usable AI systems. If they succeed, this technical challenge may become less relevant.

operational picture (COP) of a battlespace, or trust an incorrectly aggregated COP, they might make poor tactical choices that could lead to nuclear mission failure.

- Similarly, if human security guards come to trust an AI that grants or denies access to nuclear weapon storage facilities on the basis of facial or other biometric pattern recognition, and that AI fails or underperforms, unauthorized individuals could be given access to nuclear weapons, increasing the risk of accidental or unauthorized use.
- Over-/under-trusting AI for analysis or decision support could also increase the risk of leadership decision escalation. For example, a leader might trust an AI-generated analysis of alternative courses of action (COAs). However, even a well-trained, properly functioning AI could lack the human experience, subjectivity, and creativity that might be necessary for a good COA assessment under many circumstances. In this case, the leader's trust in the AI would be too great, which could lead to a misguided decision to escalate.

Skill in use of AI

AI systems are tools designed to be employed in specific ways to carry out specific tasks. When human operators are unskilled in the use of AI or attempt to use an AI system for a purpose other than what it was designed and trained for, they could increase the risk of nuclear mission failure, accidental or unauthorized nuclear use, or leadership decision escalation.

- Human operators may employ AI systems clumsily in ways that lead to unintended outcomes or undesirable responses from the AI. For example, a planner may direct an AI system to maximize the probability of destroying a given target with a given weapon or set of weapons. This instruction, absent any additional constraints or restraints, could generate a cloud of dust and fallout that would interfere with other nuclear missions aimed at nearby targets. The result would be an AI-generated mission plan that would succeed on its own, while causing other nuclear missions to fail.
- Similarly, a leader could frame a request for AI analysis or decision support in a way that contributes to an uninformed decision to escalate. For example, a leader might ask an AI whether there was "evidence to suggest that an enemy nuclear attack was likely." If the AI interpreted "likely" to mean greater than 50 percent probability, it might give an affirmative answer. However, the leader might interpret the word "likely" differently and come away with the belief that the probability of enemy nuclear attack was higher than the AI's actual assessment. This misunderstanding between a human using loose language and an AI that operates on precision could increase the risk of escalation due to a leader's decision-making.

Effect on human skills

Reliance on AI can increase the risk of nuclear mission failure or accidental/unauthorized use and escalation as a result of leadership decision-making by degrading the skills of human operators.

- If human operators use an AI on a regular basis over a protracted period of time, they may cease to cast a critical eye on the outputs or results that their AI produces. They may become unable to identify malfunctions or unexpected performance unless they are very obvious. Overlooking these AI failures could result in nuclear mission failure, accidental or unauthorized use, or (if the AI user is a national leader) a decision to escalate rooted in misperception.[44]
- Similarly, habitual reliance on AI for nuclear decision-making support could lead to skill atrophy in this area. For example, a leader's staff may struggle to gather and analyze relevant data to support decision-making if they have come to rely on AI systems for this work. This could contribute to a leader's decision to use nuclear weapons based on incomplete or imperfect information.
- Reliance on AI could also cause atrophy in skills and characteristics like creativity, intuition, and self-confidence. This is critical because the practice of deterrence and war is innately human. Leaders need human skills and characteristics to navigate crises and (ideally) avoid nuclear escalation. For example, if leaders' and their staffs' creative thinking skills have atrophied as a result of habitual reliance on AI option generation, they might choose to employ nuclear weapons because of their inability to find a better, more creative option.

Decision time compression

Some AI applications could reduce the amount of time that leaders have available for decision-making. If one side in a competition fields AI systems to speed information processing, decision-making, and decision execution, it could gain an advantage. This advantage could be especially meaningful in crises and wars, when fast, correct action can mean the difference between victory and defeat. Thus, it is reasonable to expect that the US, Russia, and China will all seek to capture the advantages of expedited, AI-enabled decision-making. However, the net effect of all three competitors' pursuit of these advantages could be a downward spiral in the

[44] This concept is related to human trust in AI, but we distinguish between baseline trust in AI and the perishable skill of continuously monitoring AI system performance.

time available for leadership decision-making. This dynamic, coupled with other AI challenges, could increase the risk that a leader may choose to escalate in haste.[45]

- If the use of AI increases the tempo of future conflicts, national leaders may make hasty decisions based on incomplete information. For example, if a leader received word that an attack on a nuclear base was underway, and if the leader believed that with AI-enabled cyber and kinetic weapons, the adversary had the ability to disarm the leader's defenses within minutes, the leader might assume the worst and choose a nuclear response—even before knowing whether the attack extended beyond a single nuclear base.
- Similarly, if AI increases the tempo of future conflicts, national leaders may reason that nuclear use is the least bad available option under some circumstances. For instance, in a rapidly escalating conventional conflict, leaders may believe that the risk of adversary nuclear use is growing. In that case, they could judge that striking enemy nuclear forces first is far preferable to absorbing an undegraded nuclear attack. Their judgment could be aided by advanced AI-enabled nuclear capabilities that could increase the efficacy and reduce the collateral damage from their strike.[46]

Risks from leader calculus

AI and the military balance

Use of AI for nuclear operations also has the potential to increase the risk of nuclear mission failure or escalation by altering the actual or perceived balance of military power among nuclear-armed states. This is because the balance of military power is a powerful driver of leaders' decisions to wage war or to escalate an ongoing war.[47] The introduction of AI capabilities could have a significant effect on military effectiveness, which could change the

[45] For a historical example of how technology-driven decision time compression caused dramatic change in early US nuclear policy, see Edward Kaplan, *To Kill Nations: American Strategy in the Air-Atomic Age and the Rise of Mutually Assured Destruction,* Ithaca, NY: Cornell University Press, 2020. According to Kaplan, the transition from the reliance on bombers to deliver nuclear ordnance to intercontinental-range missiles reduced the amount of time—from several hours to roughly 20 minutes—leaders would have between learning of an enemy attack in progress and having to decide how to respond. The advent of AI-enabled nuclear operations—possibly including AI-enabled hypersonic weapons—could reduce this decision-making time even further. For compounding risks, see Marina Favaro and Elke Schwarz, "Human Augmentation and Nuclear Risk: The Value of a Few Seconds," *Arms Control Today*, Mar. 2022, https://www.armscontrol.org/act/2022-03/features/human-augmentation-nuclear-risk-value-few-seconds.

[46] Michael C. Horowitz, "When Speed Kills: Lethal Autonomous Weapon Systems, Deterrence and Stability," *Journal of Strategic Studies* 42, no. 6 (2019); Durkalec et al., *Nuclear Decision-Making, Complexity, and Emerging and Disruptive Technologies.*

[47] Specific ways that AI could affect nuclear risk by conferring advantage to one side are explored further in the section below on other AI applications and nuclear risk.

actual balance of power. The use of AI can also increase the opacity of military power, since AI is software that can increase or decrease capabilities in ways that are difficult to observe or measure. Thus, AI both changes the balance of military capabilities and increases the uncertainty about that balance.

- AI capabilities could alter the military balance enough to make nuclear attack advantageous to one side. This could happen if AI conferred impressive capabilities on the attacker's nuclear forces. It could also happen if the use of AI made the prospective victim's nuclear or other military forces vulnerable by offering a new or enlarged attack surface. Either way, AI could alter the nuclear balance of power enough to increase the likelihood of a leadership decision to escalate.
- A large gap in the nuclear capabilities of AI haves and have-nots could also increase the risk escalation by leadership decision as well as accidental or unauthorized use. Responding to their own weakness, AI have-nots could adopt an asymmetric escalation posture. This would effectively spring-load their nuclear forces by leaving lower-level commanders with little choice but to use nuclear weapons in case of attack. On one hand, adopting such a posture would be a reasoned choice by national leaders well in advance to escalate, conditional on being attacked; this would raise the risk of nuclear escalation as a result of conventional war. This kind of spring-loaded nuclear posture could also be more prone to the risk of accidental or unauthorized nuclear use. On the other hand, these risks, if well understood by all sides, could also induce cautious behavior all around, paradoxically reducing nuclear risks.[48]
- Leaders may also choose to employ nuclear weapons due to a false belief that they can gain some advantage in doing so. The balance of military capabilities between two or more states is always difficult to assess. This is the case even when the main markers of military power—the number and quality of tanks or the training of ships crews—are readily observable. If AI becomes important to nuclear operations and thus a driver of the nuclear balance of power, leaders may find it increasingly difficult to assess that balance of power. That is because it is difficult for outsiders to evaluate how well AI performs or how effectively human-machine teams operate. This could allow leaders on one side of a conflict to falsely believe that their AI-enabled nuclear forces are superior to their opponent's and that they could advance their national objectives with a nuclear attack. This would be an example of a leadership decision to escalate rooted in misperception.

[48] Vipin Narang, *Nuclear Strategy in the Modern Era: Regional Powers and International Conflict*, Princeton, NJ: Princeton University Press, 2014.

How could AI reduce nuclear risks?

In addition to exploring how AI challenges could drive nuclear risks, we also synthesized the existing literature, workshop discussions, and additional analysis to identify opportunities to use AI to mitigate nuclear risks. Specifically, we identified four potential AI applications that could reduce the risk of nuclear mission failure or escalation: nuclear weapon surety, survivability and resilience of nuclear forces, decision time expansion, and crisis/conflict de-escalation.

Like the AI challenges discussed above, these opportunities are distinct but related, and potentially mutually reinforcing. For example, using AI to make the force more survivable or resilient could expand leaders' decision-making time.

In many cases, capturing these opportunities requires first overcoming some of the AI-related challenges that this report has highlighted. Poor-quality training data, human-skills degradation, inappropriate trust in AI, and other challenges could undermine efforts to capture many of the risk-reducing benefits we highlight. If poorly implemented, efforts to pursue these applications could backfire, inadvertently increasing nuclear risk instead of reducing it.

Nuclear weapon surety

AI tools can help enhance nuclear weapons' surety—that is, their safety, security, and the guarantee that they remain under authorized leaders' positive control.[49] Practical steps in this direction include preventing accidents involving nuclear yield and preventing unauthorized access to or detonation of the weapons systems. All are vital to managing both sides of the "always/never" dilemma. According to this framework, to deter, nuclear weapons must always be employed and must function in response to valid orders from authorized leaders—but must never be employed or detonate under any other conditions.[50] AI applications to enhance nuclear surety could reduce nuclear risk in three main ways:

- AI-enhanced supply chain monitoring could identify potential manufacturing issues and security concerns in the production of nuclear weapons, delivery systems, and storage facility equipment. For example, such defects might include a compromised microelectronic component for a security checkpoint system, a component that was unknowingly sourced from restricted suppliers, an exploitable software package for an

[49] Deputy Assistant Secretary of Defense for Nuclear Matters (DASD(NM)), *Nuclear Matters Handbook 2020 (Revised),* Office of the Secretary of Defense, 2020, https://www.acq.osd.mil/ncbdp/nm//NMHB2020rev/index.html, pp. 124–125.

[50] DASD(NM), *Nuclear Matters Handbook 2020 (Revised)*, pp. 124–125; Peter Feaver, "Command and Control in Emerging Nuclear Nations," *International Security* 17, no. 3 (Winter 1992-1993), pp. 160–187.

early-warning satellite, or a fuse that is incorrectly calibrated.[51] AI tools could identify these defects earlier and with greater accuracy than traditional supply chain monitoring systems. This could allow for a higher degree of confidence in all aspects of weapon surety, reducing the risks of nuclear mission failure or accidental/unauthorized use.

- AI modeling could help reduce the risk that nuclear weapons are exposed to abnormal environments during routine handling and maintenance and could reduce the risk of nuclear yield when weapons are exposed to abnormal environments. Abnormal environments are the set of circumstances where a nuclear weapon is neither expected nor intended to detonate and could include scenarios such as natural disasters, lightning strikes, vehicle or aircraft accidents, or strike by a conventional or nuclear weapon.[52] AI-enabled modeling of routine handling and maintenance, coupled with use control features and permissive action links (PALs) designed to better distinguish normal and abnormal environments, could help to reduce the risk of accidental/unauthorized detonation.[53]
- AI tools could increase nuclear security by ensuring that only authorized personnel are able to access and/or launch the weapons. Such measures could include enhanced multifactor and biometric access points, algorithms to detect unusual patterns in and around nuclear storage facilities, autonomous patrol units, and AI-enabled insider threat monitoring tools designed to flag abnormal trends and potential threats.[54] Such measures could reduce the risk of accidental or unauthorized use.

Survivability and resilience of nuclear forces

Concern about the possible vulnerability of formerly secure second-strike capabilities due to AI-enabled advances in precision, target tracking, and identification are reasonable, but AI also offers a variety of potential opportunities to enhance the survivability of nuclear assets during a time of crisis or war. Moreover, in war, when some systems and resources may be destroyed, damaged, or overwhelmed, it is important that crucial functions such as NC3 systems, which receive, relay, and execute nuclear orders, are quickly restored. Here, AI-enabled tools can also

[51] Lee Hudson, "Pentagon Suspends F-35 Deliveries after Discovering Materials from China," Politico, Sep. 7, 2022, https://www.politico.com/news/2022/09/07/pentagon-suspends-f-35-deliveries-china-00055202; Valerie Insinna, "F-35 Deliveries Suspended after Finding Chinese Alloys in Magnets," Breaking Defense, Sep. 7, 2022, https://breakingdefense.com/2022/09/f-35-deliveries-suspended-after-finding-chinese-alloys-in-magnets/.

[52] DASD(NM), *Nuclear Matters Handbook 2020 (Revised),* p. 126.

[53] Donald R. Cotter, "Peacetime Operations," in Ashton B. Carter, John D. Steinbruner, and Charles A. Zraket, eds., *Managing Nuclear Operations*, Washington, DC: Brookings Institution Press, 1987, pp. 42–51.

[54] Johnson, "AI, Autonomy, and the Risk of Nuclear War."

be of use, contributing to overall network resilience. There are four primary opportunities for AI to reduce nuclear risk by fortifying nuclear assets against attack:

- AI-enabled measures could enhance concealment of second-strike weapons, increasing their survivability in time of crisis or war. These could include AI tactics designed evade detection, move or conceal weapons, introduce decoys, interfere with adversary signal intelligence, or other AI-enabled active defenses that protect second-strike capability.[55] Such measures may reduce the risk of mission failure and leadership decisions to escalate to the nuclear level.
- AI-enabled network monitoring tools could improve the security of NC3 systems against cyberattack. AI can provide more thorough and comprehensive data analysis than humans and faster responses to potential attacks. These attributes could support faster vulnerability identification, software patching, network anomaly detection, user behavior monitoring, threat flagging, and triage of incidents/system errors. By making critical NC3-relevant systems more resilient and reliable, such improvements could reduce the chance of nuclear mission failure and leadership decisions to escalate.
- AI network monitoring tools could improve NC3 system resilience in conventional wartime or in trans-nuclear environments. For example, in the event that a portion of the satellite constellations for early warning or communications has been rendered unusable by an adversary, AI algorithms and network monitoring tools could identify and connect with available stand-in capabilities from domestic military, commercial, or allied systems to restore coverage and function in as little time as possible. Alternatively, swarm micro-satellites could maneuver together to reinstate a compromised NC3 capability. Such tools would help ensure that seamless, reliable NC3 capabilities are available at all times and reduce all categories of nuclear risk.
- AI decision-support tools could increase the capabilities and capacity of smaller dispersed battle staffs to carry out more efficiently diverse and complex tasks associated with retaining NC3 functions and overseeing continuity of operation plans during a crisis or following enemy attack. By providing battle staffs (e.g., embarked aboard aircraft) with better information and analysis and helping them make better decisions, such applications could reduce the risk that leaders would make hasty or underinformed decisions to escalate.

[55] Gottemoeller, "The Standstill Conundrum."

Decision time expansion

If Russia or China launched ICBMs against the United States, or vice versa, the target nation's leadership would have roughly 30 minutes to select and execute its immediate response before warheads started to detonate.[56] In this short window of time, the incoming attack would have to be characterized and described to the target nation's leader(s). They would then confer with high-ranking advisors to consider various sets of options, issuing orders that, from the time they are received, would take 5 to 15 minutes to execute.[57]

AI tools could reduce nuclear risk by increasing the warning time available to nuclear decision-makers in the event of a nuclear strike and/or reducing the time it takes to pass orders through the chain of command. Both approaches would allow for less hurried decision-making. Also, AI-enabled tools could aid in the decision-making process itself. These types of AI innovations would increase the chances that (1) leaders will have the time and information necessary to make reasoned decisions, and (2) that their orders can be carried out while there is time. There are five key ways AI tools can reduce nuclear risk:

- AI tools could improve states' strategic and tactical early-warning capabilities. They have the potential to help monitor a wide range of adversaries' nuclear-related activities, including construction of new facilities, unusual movement of vehicles around warehouses or other nuclear facilities, or abnormal concentrations or dispersal of key military personnel and equipment.[58] Specifically, AI could increase the scope, fidelity, and persistence of monitoring and could help flag important changes for humans more promptly.[59] AI-enabled technologies such as ubiquitous sensing, cloud computing, and big-data analysis can simultaneously mine and assess larger quantities of data at more granular levels to better identify trends and abnormalities, potentially providing prompter or more accurate tactical and strategic warnings that an adversary

[56] United States Senate, Committee on Foreign Relations, Senate Hearing 115-439: "Authority to Order the Use of Nuclear Weapons," Nov. 14, 2017, https://www.govinfo.gov/content/pkg/CHRG-115shrg34311/html/CHRG-115shrg34311.htm.

[57] In some instances, adversary submarine-launched missiles could take much less time to strike. See Bruce Blair, *Strategic Command and Control,* Washington DC: Brookings Institution Press, 1985; Marina Favaro and Elke Schwarz, "Human Augmentation and Nuclear Risk: The Value of a Few Seconds," *Arms Control Today*, Mar. 2022, https://www.armscontrol.org/act/2022-03/features/human-augmentation-nuclear-risk-value-few-seconds.

[58] Vaynman, "Better Monitoring and Better Spying."

[59] To borrow a historical example, at the start of the Cuban Missile Crisis there was a lag of at least 36 hours between the time a U2 aircraft photographed Soviet forces on Cuba and analysts received the film, processed it, reviewed it, interpreted what they saw (in part, by using a rudimentary room-size computer to estimate missile lengths from photographs), and alerted senior government officials. An AI system that could shrink this time lag might have been useful. See Michael Dobbs, *One Minute to Midnight: Kennedy, Khrushchev, and Castro on the Brink of Nuclear War,* New York: Vintage Books, 2009, p. 4.

is preparing an attack.[60] Such tools, if effective, could reduce the risk of leadership decisions to escalate by strengthening deterrence and preventing surprise.[61]

- AI tools could also support the nuclear decision-making process during a nuclear attack by providing better attack assessment, generating options for decision-makers, and more quickly and thoroughly evaluating the trade-offs of these options, including considerations such as risk, feasibility, chances of collateral damage, and potential adversary responses. Such tools to help decision-makers may reduce the risks of underinformed escalation.
- AI-based automation tools, such as advanced communications systems that rapidly disseminate launch orders from leaders to crews directly and/or expedite the order-validation process, could shrink time between employment decision and mission execution.[62] Such tools could expand the time available for leaders to make weighty decisions, thereby reducing the risks of underinformed and rational escalation.
- AI tools could bolster the survivability resilience of nuclear launch platforms and communication systems, making it more likely that they could endure following a nuclear attack. This would reduce leaders' incentives to use their nuclear forces in case of actual or suspected massive nuclear attack for fear of losing them.[63] Such tools would reduce the risks of a leadership decision to escalate driven by the use-them-or-lose-them dilemma.

Crisis/conflict de-escalation

In the event that a crisis escalates between two nuclear powers and conventional or nuclear war breaks out, there may be a desire to prevent further intensification of the conflict. This can be challenging, as fears, motives, stakes, and red lines between the two (or more) adversaries do not always neatly align and the fog of war is thick. Even if both sides seek de-escalation, credibly signaling this desire during crisis or war can be difficult. There are a number of ways AI could aid in avoiding further escalation or in helping leaders identify and pursue de-escalatory off-ramps.

- AI systems could better identify unintended escalation risks by highlighting overlaps in doctrine/standard operating procedure between red and blue. For example, such AI

[60] Johnson, "AI, Autonomy, and the Risk of Nuclear War."

[61] These capabilities also have applications for nuclear arms control verification; see Vaynman, "Better Monitoring and Better Spying."

[62] Favaro and Schwarz, "Human Augmentation and Nuclear Risk."

[63] Johnson, "AI, Autonomy, and the Risk of Nuclear War."

systems could identify instances in which routine blue actions such as missile tests, exercises, or reconnaissance flights could cross the opponent's escalatory red lines in the context of a crisis or war. A tool like this could prevent possible clashes between adversaries before they happen, or more fully inform leadership of the potential risks of different options ahead of time. These tools would reduce the risk that one state could inadvertently provoke its opponent into choosing escalation.

- AI-enabled support tools that generate options for decision-makers could be designed or trained with reinforcement learning to avoid conflict escalation. History suggests that such a capability could be useful. For example, during the Cuban Missile Crisis, President Kennedy was surrounded by advisors whose recommendations, if followed, would have led to nuclear war. US Ambassador to the UN Adlai Stevenson and, to a lesser extent, Under Secretary of State for Economic Affairs George Ball were the exceptions. Their arguments against military action in Cuba carried the day and helped to avert a potential nuclear war.[64] In future crises, there is no reason to assume that opponents of escalation would be in the room, stubborn, and sharp enough (as both Stevenson and Ball were) to make strong arguments in the face of overwhelming opposition. Given this history, letting an AI put a proverbial thumb on the scale in favor of de-escalation could be valuable.

How could AI have an uncertain impact on nuclear risks?

In addition to challenges and opportunities that could emerge from the use of AI in nuclear operations, we also identified five AI applications that could have an uncertain effect on nuclear risk. These applications all involve using AI to gain some military benefit or advantage that could in turn affect nuclear risk. The magnitude and direction of these effects would likely depend on the interplay of three related factors:

1. *The details of how, and how effectively, AI is applied to a given problem.* For example, as discussed above, low-quality AI training data leading to poor AI performance, in combination with human-skills degradation, could mean that AI in a particular application is more of a liability than a benefit—even if it is intended to confer an advantage.
2. *The net effect of AI-enabled nuclear competition on the balance of power, and how leaders perceive that balance.* Escalatory and mission failure risks are very different in

[64] Martin J. Sherwin, *Gambling With Armageddon: Nuclear Roulette from Hiroshima to the Cuban Missile Crisis,* New York: Vintage Books, 2022.

a world where the US, Russia, and China all have AI-enabled nuclear forces but remain confident in their secure second-strike capabilities than in a world where one country has or believes it has a first-strike advantage. If all three sides retain a secure second strike against the other two, the risk of nuclear escalation would remain low.[65] However, if one country gained a nuclear edge over others through the use of AI, that country could use its advantage in an attempt to impose its will on the others. That kind of behavior could increase the risk of conflict and nuclear escalation.

3. *The way that new, revolutionary military technologies affect states' foreign policy objectives.* For example, new capabilities might embolden some states, while making others more confident in their security, encouraging their restraint.[66]

On balance, states seem very likely to pursue these nuclear advantage-seeking applications of AI.[67] At the same time, their effects on nuclear risk remain very uncertain.

Operations and maintenance

One way that states might attempt to improve their nuclear capabilities is by using AI to make operations and maintenance more efficient and potentially safer.

- At the basic level, AI modeling could support predictive maintenance. Parts of nuclear weapons or delivery systems could be repaired or replaced just before they fail. That would reduce the risk of mission failure.
- Moreover, at the level of the overall force, AI-enabled predictive maintenance, coupled with AI-supported tools, could help get the most use out of maintenance downtime. This would reduce the percentage of time that weapons and delivery systems spend in maintenance. This would increase their availability for use, incrementally increase

---

[65] Here, we bracket a discussion of how tripolar nuclear competition could add complexity to the requirements for a secure second strike.

[66] For discussion of the concept outside the AI context, see Mark S. Bell, "Beyond Emboldenment: How Acquiring Nuclear Weapons can Change Foreign Policy," *International Security* 40, no. 1 (Summer 2015), pp. 87–119.

[67] For states as security maximizers, including the nuclear realm, see John Mearsheimer, *The Tragedy of Great Power Politics*, New York: W.W. Norton & Co., 2014. For the counterargument that even modest nuclear capabilities can revolutionize competitive international politics by ensuring state security, see Robert Jervis, *The Meaning of the Nuclear Revolution: Statecraft and the Prospect of Armageddon*, Ithaca, NY: Cornell University Press, 1990, and Charlie Glaser, *Analyzing Strategic Nuclear Policy*, Princeton, NJ: Princeton University Press, 1990. For detailed documentation of US officials' persistent rejection of this position, see Brendan Green, *The Revolution that Failed: Nuclear Competition, Arms Control, and the Cold War*, New York: Cambridge University Press, 2020. For bureaucratic, economic, and technical explanations for states' persistent pursuit of increasingly capable nuclear forces, see Donald MacKenzie, *Inventing Accuracy: A Historical Sociology of Nuclear Missile Guidance*, Cambridge, MA: MIT Press, 1993; Ted Greenwood, *Making the MIRV: A Study of Defense Decision-Making*, Pensacola, FL: Ballinger Publishing Co., 1975; and Steven J. Zaloga, *The Kremlin's Nuclear Sword: The Rise and Fall of Russia's Strategic Nuclear Forces, 1945–2000*, Washington, DC: Smithsonian Institution Press, 2002.

the force's readiness and capabilities, reduce the risk of mission failure and have uncertain affect on the risk of leadership decision escalation..

Performance of non-nuclear forces

AI could improve the performance of non-nuclear forces in any number of ways. These could include providing enhancements for such ordinary military functions as training, logistics, planning, ISR, targeting, and C2. Potential AI applications could also include performance enhancements for non-kinetic weapons and information warfare. A full exploration of all the ways AI could improve non-nuclear mission performance is beyond the scope of this study; however, the general category of AI applications to enhance non-nuclear forces seems likely to impact the risks of leadership decisions to escalate in two fundamental ways:

- AI-enabled non-nuclear forces could give a state the ability to threaten its rival existentially without resorting to nuclear weapons. For example, a concerted attack by highly capable AI-enabled conventional forces, coupled with AI-supported cyberattacks on critical infrastructure, and AI-generated disinformation, including deepfake video and audio of key leaders, could constitute an existential threat, even to a great power. While conventional, cyber, and disinformation attacks generally would not warrant a nuclear response, that could change if they were undertaken together and were sufficiently effective. Such attacks could cause a leader to choose escalation in the fog of war. Alternatively, well-informed leaders could correctly assess that the non-nuclear AI-enabled combined arms onslaught they were facing was in fact an existential threat and could make a rational decision to escalate to the nuclear level.
- Similarly, AI-enabled non-nuclear forces could be used to generate effects that would otherwise require nuclear forces. For example, one way to increase the odds of destroying enemy mobile nuclear missile launcher trucks is to launch a nuclear barrage against the areas where the launchers are believed to patrol; such a barrage could require many nuclear warheads. Alternatively, AI-enabled conventional forces could combine enhanced ISR with improved target recognition and terminal guidance to obviate the need for nuclear barrage attacks. Conventional missiles could carry out missions that formerly required nuclear weapons. If such attacks were effective, the leaders of the target state could be driven to choose nuclear escalation in response.

Performance of nuclear forces

AI could also improve the performance of states' nuclear forces. As in the case of non-nuclear force enhancements, these AI-driven improvements to nuclear forces could center on mundane but vital military functions like training and logistics, as well as nuclear-specific applications.

- States could use AI to enable nuclear employment with little or no fallout and with minimal collateral damage. For example, AI-enabled modeling of weapons effects on specific targets could give targeters confidence that the desired level of destruction could be achieved with lower yields and/or higher burst heights. Similarly, AI target recognition for terminal guidance could increase warhead accuracy, further reducing yield required and fallout generated. These and other approaches to reducing the consequences of nuclear use could make nuclear weapons more usable from the leader's perspective, increasing the risk of nuclear escalation. If these AI harm-reduction tools do not work as designed, they could increase the risk of mission failure.
- Similarly, states could use AI in any number of ways in an attempt to improve the odds that their nuclear missions, if ordered, succeed. Should those AI applications fail to work as intended, these attempts could backfire, increasing the likelihood of mission failure. In addition, they could increase leaders' confidence in the capabilities of their AI-enabled nuclear forces. Under certain circumstances, this could lead them to conclude (correctly or falsely) that nuclear use is the best available option—an example of escalation by leadership decision.

Analytics, planning, and decision support

Beyond improving the military capabilities of conventional and nuclear forces, AI could be used to help leaders wield these forces more effectively as they pursue political ends. These applications could shape leaders' decisions about whether to escalate to nuclear use.

- States use their nuclear forces to deter adversaries with the threat to destroy things that they value. AI-enabled analysis could be used to clarify what different adversary leaders value, for example, by identifying hidden patterns in their behavior. AI could also be used to develop or model novel ways of threatening things that adversary leaders value. Both applications of AI could help countries tailor their deterrent threats to align more closely with adversary values. They could help leaders make choices about whether and how to choose to escalate to the nuclear level.
- AI simulation and training tools could also be used to help train leaders and their staffs to make decisions during crises and war. Advanced, realistic simulations could help leaders and staffs practice making difficult choices during high-stress situations. To the extent that they give trainees/players the ability to make choices in private, they could also help them explore a wider range of options (especially for nuclear use) without incurring the potential reputational costs that are a perennial challenge in

nuclear wargaming.[68] As with other AI analytics, planning, and decision-support applications, AI for simulation and training could either increase or decrease the risk that leaders will choose escalation.

Active air and missile defenses

One likely application of AI is to improve the effectiveness of active air and missile defenses. This application would leverage AI technology's strengths in the fields of automation and pattern recognition. Yet while improving defenses may appear benign, in the context of a conventional war or nuclear crisis, quality defenses could increase the risk of underinformed or reasoned escalation.[69]

- Effective defenses could reduce the consequences of nuclear use for states that possess them. Leaders whose defenses reduce or eliminate their fear of nuclear retaliation could be emboldened to use nuclear weapons to achieve their goals in crisis or war.
- Reciprocally, if leaders falsely believe that their own or their opponents' AI-enabled defenses are effective, they could choose to escalate based on misperception. The possessors of ineffective defenses could incorrectly believe that they could use nuclear weapons with impunity. This overestimation of the efficacy of AI-enabled defenses could support a decision to use nuclear weapons.

[68] Reid Barret Charles Pauly, "Would US Leaders Push the Button? Wargames and the Sources of Nuclear Restraint," *International Security* 43, no. 2 (Fall 2018): 151–192.

[69] Charlie Glaser, "Why Even Good Defenses May Be Bad," *International Security* 9, no. 2 (1984): 92–123.

Conclusions and Recommendations

In this project, we developed an understanding of how the US, Russia and China have used, or are using AI in their nuclear operations. We built on this effort to look ahead to what kinds of AI-enabled nuclear forces these countries might field in approximately 2035. Finally, we used this thought experiment to trace how these different AI applications to nuclear operations could increase, reduce, or have an uncertain effect on future nuclear risks.

The main risks we highlighted are rooted in AI's technical characteristics and vulnerabilities; human factors associated with human-machine teaming (HMT); and how leadership decision-making will be affected by AI's effect on the perceived and actual balance of power. This array of risks is broad and complex, reflecting the following:

- The wide variety of roles and functions AI can play within nuclear operations
- The need to navigate the strengths and vulnerabilities of AI, neither of which are yet fully understood
- The many aspects of effective HMT and trust
- The increased opacity of AI-enabled capabilities and their effect on nuclear deterrence, which is, in turn, based on perceptions of capabilities and intent
- The current and relatively immature state of the capabilities and infrastructure that militaries require to use AI effectively and safely

Recommendations

How can nuclear powers avoid bad outcomes and bring about good ones with regard to AI and nuclear operations? We identified three sets of steps that can promote the desirable nuclear risk-reducing benefits of AI-enabled nuclear operations and mitigate risks. These steps are nested, reflecting the fact that AI applications in the nuclear niche will be shaped by applications in military applications more broadly, as well as in the non-military AI ecosystem. Specifically, we propose the following:

- ***Focused risk mitigation for AI applications in nuclear operations.*** Because of the unique context and characteristics of nuclear operations and the high stakes involved, some risk mitigation steps should focus specifically on AI applications in nuclear operations. Such steps can include active risk management steps within the US nuclear operations community, engagement with allies and competitors, and agreements among nuclear powers.

- ***Applied efforts on risk mitigation of AI applications in military operations.*** The US military, like many militaries around the world, is seeking to apply AI to many functions involving conventional warfare. These general military applications will share many of the same challenges as applications to nuclear operations. This reflects an opportunity for parts of the military and government responsible for nuclear operations to work with the US military as a whole to reduce risks from military applications of AI overall. The US government can also work with foreign allies/partners to this end through technical cooperation. Broader international agreements and discussions of AI safety and ethics may also help reduce risks.
- ***Basic research and practical solutions for fundamental sources of AI-related risks.*** Given the relative newness of modern AI techniques and a focus on commercial applications versus fundamental understanding and safety, there are many aspects of AI risks that are still not well understood. For example, HMT and trust, AI machine-machine interactions, and validation of appropriate areas of AI applications are topics that are widely acknowledged challenges. The US government can work with a wide array of partners—other governments, industry, and academia—to better understand these risks and to seek collective solutions to mitigate them. Such fundamental research would help reduce the risks of using AI in a wide range of fields, including nuclear operations.

Closing thoughts

Our detailed characterization of the connections between AI, nuclear operations, and nuclear risk provides a broader and deeper exploration of these issues than that found in the existing literature. Based on the complexity of and interaction among identified factors, we could not make an absolute conclusion regarding whether the net effect of AI-enabled nuclear operations will be positive or negative: the details of what countries choose to do in the AI-nuclear space and how exactly they do it will matter a great deal—and it is by no means clear today what path each country will take. However, the steps provided above can help guide nuclear powers, and militaries overall, to use AI applications to reduce risks associated with nuclear operations.

Appendix A: Approach and Methodology

We approached this project in five steps.

1. We began with a detailed literature review covering both the fields of artificial intelligence and nuclear operations. This helped us define terms and scope the project.
2. Next, we augmented the literature review with additional research to develop an AI implementation matrix (AIIM) that captures how the US, Russia, and the PRC are currently using or have used AI to enable their nuclear operations.
3. Subsequently, we built on this baseline analysis to devise a circa 2035 AI-enabled nuclear order of battle (OOB) for the US, Russia, and China. Our goal with this OOB was to provide a basis for discussion about how future AI-enabled nuclear postures could interact in crisis or conflict.
4. We convened two day-long workshops that included experts in both AI and nuclear issues from academia, think tanks, and government to generate hypotheses on how future AI-enabled nuclear postures could interact and what steps State AVC could take to mitigate AI-driven nuclear risks and capture risk-reducing benefits.
5. Finally, we compiled and analyzed the results of these workshops alongside existing literature on such topics as deterrence, escalation, and AI and emerging technologies more broadly in order to explicate the different mechanisms by which AI could shape future nuclear risks and how the US government could mitigate those risks and capture possible risk-reducing benefits of AI-enabled nuclear operations.

Defining AI and nuclear operations

This project brings together two separately and immensely complicated fields: nuclear operations and AI. Each has its own core concepts, debates, and jargon. Therefore, we began by writing brief introductions to each topic. This generated definitions for each field, scoped the research, helped the team's AI experts and nuclear experts achieve shared understanding of one another's fields, and illuminated gaps in the existing literature that we would attempt to fill.

Artificial intelligence

We adopted a broad definition of AI that reflects the range of AI applications that we see being implemented or discussed in the US, Russia, and the PRC: "the ability of a digital computer or computer-controlled robot to perform tasks commonly associated with intelligent beings."[70] In concrete terms, this definition encompasses a range of technologies, from "classic AI," which now appears rudimentary, through cutting-edge or aspirational machine learning (ML) and deep-learning technologies.

Nuclear operations

In contrast, we defined nuclear operations relatively narrowly to enable a granular focus on the seemingly minor military details on which the outcomes of crises and wars sometimes turn. Nuclear operations are activities that a state carries out to manage its deployed nuclear forces in peacetime, crises, and war. They include the following distinct but mutually supportive functions:

1. Targeting
2. Employment planning
3. Intelligence, surveillance, and reconnaissance (ISR)
4. Early warning and attack characterization
5. Active (air and) missile defense
6. Leadership decision-making/command and control (C2)
7. Communications
8. Battle damage assessment (BDA)

Each of these functions is explicitly *operational* in nature. Nuclear operations should be distinguished from nuclear strategy and posture, which, while related, are beyond the scope of this study.

AI implementation matrix

Next, having scoped the project, we built on our literature review to develop an AIIM. Drawing on research in English, Russian, and Mandarin, we developed a detailed, thoroughly referenced table that presents two categories of information:

[70] B.J. Copeland, "Artificial Intelligence," *Encyclopedia Britannica,* https://www.britannica.com/technology/artificial-intelligence.

1. How the US, Russia, and China have integrated or are integrating AI into their nuclear and nuclear-related conventional operations—to the extent we can tell, given data limitations—as of its completion in 2022.
2. How these countries could choose to integrate AI into their nuclear operations in the future.

The AIIM provided the study team's answer to the first research question and provided the foundation for follow-on work to understand how AI could exacerbate or mitigate nuclear risks in the future. The AIIM is reproduced in Appendix B: AI Implementation Matrix.

Future AI-enabled nuclear order of battle

We built on the AIIM—which captured past and contemporary applications of AI to nuclear operations—to conceptualize how the US, Russia, and China might use AI in nuclear operations in the future. The goal was to provide participants in two planned workshops with a common reference point for their conversations about AI, nuclear risk, and policy options.

The result of this effort was a circa 2035 AI-enabled nuclear order of battle (OOB). This OOB depicts both plausible future nuclear forces and AI applications for the US, Russia, and China. We circulated it to discussion participants in advance of the workshops and provided copies during the workshop as a way of anchoring the conversation.

To accomplish this, we proceeded in four steps:

1. First, we drew on open sources to generate high-end estimates of the nuclear forces that each country might field in the c. 2035 timeframe and depicted those forces using bar graphs.
2. Second, we identified the drivers of each country's pursuit of AI-enabled nuclear capabilities—detailed above.
3. Third, we nominated a wide range of AI contributions to nuclear operations that could be *useful from a nuclear operations perspective* for inclusion in the OOB.
4. Fourth, we eliminated any of the AI contributions that we believed would be *infeasible or impractical from an AI perspective.*

The result was a depiction of each country's possible future nuclear forces, coupled with a detailed list of plausible ways that each country might use AI in the circa 2035 timeframe to enhance those forces' capabilities. The circa 2035 AI-enabled nuclear OOB is reproduced in Appendix C: Notional Circa 2035 AI-Enabled Nuclear Order of Battle.

Workshops on future risks, opportunities, next steps

In the next stage of the project, we hosted two day-long workshops involving AI and nuclear experts from government, academia, and think tanks at CNA headquarters. Both workshops were identical in design but involved different sets of participants whose collective expertise helped the CNA study team explore the different ways AI might shape future nuclear risks.

Workshop participants

Workshop participants were invited with a view towards assembling two groups whose members collectively possessed expertise in the following fields:

1. Nuclear policy issues, including nuclear strategy, posture, and deterrence
2. Nuclear operations
3. Artificial intelligence, especially with respect to military uses
4. US, Russian, and/or PRC militaries and nuclear forces
5. US government policymaking and policy implementation

In evaluating potential invitees for inclusion, we looked for relevant past or current professional experience as well as past research and publication records to distinguish bona fide experts from others.

As a result of this selection process, we were able to ensure that each group was populated with a combination of relevant subject matter experts (SMEs) and current or former officials with the knowledge and experience necessary to credibly generate reasonable hypotheses on how AI could shape future nuclear risks.

Workshop design and execution

During the workshops, we used design-thinking mechanics to harness participants' collective knowledge, experience, and creativity. We divided them into two parts:

1. First, participants were introduced to the circa 2035 AI-enabled nuclear OOB and a loosely constructed conflict scenario, then asked to brainstorm ways that all three countries' AI-enabled nuclear forces could interact, raising or lowering nuclear risk.
2. Second, participants built on this exercise to identify specific risks and opportunities in three different categories derived from our review of the Cold War and more recent

literature on nuclear strategy and escalation, as well as an assessment of how AI could influence each category of risk: [71]

a. Accidental or unauthorized use and mission failure

b. Underinformed escalation

c. Escalation by rational choice

The carefully designed overall structure of the workshops ensured that the ideas of all participants—not only the most vocal—were shared with the group and captured by CNA rapporteurs. In addition, by framing the workshops around both risks and opportunities, the design avoided biasing or priming experts' contributions in any given direction. The results of these workshops, along with additional research and analysis by the CNA team that drew on previous CNA work and an extensive review of relevant literatures, are reflected in the section of this report on connecting AI to nuclear risk, as well as in the conclusions and recommendations.

[71] During the workshops, we batched accidental and unauthorized use with mission failure. The logic was that these categories of risk were similar from an AI perspective in that they are all principally rooted in the technical performance of AI systems. In addition, we disaggregated underinformed escalation and escalation by rational choice. For clarity of presentation, we placed mission failure in its own category in our report and combined the underinformed and rational choice escalation categories into the umbrella category of escalation by leadership decision.

Appendix B: AI Implementation Matrix

See subsequent page.

CNA

AI IMPLEMENTATION MATRIX

ARTIFICIAL INTELLIGENCE IN US, RUSSIAN, AND PRC NUCLEAR OPERATIONS

KEY

Probability [1]	• Almost no chance/remote: 01–05% • Very unlikely/highly improbable: 05–20% • Unlikely/improbable: 20–45% • Roughly even chance/roughly even odds: 45–55%	• Likely/probable: 55–80% • Very likely/highly probable: 80–95% • Almost certainly/nearly certain: 95–99%
Seriousness [2]	• N/A: AI tech not suitable for given application • Doable: AI tech possibly useful for given application, but not yet (to our knowledge) pursued, explored, or rejected • Exploring: State is seriously considering this AI nuclear application, but has not (to our knowledge) taken concrete steps toward that end • Pursuing: State is making active effort to apply given AI tech to this nuclear application • Implemented: State has applied AI tech to this nuclear application • Rejected: State has explored, pursued, or implemented this AI nuclear application, but has abandoned it	

AI Technologies (means)	• AI—umbrella term for AI technology unknown or unspecified by source • CAI—classic AI • ML—machine learning • DL—deep learning	
AI Application (ways)	• Optimization • Autonomy/automation • Decision support	
Nuclear Operations (ends)	• Targeting • Employment planning • ISR • Early warning/attack characterization	• Active missile defense • Leadership decision making • Communications • Battle damage assessment

Nuclear Operation	Operational Challenge	UNITED STATES	RUSSIA	PEOPLE'S REPUBLIC OF CHINA
Targeting	**In General…**	• Exploring, pursuing, or has implemented a wide range of AI capabilities in support of nuclear targeting.	• Likely pursuing use of AI to find and fix stationary and mobile targets for strategic conventional and novel nuclear strike capabilities.[3]	• Very likely implemented classic AI and enabled neural networks with greater autonomy to improve cruise missile and hypersonic glide vehicle targeting.[4]
	Find, Fix, Track & Target Mobile Land- and Sea-Based Missiles	• Likely exploring AI-enabled Uncrewed Aerial Systems (UAS) to enable Find, Fix, Track, Target, Engage, Assess (F2T2EA) cycle against mobile missiles in contested airspace.[5] • Almost certainly pursuing use of classic AI to automate data fusion from multiple sensors to optimize search for mobile Transporter Erector Launchers (TELs).[6] • Almost certainly pursuing use of ML to automate image recognition of mobile TELs.[7] • Likely exploring DL and ML to identify mobile missile patterns of life to narrow search area.[8] • Likely exploring use of ML to optimize and automate signal processing for acoustic strategic Anti-Submarine Warfare (ASW).[9]		• Very likely pursuing classic AI to optimize data fusion for ASW by integrating information from sensors and unmanned systems.[10] • Almost certainly exploring use of AI to find and fix mobile targets for conventional and nuclear forces.[11]
	Find and Fix Stationary Nuclear Targets			• Almost certainly using advanced algorithms for automatic target recognition to enhance precision.[12]
Other Possible AI Applications for Targeting		• ML/DL-enabled natural language processing to optimize situational awareness (SA) by analyzing patterns in chat feeds and highlighting relevant info. • ML to automate or optimize weapons/sensor cueing decisions throughout F2T2EA. • Classic AI to automate data fusion from multiple sensors to maintain target tracks. • Classic AI to automate data fusion to differentiate decoys from genuine targets. • Classic AI to monitor activity at known targets and de-nominate as they fall into disuse. • ML-enabled image recognition to automate search for new targets that fit criteria.		
Employment Planning	**In General…**	• Likely exploring or pursuing a variety of AI-enabled employment planning applications generally intended to reduce risk of mission failure.	• Exploring, pursuing, or has implemented AI-enabled approaches to improve guidance and increase prospects of mission success, as well as to support real-time analysis of pol-mil situation.[13]	• Unclear whether/how AI may support PRC employment planning beyond guidance system applications.
	Deliberate and Adaptive Strategic Nuclear Mission Planning	• Likely pursuing CAI for data fusion to enable penetrating low-observable aircraft and cruise missile route planning.[14] • Likely exploring use of ML to enable adaptive route planning for penetrating low-observable aircraft and cruise missiles.[15] • Roughly even odds exploring AI to automate and optimize weapon-target assignments.[16]	• Almost certainly implemented AI-enabled modeling in the National Defense Management Center (NDMC) systems to be able to model real-time and forward-looking analysis of the military political situation (correlation of forces, and courses of action (COAs)).[17] • Very likely using ML/DL-enabled natural language processing to automate translation from several languages, as well as data analysis in NDMC.[18]	
	NSNW Mission Planning	• Likely pursuing CAI for data fusion to enable penetrating aircraft route planning, Suppression / Destruction of Enemy Air Defenses (SEAD/DEAD).[19]	• Very likely implemented CAI in some non-strategic nuclear weapons (NSNW) guidance systems to automate guidance/optimize accuracy using scene-recognition matching.[20]	
	Model Weapons Effects on Targets		• Likely pursuing AI-enabled approaches to nuclear effects modeling.[21]	• Almost certainly pursuing AI-enabled modeling for nuclear effects simulations.[22]
	Mission Execution	• Likely pursuing CAI to automate reprogramming (retargeting) spare missiles to compensate for primary missile failure/ensure strike success.[23] • Likely exploring use of AI-enabled UAS to enable bomber/cruise missile penetration to targets.[24]	• Almost certainly pursuing AI-enabled approaches to automate/optimize guidance and navigation for novel nuclear strike systems, as well as hypersonic systems.[25] • Almost certainly implemented CAI for automation in Strategic Rocket Forces systems, including for potential quick retargeting.[26]	• Almost certainly pursuing AI to optimize accuracy of hypersonic weapons (following release).[27]
Other Possible AI Applications for Targeting		• DL or ML to understand enemy values, identify centers of gravity, and trace enemy systems and networks (broadly understood) in order to tailor deterrent threats. • DL or ML to model effects of various COAs on strategic interaction with adversary (in game theory sense) across spectrum from competition through post nuclear environment. • Classic AI to automate process of building adaptive plans from parts of existing deliberate plans. • Classic AI to enhance capabilities/capacities of smaller survivable battle staffs through automation. • ML/DL for natural language processing to expedite transformation of stated or implied leadership intentions (e.g., in decision conferences) to adaptive plans. • ML for decision support to enable target prioritization, weaponeering, weapon allocation. • DL to model climate effects of war plan execution in order to avoid inadvertently triggering nuclear winter. • DL to understand likelihood of/impact of mass fire on targets for given weapon application(s). • DL to generate local (grid square/city block)-level fallout models. • Combination of DL-enabled mass fire and/or fallout models with decision support function.		

Nuclear Operation	Operational Challenge	UNITED STATES	RUSSIA	PEOPLE'S REPUBLIC OF CHINA
Intelligence/ Surveillance/ Reconnaissance	**In General...**	• Unclear to what extent "advanced" AI approaches such as ML/DL are being used to support Intelligence, Surveillance, Reconnaissance (ISR). • Long-standing use of CAI for automated data fusion.	• Apparent focus on enhancing capabilities of NDMC, including via AI. • Likely implemented unknown AI in avionics systems to automate remote sensing for "automatic detection of submarines and surface, ground, and air targets".[28]	• Almost certainly pursuing the adoption of advanced algorithms and ML for remote sensing and battlefield environmental support.[29]
	Understand Adversary Capabilities, Intentions, Decision-Making	• Probably exploring ML/DL for natural language processing-based data collection to augment human analysts assessing risk of adversary aggression.[30]	• Almost certainly implemented unknown AI-enabled modeling in the NDMC systems to be able to model real-time and forward-looking analysis of the military-political situation (correlation of forces and COAs).[31]	
	Optimize Situational Awareness Within/ Across Command Centers	• Definitely implemented CAI to automate data fusion from multiple sources within/across various nuclear operations centers.[32]	• Almost certainly implemented AI-enabled systems in NDMC systems to be able to fuse data to generate a common operational picture.[33]	• Almost certainly pursuing the use of AI-enabled systems to improve common operational picture.[34]
Other Possible AI Applications for Intelligence/Surveillance/ Reconnaissance		• DL or ML to analyze adversary current and future military capabilities and strategy. • DL or ML to optimize analysis of what specific concepts/capabilities/individuals adversary leaders value to enhance deterrence through superior target identification. • DL or ML decision support via social network analysis of adversary decision-making cadre to identify cliques and cleavages that can be manipulated for deterrent effect.		
Early Warning & Attack Characterization	**In General...**	• Unclear whether the US has proceeded beyond use of classic AI for tactical warning.	• Apparent interest in advanced AI applications for early warning and attack characterization.	• Roughly even chance of the PRC pursuing AI for early warning and attack characterization.[35]
	Strategic & Tactical Warning	• Definitely implemented classic AI to automate data fusion from multiple sensors and across command centers for tactical warning.[36]	• Almost certainly implemented AI-enabled modeling in the NDMC systems to be able to model real-time and forward-looking analysis of the military political situation for strategic warning.[37]	
	Attack Characterization		• Very likely pursuing upgrade of radar stations that are part of Russia's missile attack warning system to incorporate AI technology to optimize its ability to measure and assess incoming threats.[38]	
Other Possible AI Applications for Early Warning/Attack Characterization		• Classic AI to automate monitoring of existing sources of indication and warning. • DL or ML to identify new sources of indication and warning for assessment. • ML to automate and optimize trans- or post-attack characterization of adversary targeting strategy in support of response decision-making. • Classic AI to automate impacts of enemy attack on universe of possible response options.		
Active Air & Missile Defense	**In General...**	• Significant interest in uses of various AI approaches to enhance active air and missile defense.	• Likely pursuing for Air and Missile Defense (AMD)[39], particularly given concerns about Western aerospace attack and the evolution of hypersonic systems, interest in the ability to "speed up the task of defining the characteristics and the type of detected objects and the direction of their flight."[40]	• Probably pursuing CAI for sensor fusion to automate and optimize AMD.
	Fuse Data from Multiple Sensors	• Definitely exploring use of ML to optimize analysis of data from multiple Integrated Air and Missile Defense (IAMD) sensors and cue human operators.[41]		
	Sensor, Weapon Allocation/Release	• Very likely exploring use of ML to optimize target discrimination.[42] • Very likely exploring use of ML + CAI to optimize and automate C2 and target engagement.[43]		
	Deny/Degrade Enemy Dissemination of Launch Orders (Left of Launch)	• Likely exploring use of ML/DL to deep fake enemy leadership voiceprints/images to degrade nuclear command, control, communications (NC3) functioning.[44] • Likely exploring use of ML to exploit cyber or other electronic vulnerabilities in adversary NC3 to degrade functioning/prevent launch.[45]		
Other Possible AI Applications for Active Missile Defense		• Classic AI or ML to adaptively optimize interceptor shot doctrine in response to different adversary salvo sizes and targeting strategies. • ML to optimize sensor and interceptor allocation decisions.		
Leadership Decision-Making/C2	**In General...**	• Unclear whether US exploration or pursuit of AI-enabled decision support for non-nuclear operations has or will be applied to nuclear decision support.[46]	• Russia is very interested in the use of AI for decision support. However, many of its AI decision-support systems are likely relatively simple classic AI or expert systems.	• Very likely exploring AI-enabled data fusion processes to improve and accelerate combat guidance and command and control methods.[47]
	Develop & Evaluate COAs for Intended & Incidental Effects		• Almost certainly implemented AI-enabled systems in the NDMC systems to optimize decision-making.[48] • Almost certainly the Russian Strategic Rocket Forces are also exploring AI technologies for decision support systems, intelligent systems and weapons (onboard control systems), and expert systems and automation.[49] • Almost certainly developing system of systems utilizing AI for managing battlefield information in the Automated Control System of the Russian Military.[50] • Very likely implemented CAI for sensor fusion to enable nuclear launch order dissemination via Perimetr system.[51]	
Other Possible AI Applications for Leadership Decision-Making/C2		• ML/DL enabled natural language processing to present leadership with discussion-relevant COAs during decision conferences. • ML/DL enabled natural language processing to identify leadership intentions in support of COA development. • ML or DL to automate analysis of likely adversary responses to potential COA execution, in support of COA evaluation.		
Communications	**In General...**	• Long-standing use of classic AI to automate communications being augmented by more sophisticated AI-enabled cyber defenses.	• Some use of unknown AI to automate launch order transmission.	• Very likely the PRC is exploring CAI for cyber network defense. • It is doable that CAI could be applied to to NC3 network monitoring and protection.[52]
	Monitor Comms System/Network Status	• Very likely exploring use of ML to automate NC3 network monitoring and protection.[53]		
	Automated / Adaptive Comms Routing	• Implemented CAI to automate transmission of Emergency Action Messages.[54]	• Almost certainly using AI to automate communications in support of secure transmission of orders for mission launch.[55]	• Almost certainly implemented CAI to automate C2 for land-based missiles, including for transmitting commands, fusing intelligence, and real-time monitoring of launches.[56]
Other Possible AI Applications for Communications		• ML enabled message routing/re-routing around damage to networks.		
Battle Damage Assessment	**In General...**	• Unclear whether/how US envisions using AI for battle damage assessment.	• Unclear whether/how Russia envisions using AI for battle damage assessment.[57]	• Unclear whether/how PRC envisions using AI for battle damage assessment.
	Fuse Data from Multiple Sensors			
	Assess Pol-Mil Implications of Damage		• There is very likely interest within Russia's Ministry of Defense institutes, but capability unclear.[58]	
Other Possible AI Applications for Battle Damage Assessment		• DL or ML to automate analysis of politico-military implications of attack.		

ENDNOTES

1 Borrowed from the US intelligence community's standardized vocabulary for communicating confidence in its assessments. See Office of the Director of National Intelligence, "Intelligence Community Directive 203. Analytic Standards," p. 3. https://www.dni.gov/files/documents/ICD/ICD%20203%20Analytic%20Standards.pdf. Not all terms are represented in the AIIM. The full set in the key is for completeness.

2 Adapted from vocabulary used to differentiate the comparative seriousness of nuclear proliferation efforts. See Sonali Singh and Christopher Way, "The Correlates of Nuclear Proliferation: A Quantitative Test," *Journal of Conflict Resolution* 48:6 (Dec. 2004): 859–885. Not all terms are represented in the AIIM. The full set in the key is for completeness.

3 There is reporting suggesting that Russian novel nuclear systems, currently either in service or under development, rely on AI/autonomy applications for improving guidance. See Jeffrey Edmonds et al, *AI and Autonomy in Russia*, CNA, 2021, p. 90–91.

4 Wang Changqing, "The Application and Prospects of Artificial Intelligence in Cruise Missiles", http://chuansong.me/n/711504451360

5 Steve Trimble, "Hunter-Killer II: Northrop Grumman Unveils its Vision for Replacing MQ-9," *Aviation Week and Space Technology*, Sept. 13–27, 2020, pp. 50-52.

6 For US post–Cold War era use of real-time sensor fusion for targeting in a counterinsurgency context, see Austin Long & Brendan Rittenhouse Green, "Stalking the Secure Second Strike: Intelligence, Counterforce, and Nuclear Strategy," Journal of Strategic Studies, 38:1-2; pp. 63–64, 2015.

7 This would be an extension of work done under Project Maven—an early DOD foray into applied ML. See Robert O. Work, Memorandum on "Establishment of Algorithmic Warfare Cross-Functional Team," DOD, Apr. 26, 2017, https://dodcio.defense.gov/Portals/0/Documents/Project%20Maven%20DSD%20Memo%2020170425.pdf.

8 Alan Vick et al. Aerospace Operations Against Elusive Ground Targets. Santa Monica, CA, Rand Corporation, 2001, pp. 74-75. Cited in see Austin Long & Brendan Rittenhouse Green (2015) Stalking the Secure Second Strike: Intelligence, Counterforce, and Nuclear Strategy, Journal of Strategic Studies, 38:1-2, p. 56.

9 For US Cold War–era use of advanced signal processing for ASW, see Austin Long & Brendan Rittenhouse Green, "Stalking the Secure Second Strike: Intelligence, Counterforce, and Nuclear Strategy," *Journal of Strategic Studies*, 38:1-2, pp. 47–51, 2015. For contemporary applications see Bryan Clark, "The Emerging Era in Undersea Warfare," CSBA, January 22, 2015, pp. 8–10. https://csbaonline.org/research/publications/undersea-warfare/publication/1. It is unclear whether the US Navy continues to pursue the Cold War legacy strategic ASW mission. See Brad Dismukes, "Strategic ASW in 2021: A stunningly bad idea," *Clio's Musings* blog, https://cliosmusings.blog/2022/01/24/strategic-asw-in-2021-a-stunningly-bad-idea/.

10 For example, the People's Liberation Army Navy is funding and engaging in ongoing research concentrated on data fusion to integrate information from sensors and unmanned systems in support of anti-submarine warfare. See: "Academician He You: Accelerate the development of maritime information processing technology, and provide scientific and technological support for a powerful maritime nation", Strategic Frontier Technology, Nov. 4, 2017, http://webcache.googleusercontent.com/search?q=cache:Fe82RK1Gzu8J:www.sohu.com/a/202366530_465915+&cd=5&hl=en&ct=clnk&gl=us

11 Researchers associated with the People's Liberation Army Rocket Force Engineering University are exploring the application of machine learning and neural networks in ways that could be used for future targeting. The PLARF controls the PLA's conventional and nuclear missile force. See: Xu Suhui et al., "Unsupervised Remote Sensing Domain Adaptation Method with Adversarial Network and Auxiliary Task".

12 Military efforts to use AI to improve targeting go back to the mid-2000s, see: All-Military Military Terminology Management Committee, People's Liberation Army Military Terminology, Military Science Press, 2011, p. 660.

13 The NMDC also has a strategic nuclear forces control center that reportedly helps to coordinate employment, but we have no evidence that that part of the NMDC involves AI-enabled systems.

14 Myron Hura and Gary McLeod, "Route Planning Issues for Low Observable Aircraft and Cruise Missiles," RAND Corporation, 1993. Cited in Austin Long & Brendan Rittenhouse Green, "Stalking the Secure Second Strike: Intelligence, Counterforce, and Nuclear Strategy," *Journal of Strategic Studies*, 38:1-2, 2015.

15 Ibid.

16 The US Army is experimenting with a similar AI application for ground combat. See Lee Hudson, "War Footing," *Aviation Week and Space Technology*, Oct. 12–25, 2020, p. 50.

17 "Russian National Defense Management Center uses artificial intelligence", Regnum.ru, Jan. 27, 2020, https://regnum.ru/news/polit/2836730.html. See more in Edmonds et al., pp. 145–147.

18 See "National center for Defense Management will receive a smart monitoring system and forecasting from the defense industrial complex" , Jan. 29, 2015, Rostec press release available at https://vpk.name/news/125525_nacionalnyi_centr_upravleniya_oboronoi_poluchit_umnuyu_sistemu_monitoringa_i_prognoza_ot_opk.html.

19 Myron Hura and Gary McLeod, "Route Planning Issues for Low Observable Aircraft and Cruise Missiles," RAND Corporation, 1993. Cited in Austin Long & Brendan Rittenhouse Green, "Stalking the Secure Second Strike: Intelligence, Counterforce, and Nuclear Strategy," *Journal of Strategic Studies*, 38:1-2, 2015.

20 Similar to the TERCOM system used for US nuclear-armed cruise missile guidance.

21 Supercomputer-enabled effects modeling capability resides in the 12 TsNII, the Ministry of Defense research institute supporting Russia's nuclear security forces (formerly known as the 12th GUMO). A recruitment brochure for the 12 TsNII scientific corps notes the "development of newest applied and systemic software for supercomputers." See undated https://ftf.tsu.ru/wp-content/uploads/broshyura_12-nauchnaya-rota.pdf.

22 "Supercomputers Drive Military Revolution, Simulating Nuclear Explosions is One of the Important Applications," *Xinhua*, Jul. 14, 2021, http://www.xinhuanet.com/mil/2021-07/14/c_1211240632.htm.

23 Keir Lieber and Daryl Press, "The New Era of Counterforce: Technological Change and the Future of Nuclear Deterrence," *International Security* Vol. 41 No. 4, p. 24. This would be a logical feature to include in the new Ground-Based Strategic Deterrent ICBM.

24 Steve Trimble. "Hunter-Killer II: Northrop Grumman Unveils its Vision for Replacing MQ-9," *Aviation Week and Space Technology*, Sept. 13–27, 2020, pp. 50–52.

25 There is reporting suggesting that Russian novel nuclear systems, currently either in service or under development, rely on AI/autonomy applications for improving guidance. See Jeffrey Edmonds et al, 2021, "AI and Autonomy in Russia," CNA, p. 90–91.

26 As per Yarynich, "Signal-A allows retargeting of missiles remotely from the General Staff or from the SRF main staff. Several sets of the flight plans are stored in the equipment of the seventh level (launchers). For retargeting missiles, it is sufficient to indicate in the launch order the number of the corresponding combat plan. Upon receiving the plan number, the automated system gives the command to the missile for the selection of the required flight path, which is carried out automatically within 10 go 15 seconds, after which the missile is launched." Valeriy Yarynich, C3: Nuclear Command, Control, Cooperation (CDI, 2003), p. 148.

27 For an in-depth assessment, see: Lora Saalman, "China's Integration of Neural Networks into Hypersonic Glide Vehicles," Dec. 2018, https://nsiteam.com/social/wp-content/uploads/2018/12/AI-China-Russia-Global-WP_FINAL.pdf

28 ['Radar MMS': Artificial intelligence system for aircraft and drones has been created in Russia], Radar MMS, 25 Aug. 2018 (in Russian). http://www.radar-mms.com/news/media/radar-mms-v-rossii-sozdan-iskusstvennyy-intellekt-dlya-samoletov-i-bespilotnikov/.

29 See: Elsa Kania, "'AI Weapons' in China's Military Innovation," Global China, April 2020, https://www.brookings.edu/wp-content/uploads/2020/04/FP_20200427_ai_weapons_kania_v2.pdf

30 A number of universities and nonprofit organizations are already pursuing conflict prediction models with varying results. It is reasonable to assume that the DOD or intelligence community is exploring (if not pursuing) similar capability. See Tate Ryan-Mosley. "Bringing Order to Chaos; Predicting Conflict Could Save Lives. Are we finally getting better at it?" *MIT Technology Review*, Nov./Dec. 2019, vol. 122, no. 6 pp. 12–14.

31 "Russian National Defense Management Center uses artificial intelligence", Regnum.ru, Jan. 27, 2020, https://regnum.ru/news/polit/2836730.html. See more in Edmonds et al, pp. 145–147.

32 Author visit to Cape Cod PAVE PAWS EW radar, Jan. 2014. For an example of long US experience in this regard see "SAGE: Semi-Automatic Ground Environment air defense system," MIT Lincoln Lab, https://www.ll.mit.edu/about/history/sage-semi-automatic-ground-environment-air-defense-system.

33 "Russian National Defense Management Center uses artificial intelligence", Regnum.ru, Jan. 27, 2020, https://regnum.ru/news/polit/2836730.html. See more in Edmonds et al, pp. 145–147.

34 Yuan Qunbao, "Open the Door to Victory in War Through Calculation, website of the People's Republic of China Ministry of National Defense, Aug. 02, 2018, http://www.mod.gov.cn/jmsd/2018-08/02/content_4821566.htm

35 While we found no evidence in credible PRC sourcing of the PRC directly pursuing AI to support early warning and attack characterization, frequent discussions can be found in credible PRC sources discussing U.S. defense budget increases in 2022 to "increase nuclear command and control and early warning systems." This coupled with the PRC's focus on intelligentization of its military force and past self-assessments of weaknesses in early warning and detection systems leads to our analytical assessment that the PRC may pursue AI for early warning. See for example, Chen Hanghui, "In 2022, the Military Game of Great Powers Will Intensify 2022, China Military Online, January 13, 2022, http://www.81.cn/jfjbmap/content/2022-01/13/content_307244.htm; Ryan Fedasiuk, Jennifer Melot, Ben Murphy, "Harnessed Lightning: How the Chines Military is Adopting Artificial Intelligence," Center for Security and Emerging Technology, October 2021, https://cset.georgetown.edu/wp-content/uploads/CSET-Harnessed-Lightning.pdf

36 Author visit to Cape Cod PAVE PAWS EW radar, Jan. 2014.

37 "Russian National Defense Management Center uses artificial intelligence", Regnum.ru, Jan. 27, 2020, https://regnum.ru/news/polit/2836730.html. See more in Edmonds et al, pp. 145–147.

38 "Russia to boost missile attack warning system's capabilities after upgrade," Feb. 15, 2021, https://tass.com/defense/1256603

39 Aleksei Kozachenko and Aleksei Ramm, "Watching From Afar: Air Defense Forces Received Ground AWACS", Iz.ru, Sept. 15, 2019. https://iz.ru/918749/aleksei-kozachenko-aleksei-ramm/daleko-slezhu-voiska-pvo-poluchili-nazemnyi-avaks.

40 Col. D.V. Galkin, Col. P.A. Polyandra, and Col. A.V. Stepanov, "The state and prospects of employment of AI in military affairs,", Voennaya Mysl, Jan. 2021, pp. 113–124.

41 Lee Hudson, "Silicon Valley Assists US Military in Homeland Defense," *Aviation Week and Space Technology*, Mar. 22–April 4, 2021, pp. 64–65. Tyler Rogoway. "Everything you ever wanted to know about the Navy's ever-evolving AEGIS combat system." The Warzone blog, March 4, 2021. https://www.thedrive.com/the-war-zone/39508/how-the-aegis-combat-system-is-evolving-to-dominate-naval-warfare-of-the-future.

42 Todd Lopez, "Vice Admiral Discusses Potential of AI in Missile Defense, Testing, Operations," DOD News, Aug. 12, 2021, https://www.defense.gov/News/News-Stories/Article/Article/2730215/vice-admiral-discusses-potential-of-ai-in-missile-defense-testing-operations/.

43 Todd Lopez, "Vice Admiral Discusses Potential of AI in Missile Defense, Testing, Operations," DOD News, Aug. 12, 2021. https://www.defense.gov/News/News-Stories/Article/Article/2730215/vice-admiral-discusses-potential-of-ai-in-missile-defense-testing-operations/; Tyler Rogoway, "Everything you ever wanted to know about the Navy's ever-evolving AEGIS combat system," *The Warzone blog*, Mar. 4, 2021. https://www.thedrive.com/the-war-zone/39508/how-the-aegis-combat-system-is-evolving-to-dominate-naval-warfare-of-the-future.

44 For US development of this capability against the Soviet Union during the 1970s, see Benjamin Fischer, "CANOPY WING: The US War Plan that Gave the East Germans Goose Bumps," *International Journal of Intelligence and Counterintelligence* 27/3 (2014) p. 439.

45 For US development of this capability against the Soviet Union during the 1970s, see Benjamin Fischer, "CANOPY WING: The US War Plan that Gave the East Germans Goose Bumps," *International Journal of Intelligence and Counterintelligence* 27/3 (2014) p. 448–449.

46 For discussion of the benefits of streamlined decision-making, especially when employing hypersonic weapons against mobile targets see Alan Vick et al., *Aerospace Operations Against Elusive Ground Targets*, Santa Monica, CA, RAND Corporation, 2001, p. 74. For an example of an Army program that leveraged AI and other capabilities to reduce decision time from 20 minutes to 20 seconds, see "The US Army is experimenting with a similar AI application for ground combat." See Lee Hudson, "War Footing," Aviation Week and Space Technology, October 12-25, 2020, p. 50. At the same time, given the United States' policy of posturing its forces to maximize presidential decision-making time, it is unclear whether DOD leaders would judge an effort to develop such a decision-support system desirable. See e.g., 2018 *Nuclear Posture Review*, p. 22.

47 Yang Zuo, "The Information Age Accelerates the Transformation of War Patterns: Using Information Concepts to Open the Door to Military Theoretical Innovation," China Military Online, December 09, 2021, https://www.81.cn/yw/2021-12/09/content_10113555.htm

48 "Russian National Defense Management Center uses artificial intelligence", Regnum.ru, Jan. 27, 2020, https://regnum.ru/news/polit/2836730.html. See more in Edmonds et al, pp. 145–147. The NDMC also houses the Control Center of Strategic Nuclear Forces intended for C2 "of nuclear weapons employment based on the decision of the highest military-political leadership." See "National defense management center of RF has started combat duty", RIA Novosti, Jan. 12, 2014, https://ria.ru/20141201/1035951618.html.

49 "AI in military affairs", Strategic Rocket Forces dictionary, MOD website, undated, https://encyclopedia.mil.ru/encyclopedia/dictionary/details.htm?id=13200@morfDictionary.

50 Aleksandr Khokhlov, "The bullet is no longer the fool", Feb. 15, 2021, https://vm.ru/technology/861589-pulya-bolshe-ne-dura.

51 Edmonds, pp. 88-89; Defense Intelligence Agency, "Russia Military Power: Building a Military to Support Great Power Aspirations," 2017, https://www.dia.mil/portals/27/documents/news/military%20power%20publications/russia%20military%20power%20report%202017.pdf; Pavel Podvig, ed., Russian Strategic Nuclear Forces, Cambridge, MIT Press, 2004, pp. 65-66.

52 See: Wang Zongyi, Li Haoran, "School of Electronic Countermeasures, National University of Defense Technology: Forging Intelligent Shields to Protect Cyberspace," PRC Ministry of National Defense, October 15, 2021, http://www.mod.gov.cn/education/2021-10/15/content_4896857.htm; Ryan Fedasiuk, "Chinese Perspectives on AI and Future Military Capabilities," Center for Security and Emerging Technologies, August 2020, https://cset.georgetown.edu/wp-content/uploads/CSET-Chinese-Perspectives.pdf

53 David Vergun, "General Says Artificial Intelligence Will Play Important Role in Network Defense," DOD News, Oct. 8, 2021, https://www.defense.gov/News/News-Stories/Article/Article/2805760/general-says-artificial-intelligence-will-play-important-role-in-network-defense/; also the Navy's Continuous Hardening and Monitoring Program (CHaMP) which aims to provide "machine-assisted assessments of" various aspects of Navy commands' network security. Statement by Vice Admiral Mike Gilday, Commander, US Fleet Cyber Command, US Tenth Fleet, Before the Senate Armed Services Committee Subcommittee on Cybersecurity Cyber Posture, Mar. 13, 2018, P. 5. https://www.armed-services.senate.gov/imo/media/doc/Gilday_03-13-18.pdf.

54 Justin Oakes, "New construction begins at Offutt, SACCS to receive new home," 8th Air Force/J-GSOC Public Affairs, Mar. 5, 2020. https://www.stratcom.mil/Media/News/News-Article-View/Article/2104070/new-construction-begins-at-offutt-saccs-to-receive-new-home/.

55 As per Yarynich, see p. 137 onward.

56 Fiona Cunningham, "Nuclear Command, Control, and Communication Systems of the People's Republic of China," NAPSNet Special Reports, July 18, 2019, https://nautilus.org/napsnet/napsnet-special-reports/nuclear-command-control-and-communications-systems-of-the-peoples-republic-of-china/

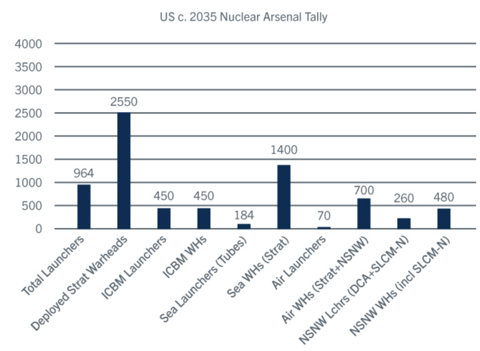
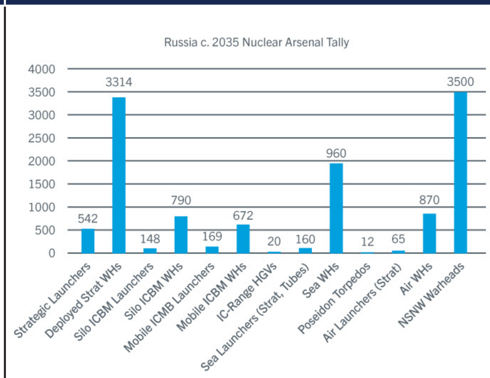
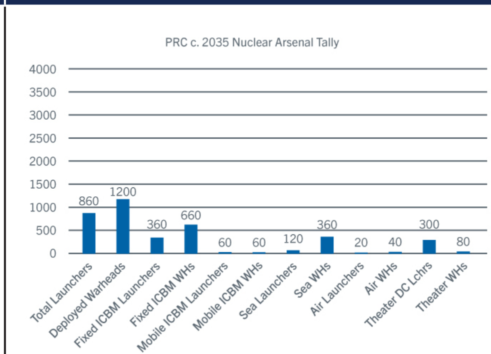
57 Capability may exist within the National Defense Management Center's strategic nuclear forces control center.

58 See the section on "Damage Considerations" in Anya Fink and Michael Kofman, "Russian Strategy for Escalation Management: Key Debates and Players in Military Thought," CNA, April 2020, pp. 18-23, https://www.cna.org/CNA_files/PDF/DIM-2020-U-026101-Final.pdf.

Appendix C: Notional Circa 2035 AI-Enabled Nuclear Order of Battle

See subsequent page.

A NOTIONAL CIRCA 2035 AI-ENABLED NUCLEAR ORDER OF BATTLE*

		UNITED STATES	RUSSIA	PEOPLE'S REPUBLIC OF CHINA (PRC)
C. 2035 Nuclear Arsenal Tally				
General Orientation		• The US has been using AI (as the term/tech has evolved) for nuclear operations since the 1950s. Driving goals center on improving existing (non-AI-enabled) capabilities and expanding presidential decision time. Examples may include: ◦ Enhancing effectiveness of counterforce strikes by improving target ID, weaponeering, delivery system reliability/penetration capability, accuracy, & battle damage assessment; ◦ Increasing pre-attack warning time by improving or accelerating intelligence collection & analysis, sensor data fusion, and warning message dissemination; ◦ Improving effectiveness of active defenses; ◦ Accelerating the dissemination of orders from the president to executing units. • The US is also investing in AI-enabled conventional military technology that could shape escalation risk.	• Russia has been using AI (as the term/tech has evolved) for nuclear operations since the 1960s. Driving goal has been to preserve secure second strike vs. the US, and applications have included air/missile defense, early warning improvements, and command and control. Examples may include: ◦ Increasing decision time via early warning, ISR, and remote sensing systems, including on land, in air, and undersea; ◦ Improving decision-making through information collection and analysis aid in command and control; ◦ Pursuing air and missile defense systems to monitor, detect, & respond to attack, including with hypersonics; ◦ Improving effectiveness of strike capabilities, including through guidance for new dual-capable boutique weapons. • Though sanctions may constrain its pursuits, Russia is also investing in AI-enabled conventional technology that could shape escalation risk.	• The PRC has explored automating some NC3 functions since the 1970s, and began using AI for certain aspects of nuclear operations in late 2010s. Driving goals are: ◦ Not getting "left behind" as other countries adopt AI into NC3; ◦ Using AI to modernize its military and "intelligentize" warfare; ◦ Improving decision-making speed and overall C2 support; ◦ Increasing targeting precision, including for hypersonic weapons; ◦ Adopting AI for nuclear effects modeling and simulation. • Although the PRC is overall pursuing AI as part of its larger goals of military modernization, how it will adopt AI into nuclear operations remains unclear. • PRC investments in AI-enabled conventional military technology could also shape escalation risk.
Example AI Applications	**ISR**	• ID and track hidden/mobile targets. • ID hidden patterns in adversary behavior. • Provide faster, more accurate, more detailed tactical warning of attack.	• Provide faster, more accurate tactical warning of attack.	• ID hidden patterns in adversary behavior. • Provide faster, more accurate tactical warning of attack.
	Decisions	• Integrate data to provide common operational picture. • Develop short list of options for evaluation/decision. • Predictive analysis of adversary responses to possible courses of action. • Accelerate OODA loop. • Analyze incoming info stream for decision-critical inputs.	• Integrate data to provide common operational picture. • Accelerate OODA loop. • Predictive analysis of adversary responses to possible courses of action. • Analyze incoming info stream for decision-critical inputs. • Automated translation of foreign data sources. • Conditionally delegate authority to release nuclear weapons to ensure retaliation/deter attempted decapitation.	• Integrate data to provide common operational picture. • Develop short list of options for evaluation/decision. • Predictive analysis of adversary responses to possible courses of action. • Accelerate OODA loop. • Analyze incoming info stream for decision-critical inputs.
	Plans	• Analyze adversary values for targeting/tailored deterrence. • Improve adaptive/dynamic target planning. • Evaluate plans/options for alignment with commander's intent. • Evaluate plans/options for collateral damage.	• Analyze adversary values for targeting/tailored deterrence. • Improve adaptive/dynamic target planning.	• Analyze adversary values for targeting/tailored deterrence. • Improve adaptive/dynamic target planning. • Evaluate plans/options for alignment with commander's intent.
	Comms	• Automated adaptive response to interference (cyber attack on node, etc.). • Audio <-> text transcription. • Network security. • Reduce tradeoffs between system security, ease of use. • Biometric ID to confirm release authority.	• Automated adaptive response to interference (cyber attack on node, etc.). • Audio <-> text transcription. • Network security. • Reduce tradeoffs between system security, ease of use. • Biometric ID to confirm release authority.	• Automated adaptive response to interference (cyber attack on node, etc.). • Audio <-> text transcription. • Network security. • Reduce tradeoffs between system security, ease of use. • Biometric ID to confirm release authority.
	Weapons	• Non-nuclear swarms to suppress/destroy enemy defenses. • Human-machine teaming to enable nuclear strike. • Automated post-launch weapon navigation/penetration to target. • Long endurance, low-observable, loitering conventional munitions to autonomously search for and destroy enemy mobile missiles. • Accelerate weapons design->simulation->iteration-> to production.	• Autonomous post-launch weapon navigation/penetration to target, including for boutique second (third?) strike weapons. • Non-nuclear swarms to suppress/destroy enemy defenses. • Human-machine teaming to enable nuclear strike. • Automated post-launch weapon navigation/penetration to target. • Maintenance and physical security solutions.	• Non-nuclear swarms to suppress/destroy enemy defenses. • Automated post-launch weapon navigation/penetration to target. • Human-machine teaming (HMT) to enable nuclear strike.
	Defenses	• National missile defense web of systems with (optional) automated cue-target ID-interceptor launch-assess/re-engage mode. • Detect and counter adversary disinformation/misinformation campaigns.	• National capital and alternate HQ missile defense web of systems with (optional) automated cue-target ID-interceptor launch-assess/re-engage mode. • Detect and counter adversary disinformation/misinformation campaigns.	• National missile defense web of systems with (optional) automated cue-target ID-interceptor launch-assess/re-engage mode.

* We present this notional c. 2035 AI-enabled nuclear order of battle as a discussion facilitation tool. This order of battle imagines all three competitors developing their nuclear arsenals and enabling AI capabilities with great vigor over the next dozen years. We built it by drawing on two main kinds of sources: First, we used open-source research on US, Russian, and PRC contemporary and projected nuclear capabilities. Examples include the *IISS Military Balance, SIPRI Yearbook, the Bulletin of the Atomic Scientists* "Nuclear Notebook" series, Defense Intelligence Agency publications, Congressional testimony, and the like. This helped the CNA team develop substantially enlarged and improved, but still plausible, nuclear arsenal tallies and descriptions. Second, we built on the small academic literature on AI in nuclear operations, as well as earlier CNA research from this project and others, to describe toward what ends, and in what specific ways, each country might apply AI to its nuclear operations in the 2035 timeframe. While we believe that this c. 2035 AI-enabled nuclear order of battle is plausible, it is not intended to be a best guess about what the future might hold. Rather, it is intended to be a useful starting point for discussion on risks, opportunities, and policy options.

Abbreviations: DCA – dual capable aircraft | NSNW – non-strategic nuclear weapon | ICBM – intercontinental ballistic missile | OODA – observe, orient, decide, act | SLCM-N – submarine launched cruise missile-nuclear | WH – warhead

Abbreviations

AI	artificial intelligence
AIIM	AI implementation matrix
AI-N WG	AI-Nuclear Operations Working Group
AVC	US State Department Bureau of Arms Control, Verification, and Compliance
BDA	battle damage assessment
C2	command and control
C3	command, control, and communications
C4ISR	command, control, communications, computers, and ISR
CDAO	Chief Digital and Artificial Intelligence Office (DOD)
CFT	cross-functional team
COA	course of action
CSBM	confidence and security-building measure
DOD	Department of Defense
FFRDC	federally funded research and development center
HMT	human-machine teaming
HSC	Homeland Security Council
ICBM	intercontinental ballistic missile
ICRC	International Committee of the Red Cross
ISR	intelligence, surveillance, and reconnaissance
JADC2	Joint All-Domain Command and Control
JAIC	Joint Artificial Intelligence Center (DOD)
ML	machine learning
MOD	Russian Federation Ministry of Defense
NATO	North Atlantic Treaty Organization
NC3	nuclear command, control, and communications

NSC	National Security Council
OOB	order of battle
OSD	Office of the Secretary of Defense
PLA	People's Liberation Army (PRC)
POTUS	President of the United States
PRC	People's Republic of China
RF	Russian Federation
RRP	Risk Reduction Playbook
SAGE	Synergistic Anticipation of Geopolitical Events
UN	United Nations
UNODA	United Nations Office for Disarmament Affairs
USG	United States government
USIC	US intelligence community
USSTRATCOM	US Strategic Command

References

Acton, James. 2018. “Escalation Through Entanglement: How the Vulnerability of Nuclear Command and Control Systems Raises the Risks of an Inadvertent Nuclear War.” *International Security* 43(1).

Adams, Karen Ruth. 2003. "Attack and Conquer? International Anarchy and the Offense-Defense-Deterrence Balance." *International Security* 28(3).

"Air Force Wants to Keep ‘Man in the Loop’ with B-21 Raider.” Sep. 19, 2016. Military.com. https://www.military.com/defensetech/2016/09/19/air-force-wants-to-keep-man-in-the-loop-with-b-21-raider .

Bell, Mark S. 2015. “Beyond Emboldenment: How Acquiring Nuclear Weapons can Change Foreign Policy.” *International Security* 40(1).

Boulanin, Vincent, Lora Saalman, Petr Topychnakov, Fei Su, and Moa Peldan Carlsson. June 2020. *Artificial Intelligence, Strategic Stability and Nuclear Risk.* SIPRI. https://www.sipri.org/publications/2020/other-publications/artificial-intelligence-strategic-stability-and-nuclear-risk.

Burenok, V. 2018. “AI: problems and solutions (Искусственный интеллект: проблемы и пути решения).” *Arsenal Otechestva* 1(33). https://arsenal-otechestva.ru/article/1010-iskusstvennyj-intellekt-problemy-i-puti-resheniya.

Chernenko, Elena. July 27, 2021. “The state is stably strategic” (Состояние стабильно стратегическое). *Kommersant*. https://www.kommersant.ru/doc/4918323.

Copeland, B.J. “Artificial Intelligence,” *Encyclopedia Britannica,* https://www.britannica.com/technology/artificial-intelligence.

Cox, Jessica, and Heather Williams. 2021. “The Unavoidable Technology: How Artificial Intelligence Can Strengthen Nuclear Stability.” *The Washington Quarterly* 44 (1). https://doi.org/10.1080/0163660X.2021.1893019.

Davis, James Jr., Bernard Finel, Stacie Goddard, Stephen Van Evera, Charles Glaser, and Chaim Kaufmann. 1999. "Correspondence: Taking Offense at Offense Defense Theory." *International Security* 23(3).

Davis, Zachary S. Mar. 2019. *Artificial Intelligence on the Battlefield: An Initial Survey of Potential Implications for Deterrence, Stability, and Strategic Surprise.* Lawrence Livermore National Laboratory/Center for Global Security Research. https://cgsr.llnl.gov/content/assets/docs/CGSR-AI_BattlefieldWEB.pdf.

Decree of the President of the Russian Federation No. 355. June 2, 2020. “On the Fundamentals of the State Policy of the Russian Federation in the Field of Nuclear Deterrence [Указ Президента Российской Федерации от 02.06.2020 № 355 "Об Основах государственной политики Российской Федерации в области ядерного сдерживания].”

Dobbs, Michael. 2009. *One Minute to Midnight: Kennedy, Khrushchev and Castro on the Brink of Nuclear War.* New York: Vintage Books.

Durkalec, Jacek, Anna Peczeli, and Brian Radzinsky. Feb. 2022. *Nuclear Decision-Making, Complexity, and Emerging and Disruptive Technologies: A Comprehensive Assessment.* European Leadership Network. https://www.europeanleadershipnetwork.org/report/nuclear-decision-making-complexity-and-emerging-and-disruptive-technologies-a-comprehensive-assessment/.

Edmonds, Jeffrey, Samuel Bendett, Anya Fink, Mary Chestnut, Dmitry Gorenburg et al. May 2021. *Artificial Intelligence and Autonomy in Russia.* CNA. https://www.cna.org/CNA_files/centers/CNA/sppp/rsp/russia-ai/Russia-Artificial-Intelligence-Autonomy-Putin-Military.pdf.

Favarro, Marina, and Elke Schwarz. Mar. 2022. "Human Augmentation and Nuclear Risk: The Value of a Few Seconds." *Arms Control Today*. https://www.armscontrol.org/act/2022-03/features/human-augmentation-nuclear-risk-value-few-seconds.

Feaver, Peter. 1992. *Guarding the Guardians: Civilian Control of Nuclear Weapons in the United States*. Ithaca, NY: Cornell University Press.

Fitzpatrick, Mark. 2019. "Artificial Intelligence and Nuclear Command and Control." *Survival* 61(3). https://doi.org/10.1080/00396338.2019.1614782.

Freeberg, Sydney Jr. Sep. 25, 2019. "No AI for Nuclear Command and Control: JAIC's Shanahan." Breaking Defense. https://breakingdefense.com/2019/09/no-ai-for-nuclear-command-control-jaics-shanahan/.

Galkin, Col. D.V., Col. P.A. Polyandra, and Col. A.V. Stepanov. Jan. 2021. "The state and perspectives of the use of AI in military affairs" (Состояние и перспективы использования искусственного интеллекта в военном деле) *Voennaya Mysl'*.

Geist, Edward, and Andrew J. Lohn. 2018. *How Might Artificial Intelligence Affect the Risk of Nuclear War?* RAND Perspective. https://www.rand.org/content/dam/rand/pubs/perspectives/PE200/PE296/RAND_PE296.pdf.

Gigova, Radina. Sep. 2, 2017. "Who Vladimir Putin Thinks will Rule the World." CNN. https://www.cnn.com/2017/09/01/world/putin-artificial-intelligence-will-rule-world.

Glaser, Charles. 1984. "Why Even Good Defenses May Be Bad." *International Security* 9(2).

Glaser, Charles. 1990. *Analyzing Strategic Nuclear Policy*. Princeton, NJ: Princeton University Press.

Glaser, Charles, and Chaim Kaufmann. 1998. "What Is the Offense-Defense Balance and Can We Measure It?" *International Security* 22(4).

Gottemoeller, Rose. Oct. 2021. "The Standstill Conundrum: The Advent of Second-Strike Vulnerability and Options to Address It." *Texas National Security Review* 4(4). http://dx.doi.org/10.26153/tsw/17496.

Green, Brendan. 2020. *The Revolution that Failed: Nuclear Competition, Arms Control, and the Cold War*. New York: Cambridge University Press.

Greenwood, Ted. 1975. *Making the MIRV: A Study of Defense Decision-Making*. Pensacola, FL: Ballinger Publishing Co.

Hersman, Rebecca. Summer 2020. “Wormhole Escalation in the New Nuclear Age.” *Texas National Security Review.* http://dx.doi.org/10.26153/tsw/10220.

Horowitz, Michael C. 2019. “When speed kills: Lethal autonomous weapon systems, deterrence and stability.” *Journal of Strategic Studies* 42(6). https://doi.org/10.1080/01402390.2019.1621174.

Horowitz, Michael C., and Paul Scharre. Jan. 2021. *AI and International Stability: Risks and Confidence-Building Measures.* Center for a New American Security. https://www.cnas.org/publications/reports/ai-and-international-stability-risks-and-confidence-building-measures.

Horowitz, Michael C., Paul Scharre, and Alexander Velez-Green. Dec. 2019. “A Stable Nuclear Future? The Impact of Autonomous Systems and Artificial Intelligence.” Available at https://arxiv.org/pdf/1912.05291.

Jervis, Robert. 1990. *The Meaning of the Nuclear Revolution: Statecraft and the Prospect of Armageddon*. Ithaca, NY: Cornell University Press.

Johnson, James. July 29, 2022. “AI and the Risk of Nuclear War.” War on the Rocks. https://warontherocks.com/2022/07/ai-autonomy-and-the-risk-of-nuclear-war/.

Johnson, James. 2022. “Inadvertent Escalation in the Age of Intelligent Machines: A New Model for Nuclear Risk in the Digital Age.” *European Journal of International Security* 7(3). https://doi.org/10.1017/eis.2021.23.

Kahn, Herman. 1965. *On Escalation: Metaphors and Scenarios.* New York: Penguin Books.

Kokoshin, A.A. 2019. “Development Prospects of the Military Technosphere and the Future of Wars and Noncombat Use of Military Force.” Vestnik AVN 2/2019.

Kozyulin, Vadim. Aug. 2019. “Militarization of AI—A Russian Perspective.” In *The Militarization of Artificial Intelligence.* Stanley Center for Peace and Security. https://stanleycenter.org/publications/militarization-of-artificial-intelligence/.

Lieber, Keir. 2000. "Grasping the Technological Peace: The Offense-Defense Balance and International Security." *International Security* 25(1).

Lowther, Adam, and Curtis McGiffin. Aug. 16, 2019. “America Needs a ‘Dead Hand’.” War on the Rocks. https://warontherocks.com/2019/08/america-needs-a-dead-hand/.

Lynn-Jones, Sean. Summer 1995. “Offense-Defense Theory and Its Critics.” *Security Studies* 4.

MacKenzie, Donald. 1993. *Inventing Accuracy: A Historical Sociology of Nuclear Missile Guidance*. Cambridge, MA: MIT Press.

Mearsheimer, John. 2014. *The Tragedy of Great Power Politics*. New York: W.W. Norton & Co.

Narang, Vipin. 2014. *Nuclear Strategy in the Modern Era: Regional Powers and International Conflict.* Princeton, NJ: Princeton University Press.

O’Brien, Luke. Sep. 11, 2019. “Whither Skynet? An American ‘Dead Hand’ Should Remain a Dead Issue.” War on the Rocks. https://warontherocks.com/2019/09/whither-skynet-an-american-dead-hand-should-remain-a-dead-issue/.

Pauly, Reid Barret Charles. 2018. “Would US Leaders Push the Button? Wargames and the Sources of Nuclear Restraint,” *International Security* 43(2).

Perrow, Charles. 1999. *Normal Accidents: Living with High-Risk Technologies*. Princeton, NJ: Princeton University Press.

Posen, Barry. 1992. *Inadvertent Escalation: Conventional War and Nuclear Risks*. Ithaca, NY: Cornell University Press.

Roberts, Brad. 2016. *The Case for US Nuclear Weapons in the 21st Century*. Stanford, CA: Stanford University Press.

Russian Federation MOD website. Dec. 9, 2021. 'ТЕЗИСЫ выступления начальника Генерального штаба ВС РФ на брифинге перед военными атташе иностранных государств." https://function.mil.ru/files/morf/%D0%A2%D0%B5%D0%B7%D0%B8%D1%81%D1%8B.pdf.

Russian Government Official Website for Legal Information. Accessed Aug. 1, 2022. http://publication.pravo.gov.ru/Document/View/0001202006020040?index=5&rangeSize=1.

Sagan, Scott. 1993. *The Limits of Safety: Organizations, Accidents, and Nuclear Weapons.* Princeton, NJ: Princeton University Press.

Sankaran, Jaganath. Apr. 25, 2019. "A Different Use for Artificial Intelligence in Nuclear Weapons Command and Control." War on the Rocks. https://warontherocks.com/2019/04/a-different-use-for-artificial-intelligence-in-nuclear-weapons-command-and-control/.

Scharre, Paul. Aug. 2019. "Military Applications of Artificial Intelligence: Potential Risks to International Peace and Security." In *The Militarization of Artificial Intelligence.* Stanley Center for Peace and Security. https://stanleycenter.org/publications/militarization-of-artificial-intelligence/.

Schlosser, Eric. 2014. *Command and Control: Nuclear Weapons, the Damascus Accident, and the Illusion of Safety*. New York: Penguin Books.

Sherwin, Martin J. 2022. *Gambling With Armageddon: Nuclear Roulette from Hiroshima to the Cuban Missile Crisis.* New York: Vintage Books.

Sisson, Melanie. Aug. 2019. "Multistakeholder Perspectives on the Potential Benefits, Risks, and Governance Operations for Military Applications of Artificial Intelligence," In *The Militarization of Artificial Intelligence,* Stanley Center for Peace and Security. https://stanleycenter.org/publications/militarization-of-artificial-intelligence/

State Council of the PRC. July 20, 2017. "Next-Generation AI Development Plan." https://na-production.s3.amazonaws.com/documents/translation-fulltext-8.1.17.pdf.

Stepanov, A.V. 2021. "Issues of safety in employing AI in military systems (Вопросы безопасности применения искусственного интеллекта в системах военного назначения)." *Voennaya Mysl'* 4.

T4GS Reports. Feb. 13, 2019. "AI and the Military: Forever Altering Strategic Stability." http://www.tech4gs.org/ai-and-human- decision-making.html.

Talmadge, Caitlin. 2017. "Would China Go Nuclear? Assessing the Risk of Chinese Nuclear Escalation in a Conventional War with the United States." *International Security* 41(4).

Topychkanov, Petr. 2019. “Autonomy in Russian nuclear forces.” In Vincent Boulanin, ed., *The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk*, vol. 1: *Euro-Atlantic Perspectives.* SIPRI. The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk, Volume I, Euro-Atlantic perspectives | SIPRI.

US Department of Defense. 2018. *2018 Nuclear Posture Review Final Report*. https://media.defense.gov/2018/Feb/02/2001872886/-1/-1/1/2018-NUCLEAR-POSTURE-REVIEW-FINAL-REPORT.PDF

US Department of Defense. 2019. *Summary of the 2018 Department of Defense Artificial Intelligence Strategy: Harnessing AI to Advance Our Security and Prosperity.* https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/SUMMARY-OF-DOD-AI-STRATEGY.PDF.

Van Evera, Stephen. 1998. "Offense, Defense, and the Causes of War." *International Security* 22(4).

Vaynman, Jane. Fall 2021. “Better Monitoring and Better Spying: The Implications of Emerging Technology for Arms Control.” *Texas National Security Review* 4(4). http://dx.doi.org/10.26153/tsw/17498.

Zaloga, Steven J. 2002. *The Kremlin’s Nuclear Sword: The Rise and Fall of Russia’s Strategic Nuclear Forces, 1945–2000*. Washington, DC: Smithsonian Institution Press.

This page intentionally left blank.

This report was written by CNA's Strategy, Policy, Plans, and Programs Division (SP3).

SP3 provides strategic and political-military analysis informed by regional expertise to support operational and policy-level decision-makers across the Department of the Navy, the Office of the Secretary of Defense, the unified combatant commands, the intelligence community, and domestic agencies. The division leverages social science research methods, field research, regional expertise, primary language skills, Track 1.5 partnerships, and policy and operational experience to support senior decision-makers.

Any copyright in this work is subject to the Government's Unlimited Rights license as defined in DFARS 252.227-7013 and/or DFARS 252.227-7014. The reproduction of this work for commercial purposes is strictly prohibited. Nongovernmental users may copy and distribute this document noncommercially, in any medium, provided that the copyright notice is reproduced in all copies. Nongovernmental users may not use technical measures to obstruct or control the reading or further copying of the copies they make or distribute. Nongovernmental users may not accept compensation of any manner in exchange for copies.

All other rights reserved. The provision of this data and/or source code is without warranties or guarantees to the Recipient Party by the Supplying Party with respect to the intended use of the supplied information. Nor shall the Supplying Party be liable to the Recipient Party for any errors or omissions in the supplied information.

This report may contain hyperlinks to websites and servers maintained by third parties. CNA does not control, evaluate, endorse, or guarantee content found in those sites. We do not assume any responsibility or liability for the actions, products, services, and content of those sites or the parties that operate them.

Dedicated to the Safety and Security of the Nation

CNA is a not-for-profit research organization that serves the public interest by providing in-depth analysis and result-oriented solutions to help government leaders choose the best course of action in setting policy and managing operations.

IRM-2023-U-035284-Final

3003 Washington Boulevard, Arlington, VA 22201
www.cna.org 703-824-2000