I. Executive Summary

1. Macrotrends

> Nuclear non-use is not an inherently permanent achievement. It is a condition that must be secured by each successive generation of leaders adjusting ... to a technology evolving at unprecedented speed.[a]

[a]Henry A. Kissinger, Eric Schmidt, and Daniel Huttenlocher, *The Age of AI: And Our Human Future* (New York: Little, Brown and Company, 2021), 89.

Rapid advancements in artificial intelligence (AI), robotics, big data, ubiquitous sensing, space commercialization, and other technologies are re-configuring the technological and strategic foundations of nuclear security.[1] These technologies are progressively interacting in complex ways, giving rise to new systems and capabilities that are disrupting traditional assumptions, systems, and practices for sustaining nuclear deterrence, yet their security-based externalities are often occluded within governments. Unlike previous technological breakthroughs that shaped nuclear security such as atomic energy, digital computing, and space flight—which were driven by governments—today's technological revolution is dominated by the private sector, whose political economy and governance are outside of, and distinct from, governments.

This report:

(i) explores how these technologies are reshaping nuclear security;
(ii) limns the key technological trends driven by the private sector that are generating new nuclear-security risks;
(iii) isolates novel opportunities for reducing nuclear risks; and
(iv) recommends steps for strengthening security.

The findings are grounded in research and in-depth interviews with prominent experts in nuclear security and emerging technologies.[2]

The immense destructive power of nuclear weapons led to the development of a complex and interconnected system during the Cold War, which was imagined, designed, and built by governments over decades. The system encompasses nuclear-deterrence strategies, arms-control agreements, nuclear-weapons policies and postures, nonproliferation measures to halt the spread of nuclear weapons and technology, efforts to secure global nuclear materials and weapons, restrictions on access to nuclear technology, and efforts to approach nuclear disarmament.

Today, the nuclear-security system is progressively entangled with emerging technologies developed in the private sector, not by governments. However, neither the private sector nor governments are working toward a comprehensive understanding of the scale and nature of the technological revolution for nuclear security, nor what tools are necessary to ensure that the interlocks designed to prevent the use of nuclear weapons remain effective in the future. Nuclear strategy remains stuck in decades-old thinking, and current debates within the U.S. Government largely center on replacing legacy nuclear-weapons platforms, while neglecting the need to adapt nuclear-deterrence architecture, strategy, and force posture to these transformational shifts.

Some world leaders express appropriate caution not to cede command-and-control authority over

[1]"Emerging" technology (or, technologies) denotes those which (i) are rapidly advancing in capability, diffusion, or autonomy; (ii) compress decision time or expand operational reach; and (iii) can perturb nuclear deterrence, escalation control, or command-and-control by altering sensing, attribution, targeting, or human judgment.

[2]Warren M. Stern, "Revolution in Nuclear Detection Affairs," *AIP Conference Proceedings* 1596 (2014): 219–225, esp. 220; PDF, https://web.archive.org/web/https://pubs.aip.org/aip/acp/article-pdf/1596/1/219/11651607/219_1_online.pdf.

nuclear weapons to AI and to ensure there will always be a "human in the loop" for nuclear-weapons command decisions. Some prioritize preventing AI from revealing "nuclear secrets" that might give rogue states or terrorists access to nuclear weapons. However, relatively little attention has been paid to the possibility that the convergence of emerging technologies may pose new risks to nuclear security by challenging the systems and approaches that nuclear-armed states use to prevent nuclear war and to "control" nuclear weapons.

Taxonomizing nuclear-security risks and opportunities emerging from the private sector and commercial innovation is a herculean undertaking. The ideas shaping the world of technological innovation evolve rapidly and do not typically overlap with those that have traditionally shaped nuclear security. Adding to the challenge is that these technologies do not operate in isolation: they interact with, and amplify, each other's impact in unpredictable ways. To understand the implications of today's technological changes requires looking not just at AI in isolation, but at how AI is converging with other emerging technologies to potentially transform the entire nuclear-weapons enterprise.

Three trends emerging from commercial innovation are particularly significant for nuclear security:

1. **Radical Transparency**—as the ability to track the location, physical parameters, and status of anything in the world grows, it becomes harder to conceal or protect objects, actions, and information, and easier to reveal them;
2. **Distributed Effects**—with radical transparency, it is increasingly possible to affect people or objects regardless of their number or physical location; and
3. **Changes to Human Control**—machines can now process data at immense volumes and speeds beyond human capacity, changing how much control humans can maintain over outcomes.

These trends create significant risks for nuclear security as well as opportunities. Whether governments will be successful in mitigating risks and reaping the benefits of the technological revolution depends on whether there is leadership that can move away from traditional approaches and thinking about nuclear security.

2. Risks and Opportunities

The nuclear-security risk identified most frequently by the experts interviewed for this study is the growing vulnerability of nuclear forces in an evolving technological landscape. Increasingly sophisticated data collection could expose sensitive information about nuclear arsenals, while adversaries could manipulate the informational environment by deliberately introducing false data. Together, these constitute a breadth of novel forms of attack difficult to fully anticipate and with unknown implications for nuclear deterrence. One particularly concerning scenario is the erosion of confidence in nuclear-weapons systems or the organizations responsible for them, which could fundamentally undermine strategic stability.

Other risks that surfaced include the creation of new pathways to inadvertent nuclear-weapons use via conventional weapons, such as hypersonic weapons, and the rapidly increasing public-private entanglement in space-based assets. Interviewees also shared their concerns that the convergence of emerging technologies could lower technological barriers to nuclear proliferation and nuclear terrorism.

Interviewees identified opportunities for nuclear security emerging from the convergence of emerging technologies. The most frequently cited opportunity is the ability for states to enhance the reliability of warnings of attacks on nuclear forces. By reducing uncertainty during crises, minimizing false warnings of nuclear attack, and creating more opportunities for de-escalation, technologies could lower the risk of nuclear catastrophe. Other opportunities include the potential for governments to shape a new form of deterrence resilience, making nuclear forces, enabling systems, and human

decision makers and operators better able to resist novel forms of attack or degradation. Finally, interviewees noted that emergent technologies could enable a more robust approach to nuclear arms control, nonproliferation, threat reduction, and nuclear disarmament, ensuring that the best available technology is applied to preventing the spread and the use of nuclear weapons.

To mitigate these risks, reap the benefits of the technological revolution, and ultimately avoid nuclear weapons' use, it is critical that governments adapt their nuclear systems to a new security landscape—one defined by rapid technological progress.

3. Recommendations

The analysis underscores the urgent need for governments to have a road-map of actions to address the nuclear-security effects of emerging technologies. They will need a broader innovation agenda focused on adapting their strategies for preventing nuclear catastrophes to fit the converging landscape of emerging technologies and nuclear security. Rather than merely proceeding with a modernization program of one-for-one replacement of legacy nuclear-weapons platforms, re-centering cutting-edge science and technology in the nuclear-security enterprise will allow for greater deterrence resilience to avoid situations in which governments must choose between capitulation or the sheer extancy of nuclear stockpiles, as well as new pathways to use technology-enabled cooperation to prevent nuclear deterrence instability, arms racing, proliferation, and terrorism.

The U.S. Congress should establish a Task Force on Artificial Intelligence, Strategic Stability, and Nuclear Risk—modeled on the National Security Commission on AI—charged with producing a comprehensive report with recommendations for nuclear-security technology development, diplomatic engagement, and public-private partnerships.

Any effective governance of AI and emerging technologies will require ambitious collaborative initiatives between governments and leading technology innovators in the private sector. These initiatives will need to incorporate new kinds of expertise and anticipate emerging capabilities on the horizon, which are likely to result from interactions between novel technological advances. The U.S. Government should create structures and incentives to fully engage the private sector in nuclear-security innovation. These could include the creation of a Nuclear Security Innovation Unit modeled after the Defense Innovation Unit; the creation of a Nuclear Security Development Agency modeled on the Space Development Agency; and a NucWERX program modeled on AFWERX and SpaceWERX.

II. Context and Method

As noted in the Executive Summary (n. 2), taxonomizing nuclear-security risks and opportunities in a commercial innovation environment is difficult. This section specifies the study's method: it develops a conceptual apparatus that can be shared between nuclear-security and emerging-technology leaders, and it sets out how interview judgments were elicited, normalized, and aggregated. A fully self-contained methodological addendum, including the complete Soufflé program and data-model definitions, appears as Appendix B.

The data and key findings in this report are derived from structured interviews with experts in nuclear security and technology innovation (see n. 2). The interview questions included the following:

- What are the risks arising from the convergence of AI and other emerging technologies that increase the risk of nuclear-weapons use?
- What are the opportunities arising from the convergence of emerging technologies for preventing the use of nuclear weapons?
- In what ways might the intersection of emerging technologies make nuclear-weapons use more or less likely?
- To what extent are key stakeholders considering the potential effects of the intersection of emerging technologies on nuclear force structure, doctrine, and policy?
- What aspects of the nuclear-security implications of the intersection of emerging technologies merit more attention?
  - In the United States?
  - On a global scale?
- What investments should be made, and by whom?
  - Which tools of governance should be used to reduce the likelihood of, and to prevent, nuclear-weapons use in the age of AI?
  - By whom?

The study team conducted follow-up interviews soliciting reactions to preliminary findings from C-suite executives and members of existential-risk organizations' boards, in light of their scientific and technical expertise.

1. Delphi Elicitation and Synthesis

The interview program was operationalized as a two-round Delphi-style elicitation layered atop semi-structured interviews. Round I captured free-form judgments and causal accounts. Round II returned a structured claim set to participants for scoring, disagreement annotation, and pinpointed revision. Scores were recorded on a 1–9 scale (1 = negligible strategic effect; 9 = catastrophic and near-term), with experts permitted to attach conditionality (triggering assumptions) as text strings retained as part of the coded corpus.

2. Coding, Propositions, and Auditability

All interview-derived statements were normalized into proposition identifiers (P-codes), preserving the speaker's modal qualifiers while enforcing single-claim granularity per code. Each proposition was then tagged by domain (NC3, ISR, cyber, human layer, space, hypersonics, enrichment, verification, and related domains) and mapped to the risk-opportunity taxonomy frozen in the Table of Contents. This yields an auditable edge list: (a) expert → (b) proposition → (c) risk or opportunity node.

3. Formal Aggregation via Soufflé

To prevent narrative drift and to guarantee that rankings remain mechanically reproducible, the coded corpus was compiled into a Datalog program (Soufflé) that computes (i) weighted mean scores, (ii) distributional robustness statistics on the discrete 1–9 scale (weighted median and interquartile range), and (iii) tier assignments under a fixed decision rule. The program emits an allocatory matrix from ranked risks to the Recommendations.

Color key for Soufflé

Directives
Relations
Types
Aggregates
Thresholds
Strings
Operators

Listing 1: Definitions of aggregatory and ranked relations

```
.decl wmean_num(p:symbol, num:float)
wmean_num(p, num) :-
  vote(e,p,2,score),
  expert(e,_,w),
  num =sum w*score.

.decl wmean_den(p:symbol, den:float)
wmean_den(p, den) :-
  vote(e,p,2,_),
  expert(e,_,w),
  den =sum w.

.decl n_votes(p:symbol, n:number)
n_votes(p, n) :-
  vote(_,p,2,_),
  n =count : { vote(_,p,2,_) }.

.decl agg(p:symbol, wmean:float, n:number)
agg(p, wmean, n) :-
  wmean_num(p,num),
  wmean_den(p,den),
  n_votes(p,n),
  den >0.0,
  wmean =num / den.

.decl ranked(node:symbol, risk:symbol, subrisk:symbol, wmean:float)
ranked(node, risk, subrisk, wmean) :-
  proposition(p,node,_),
  risk_node(node,risk,subrisk),
  agg(p,wmean,_).
```