

Introduction: Emerging Technologies and the Future of Strategic Stability

Harold Trinkunas and Herbert S. Lin



Emerging technologies developed since the end of the Cold War—and their proliferation to new actors—call into question the prospects for strategic stability in the twenty-first century. Strategic stability exists when rivals are mutually deterred and lack any rational incentive to escalate to nuclear use during conflict. Yet, as this issue’s Roundtable examines, emerging technologies—with their new knowledge and tools with the potential for enhancing military capabilities—are impacting stability in such ways that the assumptions of rationality and deterrence no longer hold. First, these emerging technologies may be able to achieve effects once reserved to nuclear weapons, creating incentives for preemption. Second, these technologies are proliferating horizontally across more states, complicating mutual deterrence. Third, such technologies affect the psychology of decision-makers during crises, undermining rationality. Just as these phenomena may undermine stability, however, adversaries may yet be able to use the very same technologies to restore the strategic balance, although how is not yet fully apparent.

During the Cold War, strategic stability between the United States and the Soviet Union rested on each state’s possession of nuclear weapons, which created incentives for restraint in the competition between these rival superpowers. Yet emerging technological developments since the end of the Cold War—both in the nuclear and (especially) non-nuclear domains—and their proliferation to new actors and emerging powers place strategic stability in the twenty-first century increasingly in question.

Strategic stability has traditionally been understood as the condition in which rivals are mutually deterred and lack the incentive to escalate during conflict. Some theories assumed that the possession of nuclear weapon was stabilizing; deterrence was usually straightforward because would-be adversaries made rational calculations that the costs of initiating an attack would be higher than any conceivable benefits and thus would refrain from attacking.

Yet scholars and policymakers often worried about exceptions to this rule, asking whether incentives existed to cross the threshold of nuclear weapons use during crises, with the implicit presumption that an

absence of such incentives contributes to stability. Thomas Schelling, perhaps the best-known American strategic theorist in the Cold War, was particularly concerned with the dynamics of state behavior at the nuclear threshold. In addition, other scholars began to realize that stability includes more than the question of nuclear attack. As Francis Gavin observes in his essay on Schelling’s work in this Roundtable, strategic stability has a vertical component—mutual deterrence among rivals due to the existential risk posed by nuclear weapons use—as well as a horizontal component—the proliferation of new, militarily useful technologies to additional powers.

The emerging technologies that are the focus of this issue call into question whether strategic stability as it was originally conceptualized is still possible. First, it is possible to envision using these technologies during crises to achieve effects once reserved to nuclear weapons—such as using non-nuclear or conventional military capabilities to paralyze or limit the viability of a retaliatory second strike.¹ This scenario may create incentives for preemption. Second, the emerging technologies discussed here are also proliferating horizontally across more states, calling into question the

1 Stephen J. Lukasik, “To What Extent Can Precision Conventional Weapons Substitute for Nuclear Weapons?,” in *The Next Arms Race*, ed. Elbridge A. Colby and Michael S. Gerson (US Army War College, 2012).

assumption of bilateral mutual deterrence that underpins classic strategic stability. And third, contributors to this Roundtable identify ways in which emerging technologies put strategic stability at risk through their impact on the psychology of decision-makers during crises. This development undermines the presumption of rationality, and also shapes decision-making prior to crises when new weapons are being tested and fielded in response to emerging technology hype, as Herbert Lin, Michael Horowitz, and Cameron Tracy examine in their essays.

Emerging technologies encompass new knowledge and tools with the potential for enhancing military capabilities. As such, they may not yet have been fully fielded or routinely incorporated into advanced militaries, although they may be available to a limited degree for use by specialized units. Some of the technologies analyzed here are more mature and closer to full incorporation, such as cyberweapons, which Jacquelyn Schneider describes in her contribution to the Roundtable; other technologies, such as the application of artificial intelligence (AI) and machine learning to military problems, are still evolving, as Horowitz discusses in his essay.²

Since the turn of the century, Chinese, Russian, and US concerns about the impact of emerging technologies have been compounded by the effects achieved in initial deployments during conflicts. Russian use of cyberweapons against Estonia (2008), Georgia (2012), and Ukraine (2014 and 2022) raised fears of the potential impact on the security of nuclear command and control.³ Allegations of US and Israeli collaboration in the deployment of the Stuxnet virus (2010) to sabotage the Iranian nuclear program's centrifuges showed the potential for cyberweapons to have physical effects.⁴ Chinese (2007) and Indian (2019) launches of anti-satellite weapons highlight the risk to space-based intelligence and surveillance platforms critical to both conventional and nuclear capabilities of the great powers, especially when nuclear and conventional warning systems are comingled.⁵ The Ukraine-Russia war (2022–present)

has witnessed the use of hypersonic weapons. The United States government has acknowledged the use of cyber capabilities in both Operation Midnight Hammer against Iranian nuclear facilities in 2025 and against Venezuela in January 2026.⁶

The growing use of AI in a wide range of systems with military applications also increases risk, as Horowitz discusses in his essay. Safety failure modes seen in civilian systems—deriving from issues related to adversarial data poisoning, homegrown algorithmic biases, and poorly developed training datasets—may spill over into conflicts with lethal and escalatory effects. Alternatively, the combination of ubiquitous sensors, AI-powered processing of intelligence data, and advanced conventional precision-strike capabilities may put second-strike mobile nuclear platforms at risk. In other words, non-nuclear and advanced conventional capabilities may achieve effects on adversary nuclear forces without the first use of nuclear weapons.

Emerging technologies, however, also have the potential to contribute to strategic stability.

Emerging technologies also have the potential to impact the psychology of human decision-making during crises in ways that undermine strategic stability. For example, a number of emerging technologies compress time frames and create conditions that deviate from expectations, thus increasing the risks of misperception and miscalculation during a crisis. By challenging or upsetting well-established policymaker expectations and organizational routines in the midst of crisis, new technologies may pose novel threats and thus may collide with human cognitive and organizational limitations to produce unexpected, unintended, and potentially catastrophic consequences involving

2 Here we rely on Chyba's definition of new technologies (or as we term them, emerging technologies) that are militarily useful but not yet widely fielded. See Christopher F. Chyba, "New Technologies & Strategic Stability," *Daedalus* 149, no. 2 (April 2020): 150–70, https://doi.org/10.1162/daed_a_01795. This definition is similar to the one implicitly used by the authors in Todd S. Sechser, Neil Narang, and Caitlin Talmadge, "Emerging Technologies and Strategic Stability in Peacetime, Crisis, and War," *Journal of Strategic Studies* 42, no. 6 (2019): 727–35, <https://doi.org/10.1080/01402390.2019.1626725>.

3 Mark Temnycky, "Russian Cyber Threat: US Can Learn from Ukraine," *Atlantic Council*, May 27, 2021, <https://www.atlanticcouncil.org/blogs/ukrainealert/russian-cyber-threat-us-can-learn-from-ukraine/>; David Cattler and Daniel Black, "The Myth of the Missing Cyberwar," *Foreign Affairs*, April 13, 2022, <https://www.foreignaffairs.com/articles/ukraine/2022-04-06/myth-missing-cyberwar>.

4 Kim Zetter, "An Unprecedented Look at Stuxnet, the World's First Digital Weapon," *Wired*, November 3, 2014, <https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/>.

5 James M. Acton, "Escalation Through Entanglement: How the Vulnerability of Command-and-Control Systems Raises the Risks of an Inadvertent Nuclear War," *International Security* 43, no. 1 (2018): 56–99, https://doi.org/10.1162/isec_a_00320.

6 Mark Pomerleau, "Cyber Command Supports Strikes on Iran's Nuclear Facilities, but Officials Keep Details Under Wraps," *DefenseScoop*, June 23, 2025, <https://defensescoop.com/2025/06/23/cyber-command-supports-attack-iran-nuclear-facilities-midnight-hammer/>; Dana Nickel and Maggie Miller, "Maduro's Fall Puts US Cyber Power in the Spotlight," *Politico*, January 5, 2026, <https://www.politico.com/newsletters/weekly-cybersecurity/2026/01/05/maduros-fall-puts-us-cyber-power-in-the-spotlight-00710452>.

the use of nuclear weapons.⁷ Others may contribute to overconfidence among decision-makers, increasing the likelihood of risky behavior during crises. Even AI decision aids may fail by producing so-called “hallucinations.” The net result of these developments is a growing risk of deterrence failures and crisis escalation across technological domains that could increase the danger of nuclear war.⁸

Emerging technologies, however, also have the potential to contribute to strategic stability. Well-developed cybersecurity organizations and technologies help to secure command-and-control networks during crises, allowing military leaders and policymakers to reliably convey their intent to forces in the field. Cyber espionage on opponents’ networks may contribute to an improved understanding of adversary intentions and capabilities before and during a crisis. Robust AI and machine learning applied to gathering, sifting, and analyzing data during crises may help decision-makers better discern signals within the noise, reducing misperception and allowing them to make decisions that are better suited to de-escalation. Space-based surveillance platforms provide crucial data and additional time for military staffs and civilian policymakers to understand the evolution of crises, relieving some of the pressure to make decisions quickly. Advanced conventional munitions able to strike with high degrees of precision at very long ranges offer additional options for policymakers to respond during crises. While it is true that these weapons allow states to achieve effects that previously would have required the use of nuclear weapons, the upside is that they offer options to avoid crossing the critical nuclear threshold.

The return of great-power rivalry in the twenty-first century, a recent concern of international relations scholars and policymakers,⁹ risks producing open conflict, as Russia’s 2022 invasion of Ukraine demonstrates. This war has featured the use of advanced ballistic missiles,¹⁰ hypersonic munitions,¹¹ and cyberweapons.¹² The effects of these weapons remain to be fully determined, but their efficacy has deviated from prewar predictions, as Tracy discusses in his essay. The US and its NATO allies responded to Russia’s invasion with all measures short of war, including unprecedented levels of intelligence support, economic and diplomatic sanctions, and transfers of advanced anti-tank and anti-air munitions to Ukraine. Ukraine itself has engaged in unprecedentedly rapid innovation in the application of emerging technologies for its own defense, particularly the use of air and sea drones and now increasingly advanced cruise missiles. The conflict has also attracted thousands of international volunteers, including “virtual” freelancers engaged in cyberattacks on Russia.¹³ Russia has in turn appealed to traditional allies in Central Asia and North Korea, and to China for additional material support.

This conflict showcases the continuing problem of nuclear deterrence. Early in the conflict, Russian President Vladimir Putin placed Russian nuclear forces on a “special combat duty regime,”¹⁴ a move that was widely interpreted as intending to deter NATO intervention in Ukraine. This measure raised alarm in the West among the public and leaders as the specter of nuclear conflict once again came to the fore. In addition, it is clear that in the fall of 2022, the Biden administration was seriously concerned that Russia would resort to battlefield

7 Andrew F. Krepinevich Jr., “The Eroding Balance of Terror,” *Foreign Affairs*, February 2019, <https://www.foreignaffairs.com/articles/2018-12-11/eroding-balance-terror>; Chyba, “New Technologies & Strategic Stability.”

8 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 (April 2017): 50–92, https://doi.org/10.1162/ISEC_a_00274; James N. Miller and Richard Fontaine, “A New Era in US-Russian Strategic Stability: How Changing Geopolitics and Emerging Technologies Are Reshaping Pathways to Crisis and Conflict,” CNAS and Harvard Kennedy School, September 2017, <https://www.cnas.org/publications/reports/a-new-era-in-u-s-russian-strategic-stability>.

9 Matthew Kroenig, *The Return of Great Power Rivalry: Democracy Versus Autocracy from the Ancient World to the US and China* (Oxford University Press, 2020); Bruce Jones, “China and the Return of Great Power Strategic Competition,” Brookings Institution, February 2020, <https://www.brookings.edu/articles/china-and-the-return-of-great-power-strategic-competition/>; Congressional Research Service, “Renewed Great Power Competition: Implications for Defense—Issues for Congress,” Congressional Research Service, March 10, 2022, https://www.congress.gov/crs_external_products/R/PDF/R43838/R43838.92.pdf.

10 John Ismay, “Russia Deploys a Mystery Munition in Ukraine,” *The New York Times*, March 15, 2022, <https://www.nytimes.com/2022/03/14/us/russia-ukraine-weapons-decoy.html>.

11 John Ismay, “Russia Claims to Use a Hypersonic Missile in Attack on Arms Depot in Ukraine,” *The New York Times*, March 19, 2022, <https://www.nytimes.com/2022/03/19/us/politics/russia-hypersonic-missile-attack-claim.html>.

12 James Pearson, “Ukraine Says It Thwarted Russian Cyberattack on Electricity Grid,” *Reuters*, April 12, 2022, <https://www.reuters.com/world/europe/russian-hackers-tried-sabotage-ukrainian-power-grid-officials-researchers-2022-04-12/>.

13 Matt Burgess, “Ukraine’s Volunteer ‘IT Army’ Is Hacking in Uncharted Territory,” *Wired*, March 22, 2022, <https://www.wired.com/story/ukraine-it-army-russia-war-cyberattacks-ddos/>.

14 “Putin Orders ‘Special Service Regime’ in Russia’s Deterrence Force,” *TASS*, February 27, 2022, https://tass.com/defense/1412575?utm_source=thebulletin.org&utm_medium=referral&utm_campaign=thebulletin.org&utm_referrer=thebulletin.org.

nuclear weapons in Ukraine.¹⁵ As Janice Stein has argued, by manipulating psychological uncertainty over the probability of nuclear weapons use, Putin led the Biden administration to more clearly signal the limits of its provisions of advanced military capabilities to Ukraine, even as the US continued to push forward with support for Ukraine, experimenting within the limits of what it understood as Russian nuclear weapons use doctrine.¹⁶ Paradoxically, even as this development slowed US supplies to Ukraine, the Ukrainian state doubled down on the use of emerging technologies—for example, developing substitutes for US capabilities in the area of long-range strike via its own cruise missiles and heavy drones.¹⁷ This example suggests that even the success of nuclear deterrence may unpredictably push the battlefield toward ways of fighting in which emerging technologies can be more decisive.

The use of emerging technologies to improve battlefield effectiveness, however—for example, cyber capabilities used offensively and defensively, space-based platforms used to provide real-time intelligence to commanders in the field, the use of conventional hypersonic and advanced precision-strike munitions to conduct deep strikes into enemy territory—have so far not yet contributed to nuclear escalation. In fact, one interpretation of the nuclear saber-rattling experienced during the first months of the Ukraine conflict is that we are witnessing the stability-instability paradox playing out among great power rivals, with both sides able to conduct operations—Russian aggression on Ukraine and Western deliveries of advanced weapons to Ukraine—that impose serious costs on their rivals while yet fearing to escalate to nuclear weapons use. The lesson to be learned, although it is too early to tell, may be that emerging technologies are in fact militarily useful short of the nuclear threshold, and perhaps too optimistically, offer opportunities to achieve significant battlefield effects short of nuclear use.

Emerging Technologies, Crisis Stability, and the Psychology of Decision-Making

In its focus on the intersection of emerging technologies and strategic stability, this Roundtable examines not only how different characteristics of technology affect stability, but also how these char-

acteristics interact with human choices and biases to impact crises. In particular, we find as an overarching proposition that emerging technologies impact strategic stability by creating incentives for preemption, increasing the risk of misperception and accident, and having a psychological effect on human decision-making through their interaction with cognitive biases. Although these suppositions are not the only possible outcomes of the introduction of new technologies on strategic stability—and under some circumstances these technologies may actually improve deterrence—the Roundtable’s authors are collectively pessimistic in the short to medium term.

Debates on the impact of new capabilities on international conflict and stability are not new. Scholars and policymakers in the 1950s and 1960s, shaped by the experience of two world wars, saw international stability and deterrence as paramount goals in international relations, and in nuclear weapons found a new technology that promised to make great-power wars unwinnable, thereby creating an incentive for avoiding conflict escalation. At the same time, then-new technologies such as powerful nuclear weapons and unstoppable intercontinental ballistic missiles promised unprecedented military capabilities and raised for policymakers the idea that these weapons could be useful for coercive or warfighting purposes. Gavin notes, for example, that the United States has never truly accepted that it should be deterred by adversary nuclear weapons, and its Cold War nuclear war planning reflected this ambition to make such wars winnable.

The tension between the pursuit of strategic stability and the wish for improved coercive or military capability goes beyond nuclear weapons, to include the contemporary crop of emerging technologies such as cyber, AI, space-based, and advanced conventional weapons. In other words, just as airpower in the first half and nuclear weapons in the second half of the twentieth century led to debates among scholars and policymakers on strategic stability, today’s emerging technologies have reignited debate on how the acquisition of new military capabilities might potentially undermine deterrence and strategic stability.¹⁸

All Bad Things Go Together: Eroding Strategic Stability

The potential “real-world” effects of emerging technologies on the survivability of second-strike

15 David E. Sanger, “Biden’s Armageddon Moment: When Nuclear Detonation Seemed Possible in Ukraine,” *The New York Times*, March 10, 2024, <https://www.nytimes.com/2024/03/09/us/politics/biden-nuclear-russia-ukraine.html>.

16 Janice Gross Stein, “Escalation Management in Ukraine: ‘Learning by Doing’ in Response to the ‘Threat That Leaves Something to Chance,’” *Texas National Security Review* 6, no. 3 (Summer 2023): 30–50, <https://doi.org/10.26153/TSW/47414>.

17 David Axe, “Ukraine’s Long-Range Strikes: Photogenic But . . .,” *CEPA*, December 17, 2025, <https://cepa.org/article/ukraines-long-range-strikes-photogenic-but/>.

18 Krepinevich, “The Eroding Balance of Terror.”

capabilities and command and control of retaliatory forces raise concerns about vulnerability to a nuclear first strike.¹⁹ For example, an AI-enabled revolution in global surveillance could combine with swarms of unmanned, long-range, stealthy autonomous systems and superfast munitions to place even the most survivable nuclear retaliatory forces (mobile missiles and ballistic missile submarines) at some additional risk, undermining mutually assured destruction and potentially encouraging rapid escalation during crises.²⁰ Offensive cyber capabilities could be used, at least in principle, to compromise adversary nuclear command-and-control systems, disconnecting nuclear forces from command authorities or degrading the information transmitted through these systems.²¹ Whereas in the past, attack of adversary nuclear forces was generally considered possible only using nuclear weapons (a point that contributed to strategic stability), the new concern is that a non-nuclear attacker might calculate that an adversary would be more hesitant to respond with nuclear weapons to a non-nuclear attack, even if that attack significantly degraded its own nuclear forces.²² By lowering the certainty of nuclear retaliation, strategic stability could be diminished.

By lowering the certainty of nuclear retaliation, strategic stability could be diminished.

Nations may respond to these new threats against their nuclear forces with changes in force posture and doctrine—changes that could, in turn, further reduce strategic stability. Perhaps the most obvious of such changes would be the adoption of a “lean forward” posture toward the use of nuclear weapons. For example, a nation might place greater reliance on nuclear weapons in its military strategy, lower thresholds for using nuclear weapons, adopt launch-on-warning policies for newly vulnerable

nuclear weapons, place greater emphasis on nuclear preemption of adversary nuclear forces in both weapons acquisition policy and operational policy, and pre-delegate authority to use nuclear weapons from national leaders to commanders in the field to protect against disconnection between the two, which could compromise retaliation.

Yet another aspect of emerging technologies is how they affect various human perceptions in different contexts. For example, it is common today to see dual-purpose military systems and platforms, that is, systems and platforms that serve or support both conventional and nuclear functions. Such systems include advanced precision-strike platforms that can carry either nuclear or conventional payloads, space-based sensors that can provide valuable real-time intelligence and warning of conventional or nuclear missile attacks, and communications networks or facilities that provide real-time connectivity to both conventional and nuclear forces. Attacks on such systems carried out with the intention of degrading or disrupting conventional capabilities could well be misinterpreted as attempts to degrade nuclear capabilities, especially during the initial stages of armed conflict.²³

Limited operational experience with these new technologies has its own effects on perception and decision-making. By definition, new technologies are not associated with a substantial body of operational experience illustrating their benefits and pitfalls. Thus, as Horowitz suggests in his essay on AI and machine learning, it is not surprising to see swings in the level of trust users have in new technologically enabled capabilities—a phenomenon often known as a technology adoption cycle. In such a cycle, the trust level of would-be users swings between irrational skepticism and overconfidence in new systems. Depending on their level of familiarity with emerging technologies and where they are in the cycle, leaders may dismiss new information produced via these capabilities; conversely, they may rely too heavily on such information due to automation bias, which is the tendency to assume that decisions produced by

-
- 19 Matthew Kroenig, “Will Emerging Technology Cause Nuclear War?,” *Strategic Studies Quarterly* 15, no. 4 (2021): 59–73. Kroenig discusses this issue, although he is skeptical that emerging technologies will outweigh the effects of politics and geopolitics of the risk on nuclear war.
- 20 David M. Allison and Stephen Herzog, “Artificial Intelligence and Nuclear Weapons Proliferation: The Technological Arms Race for (In)Visibility,” *Risk Analysis*, September 25, 2025, <https://doi.org/10.1111/risa.70105>.
- 21 Leonard Spector, “Cyber Offense and a Changing Strategic Paradigm,” *The Washington Quarterly* 45, no. 1 (2022): 38–56, <https://doi.org/10.1080/0163660X.2022.2054123>.
- 22 Lukasik, “To What Extent Can Precision Conventional Weapons Substitute for Nuclear Weapons?”
- 23 James M. Acton, “Escalation Through Entanglement: How the Vulnerability of Command-and-Control Systems Raises the Risks of an Inadvertent Nuclear War,” *International Security* 43, no. 1 (2018): 56–99, https://doi.org/10.1162/isec_a_00320; Alexey Arbatov et al., “Entanglement as a New Security Threat: A Russian Perspective,” ed. James M. Acton, in *Entanglement: Chinese and Russian Perspectives on Non-Nuclear Weapons and Nuclear Risks*, (Carnegie China, 2017), 25–26.

machines are inherently less biased than those made by human beings.²⁴

Operators suffer from their own version of this problem. Automation of alerts and false alerts was already a concern during the Cold War; both the Soviet Union and the United States experienced incidents that raised false alarms of nuclear attack, and retaliation was only avoided by individuals who used their better judgment to second-guess the machines and the automation. The sources of these incidents can be remarkably (and terrifyingly) mundane. In his book *Limits of Safety*,²⁵ Scott Sagan recounts how at the height of the 1962 Cuban Missile Crisis, a perimeter intrusion at a military base near Duluth, Minnesota (by a bear!), set off alerts that propagated through military bases in the region. At Volk airfield in Wisconsin, however, the wrong alarm—announcing the start of a shooting war—was sounded. Fortunately, a base officer recognized the mistake before nuclear-armed interceptors were launched in the conviction that a shooting war had started.

AI-enabled services that assist humans in data interpretation may not have been realistically trained on real-world events involving nuclear weapons, given the very small number of cases available, and unlike a human making a judgment call, these systems may not be able to explain their rationales for particular conclusions or recommendations. AI-enabled services for military purposes may not have access to a full range of data on which to train and make decisions if they are restricted to classified systems only, or where the data available on classified systems is systematically different from that available in open-source training sets. This scenario is particularly true of nuclear crises, where little historical or contemporary data is available, or of cyberattacks and cyber defense, where specific cases only sporadically come to light, presumably because they have spectacular or notable effects, and thus likely differ from the daily routine of such operations. This situation increases the chance that there will be “gaps” between the assessment or pre-

dictions produced by systems trained on classified data versus open-source data. In addition, when there is little to no data, such data might have to be created “synthetically” via simulations and war games, which may create additional risks of erroneous predictions or assessments during crises.²⁶ Even if data is available, military organizations around the world have an incentive to attack adversary data-collection systems and degrade data quality to affect the ability of AI to effectively assist human decision-making.²⁷ Under these conditions, how likely human operators are to trust and correctly interpret these conclusions or recommendations is an open question.

One final aspect of many emerging technologies is that they shorten timelines and increase the volume of dataflows during crises, both of which can increase pressure on human decision-makers. Intense time pressures decrease the quality of human performance and decision-making.²⁸ One reason is that compressed decision timelines often lead people to invoke less-optimal heuristic thinking strategies, as described below. Compressed timelines are thus in themselves detractors from strategic stability.

Recent findings from behavioral psychology and economics increasingly make clear that the rationality presumption—which forms a cornerstone of previous thinking on strategic stability—is untenable, either with nuclear weapons per se or with new technologies of military relevance. In particular, as we will see in the discussion that follows, emerging technologies seem to compress timelines and maximize the likelihood of relying on heuristic thinking (using mental shortcuts to make decisions); neither of these conditions is likely to improve the odds of producing rational decisions, especially in leaders burdened by stress, age, and mental health challenges. For example, the Ukraine-Russia war has raised questions of the mental health and cognitive stability of Russian President Vladimir Putin, and of how this might affect decisions on crisis management and escalation,²⁹ thus vividly calling into

24 Michal Onderco and Madeline Zutt, “Emerging Technology and Nuclear Security: What Does the Wisdom of the Crowd Tell Us?,” *Contemporary Security Policy* 42, no. 3 (2021): 286–311; James Johnson, “‘Catalytic Nuclear War’ in the Age of Artificial Intelligence & Autonomy: Emerging Military Technology and Escalation Risk Between Nuclear-Armed States,” *Journal of Strategic Studies* (January 13, 2021): 1–41, <https://doi.org/10.1080/01402390.2020.1867541>; James Johnson, “Delegating Strategic Decision-Making to Machines: Dr. Strangelove Redux?,” *Journal of Strategic Studies* 45, no. 3 (2022): 439–77, <https://doi.org/10.1080/01402390.2020.1759038>.

25 Scott D. Sagan, *The Limits of Safety: Organizations, Accidents, and Nuclear Weapons* (Princeton University Press, 1995).

26 Max Lamparth et al., “Human vs. Machine: Behavioral Differences Between Expert Humans and Language Models in Wargame Simulations,” *Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society* 7 (October 2024): 807–17, <https://doi.org/10.1609/aiies.v7i1.31681>.

27 Avi Goldfarb and Jon Lindsay, “Prediction and Judgement: Why Artificial Intelligence Increases the Importance of Humans in War,” *International Security* 46, no. 3 (Winter 2021/2022): 7–50.

28 For a literature review on this point, see D. A. Moore and E. R. Tenney, “Time Pressure, Performance, and Productivity,” *Research on Managing Groups and Teams* (2012): 15, 305–26.

29 Scott D. Sagan, “The World’s Most Dangerous Man,” *Foreign Affairs*, March 22, 2022, <https://www.foreignaffairs.com/articles/russian-federation/2022-03-16/worlds-most-dangerous-man>; Charles B. Strozier and David M. Terman, “Putin’s Psychology and Nuclear Weapons: The Fundamental Mindset,” *Bulletin of the Atomic Scientists* 78, no. 6 (2022): 310–14.

question the key assumption of the rationality of state leaders. The interaction of these questions with the cognitive bias issues introduced by emerging technologies has potentially grave consequences.

Rationalist theories of deterrence and strategic stability emerged in the 1960s when economist Thomas Schelling and his contemporaries hypothesized that stability was the product of rational calculations about the unwinnable nature of nuclear war once adversaries had achieved secure second-strike capabilities. If this hypothesis is valid, the threat of state-ending retaliation in the event of launching a nuclear attack would inevitably deter great powers from allowing conflicts to escalate and cross the nuclear threshold, thus reinforcing strategic stability.

A great deal of work in psychology done since then, however, has resulted in the new field of behavioral psychology, which is founded on the now well-documented notion that human beings do not always make decisions based on rational economic calculations. Although scholars have always recognized the rational decision-making human being as an idealized construct, traditional decision theory has nonetheless assumed that, in practice, the deviations from rational decision-making were small and random.

Behavioral economics and psychology find instead that deviations from rationality are large and systematic. Often, these deviations manifest in the use of intuitive, reflexive, heuristic thinking to make decisions, particularly when faced with time pressure, surprise, or other obstacles to deliberate calculation. Behavioral psychology tells us that humans make fast, intuitive judgments rather than using slower, more analytical thinking, even when arriving at an optimal outcome would be more likely with the latter.³⁰

Rose McDermott argues in this Roundtable that these systematic flaws in human cognition are likely to detract from strategic stability, and that emerging technologies are likely to exacerbate this tendency. She writes that human beings are prone to heuristic thinking when facing high-stakes or time-bound decisions—as would be the case in crises with the potential to escalate.³¹ For example, some heuristic biases relate to overconfidence and optimism among leaders, which may lead decision-makers to overestimate their military capabilities or their ability to accurately predict outcomes. Such biases may be on display in Russian decision-making on invading Ukraine, where against stiff Ukrainian

resistance, Russian forces have not experienced the lightning-quick victory they had apparently expected.³² If this situation were to interact with the optimism phase of the technology adoption cycle described by Horowitz, the effect could be even larger than otherwise expected.

It is at least theoretically possible that emerging technologies will alter cost-benefit calculations to favor a defender by increasing the risk associated with preemption.

In addition, Herbert Lin's contribution in this issue illustrates how, at least in the case of the United States, human cognitive limitations and biases can affect military capabilities long before crises begin, during the defense selection and acquisition process itself. In the United States, the preference for substituting technology in place of manpower for defense purposes has produced a system occasionally prone to unreasonable technological optimism. This techno-optimism is not simply the product of systematic cognitive biases during the selection, acquisition, and fielding of new capabilities; Lin shows that it is reinforced by cultural and institutional biases toward new technologies, even in cases where sober analysis of the technology and surrounding organization and doctrine might suggest that success is unlikely.³³

The Devil's Advocate: Might Emerging Technologies Bolster Strategic Stability?

Although this Roundtable's contributors are generally skeptical of the possibility that emerging technologies will contribute to strategic stability, we sketch out three pathways by which this could happen. A number of the contributors make policy recommendations in their essays about how to make these positive outcomes more likely.

30 Daniel Kahneman, *Thinking, Fast and Slow* (Farrar, Straus and Giroux, 2011).

31 See Rose McDermott's article, "The Influence of Psychological Factors in the Search for Strategic Stability," in this same issue of *Texas National Security Review*.

32 An alternative explanation is that Putin, in particular, has not received good information from subordinates, who may well have been afraid to tell him the truth about actual Russian military readiness or the disposition of the Ukrainian people towards Russia. Of course, both explanations could be true at the same time as well. See Sagan, "The World's Most Dangerous Man."

33 See Herbert S. Lin, "On Optimism About New Military Technologies," in this same issue of *Texas National Security Review*.

Emerging Technologies May Eventually Favor the Defender

It is at least theoretically possible that emerging technologies will alter cost-benefit calculations to favor a defender by increasing the risk associated with preemption. For example, even AI-enabled intelligence and surveillance networks that are ubiquitous can be spoofed so that they deliver erroneous data or no data at all to attackers. A micro-level example of this can be found in the 2019 Hong Kong protests against heavy-handed Chinese rule, where protesters learned to dazzle surveillance cameras with handheld lasers as well as use masks and umbrellas to prevent facial recognition software from working effectively.³⁴ Who is to say that the same approach to spoofing intelligence, surveillance, and reconnaissance systems cannot be done to ensure the survival of mobile second-strike nuclear forces, at least to such an extent that any potential attacker might doubt that the benefits of a first strike would outweigh the costs? Similarly, AI training sets are vulnerable to adversarial attacks such as data poisoning and training set manipulation via cyber intrusions, casting doubt on their reliability as intelligence-interpreting technologies capable of detecting adversary second-strike forces with sufficient accuracy.³⁵ Concerns about attacks on space-based ISR platforms could be countered through the proliferation of mini and micro satellites to produce deep redundancies in these systems. The threat of surprise attack via hypersonic missiles (for example, over the South Pole against the United States) can be partially mitigated through developing additional detection networks to maximize warning. All of these examples demonstrate ways in which emerging technologies would favor the defender.

It seems increasingly clear that emerging technologies may provide a limited way around the stability-instability paradox by allowing states to achieve important operational and strategic effects without provoking nuclear retaliation.

The Stability-Instability Paradox: Great Power Edition

Scholars have hypothesized that mutual possession of nuclear weapons by adversaries may not only contribute to stability at the strategic level but also create a permissive environment for sub-strategic

and non-nuclear conflict. The deterrent effect of nuclear weapons permits aggrieved or revisionist states to use conventional or covert attacks on adversaries, much as Pakistan has conducted against India. Pakistani nuclear weapons have thus far deterred major Indian retaliation against terrorist attacks by Pakistan-sponsored non-state armed actors, for example.³⁶

It seems increasingly clear that emerging technologies may provide a limited way around the stability-instability paradox by allowing states to achieve important operational and strategic effects without provoking nuclear retaliation. In the Ukraine-Russia war, most of the focus has been on Putin's nuclear threats, yet the Western nuclear shield also allows quite a range of operations that might once have been considered destabilizing. In addition, the emerging technologies the West has provided Ukraine provide some alternatives for achieving large-scale effects on the battlefield that might have once been deterred by the possession of nuclear weapons. For example, large-scale US and Western deliveries of advanced weapons systems, including emerging technologies such as drones and long-range advanced precision strike to Ukraine are taking place overtly, having been widely announced in the media and by diplomats. For all of Putin's saber-rattling, is anyone convinced that Russia would retaliate with nuclear weapons? At this point, extended saber-rattling undermines Russia's credibility. And as Stein points out, the United States and NATO allies have been able to experiment with where the Russian redline is to deliver advanced weapons and training just short of triggering a Russian response. This assistance includes the latest precision munitions, intelligence sharing that probably includes information gathered by space-based and cyber capabilities, and enhanced cyber defense for Ukraine.³⁷

Achieving Conventional Deterrence for Non-Nuclear Weapons States

The other lesson that may emerge from the Ukraine-Russia war is that the adoption of military capabilities based on emerging technologies may allow non-nuclear weapons states to impose significant costs on nuclear weapons states. As the war has progressed, Ukraine has indigenously (and strikingly rapidly) made progress in certain

34 "Hong Kong Protesters Use Umbrellas, Lasers, and Respirators to Evade Surveillance and Tear Gas," *Reason*, August 9, 2019, <https://reason.com/2019/08/09/hong-kong-protesters-use-umbrellas-lasers-and-respirators-to-evade-surveillance-and-teargas/>.

35 Christopher Whyte, "Problems of Poison: New Paradigms and 'Agreed' Competition in the Era of AI-Enabled Cyber Operations," *2020 12th International Conference on Cyber Conflict (CyCon)* 1300 (May 2020): 215–32, <https://doi.org/10.23919/CyCon49761.2020.9131717>.

36 Bryan R. Early and Victor Asal, "Nuclear Weapons, Existential Threats, and the Stability-Instability Paradox," *The Nonproliferation Review* 25, nos. 3–4 (2018): 223–47, <https://doi.org/10.1080/10736700.2018.1518757>.

37 Charles Maynes, "Russia Sharpens Warnings as the US and Europe Send More Weapons to Ukraine," *NPR*, April 29, 2022, <https://www.npr.org/2022/04/29/1095458518/russia-ukraine-us-military-aid>; Stein, "Escalation Management in Ukraine."

emerging technologies—such as long-range strike drones, interceptor drones, and sea drones—that have allowed it to achieve improved air defenses, attrit the Russian Black Sea fleet, and conduct a strategic bombardment campaign against Russian oil infrastructure, none of which has been deterred by Russian nuclear weapons. The ability of Ukraine to fend off a great-power nuclear weapons state using advanced conventional capabilities, many of which are related to the emerging technologies considered below, may in the future limit the impulse to nuclear proliferation if significant strategic effects can be achieved by defenders without them.

It seems increasingly clear that emerging technologies may provide a limited way around the stability-instability paradox by allowing states to achieve important operational and strategic effects without provoking nuclear retaliation.

At the time of writing, this war is far from over, and it remains to be seen what military and strategic lessons will be drawn from the Ukraine-Russia war. What is already certain, however, is that a much smaller state, Ukraine, has been able to inflict over one million casualties on Russia, destroy over ten thousand armored vehicles, prevent Russia from achieving air superiority, and effectively neutralize Russia's Black Sea fleet.³⁸ While Putin shows no signs yet of moving toward a negotiated solution, the damage Ukraine has been able to inflict using emerging technology may give other potential aggressors pause, even when facing smaller and weaker powers.

Past as Prologue: Keeping Established Technologies (and Humans) in the Loop

It is worth considering that states may be able to mitigate the impact of emerging technologies on strategic stability with a renewed emphasis on

tried-and-true traditional technologies, combined with revised nuclear postures and doctrines, and on keeping the human decision-makers and operators resolutely in the loop.

Two of the major components of the psychological impact of emerging technologies are the compression of time and the role of (mis)trust. Time compression is largely an artifact of some nuclear weapons states' reliance on land-based, fixed-site ballistic missiles that are vulnerable to preemptive strikes. To avert that possibility, for example, the United States has adopted a launch-on-warning posture. But if the land-based component were eliminated and if the responsibility for nuclear deterrence were shifted onto sea- and air-based nuclear weapons platforms, the US would have the possibility of adopting a launch-under-attack posture that would wait until after nuclear strikes had verifiably hit before retaliating. The time pressure would be much less because US nuclear retaliation would not be affected by adversary preemption, and this might dissuade potential attackers from preempting in the first place.

Similarly, tried-and-true hardwired technologies and platforms that are disentangled from other ISR systems and communications channels and that use human operators to detect and issue warnings concerning enemy attack worked well throughout the Cold War; there is arguably no need to improve on them, especially since they are not as vulnerable to disruption by emerging technologies. In fact, the United States and China agreed in 2024 to exclude AI from nuclear command and control.³⁹ The conclusions of many articles in this Roundtable highlight such an approach as a possible path forward toward mitigating the possible negative effects of emerging technologies on crisis stability.

Plan of the Roundtable

The discussion in the following essays brings together scholars of international relations and nuclear security with technology policy experts to better understand the impact of emerging technologies on strategic stability. To do so, the authors reexamine the debates on strategic stability and nuclear weapons that emerged during the 1950s and 1960s to better understand how emerging technologies today might alter the logic of deterrence and mutually assured destruction. Recent insights from cognitive and social psychology of human decision-making are applied to the problem of strategic stability, explaining how some

38 Seth G. Jones and Riley McCabe, "Russia's Battlefield Woes in Ukraine," CSIS, June 3, 2025, <https://www.csis.org/analysis/russias-battlefield-woes-ukraine>.

39 Jarrett Renshaw and Trevor Hunnicutt, "Biden, Xi Agree That Humans, Not AI, Should Control Nuclear Arms," *Reuters*, November 16, 2024, <https://www.reuters.com/world/biden-xi-agreed-that-humans-not-ai-should-control-nuclear-weapons-white-house-2024-11-16/>.

of the fundamental assumptions of rationality during crisis are undermined by known human cognitive biases. These essays explore and draw conclusions on the impact of critical emerging technologies for strategic stability and deterrence: cyberweapons, advanced conventional munitions such as hypersonic missiles, and the application of AI to the military domain.

This Roundtable is concerned with the risks posed by emerging technologies on strategic stability, both because of the effects of new capabilities that alter the cost-benefit calculations on which deterrence assumptions are based, and because our improved understanding of the psychology of decision-making suggests that emerging technologies have distinct and systematic patterns of risk. Emerging technologies may have a direct impact on strategic stability by providing leaders with incentives to strike first or with the capability to ensure that adversaries will not be able to launch effective retaliatory second strikes. Because these technologies are still emerging and are not fully fielded, adversaries do not yet know their full implications for strategic stability, paradoxically creating incentives to adopt riskier nuclear doctrines and postures in an effort to limit exposure to the uncertainty created by emerging technologies.

Emerging technologies also influence strategic stability via a second path—their psychological impact on decision-makers. As several of the essays show, well-known human cognitive biases limit the ability of leaders to correctly assess the cost-benefit analysis of various courses of action during nuclear crises. Emerging technologies also raise the risk of miscalculation and potentially increase the likelihood that nuclear weapons will be used. While most of the Roundtable’s authors are decidedly pessimistic about the impact of emerging technologies, their analyses and insights will equip decision-makers, experts, and citizens to mitigate the risks they identify and to better be able to take advantage of their positive dimensions in ways that enhance strategic stability. ●

Harold Trinkunas is the deputy director of the Center for International Security and Cooperation and senior research scholar at the Freeman Spogli Institute for International Studies at Stanford University. Prior to arriving at Stanford, Dr. Trinkunas served as the Charles W. Robinson chair and senior fellow and director of the Latin America Initiative in the Foreign Policy program at the Brookings Institution. His research focuses on issues related to foreign policy, international security, emerging technologies, and armed non-state actors, particularly in Latin America. Dr. Trinkunas previously served as an associate professor and chair of the Department of National Security Affairs at the Naval Postgraduate School in Monterey, California. He received his doctorate in political science from Stanford University in 1999. He was born in Maracaibo, Venezuela.

Stanford University, Stanford, CA, USA, email: antanas@stanford.edu.

Herbert Lin is a senior research scholar and research fellow at Stanford University, with interests at the intersection of national security and emerging technologies. He is also director of the Stanford Emerging Technology Review (<http://setr.stanford.edu>). Additionally, he is chief scientist emeritus for the Computer Science and Telecommunications Board of the National Academies. He also served on the Science and Security Board of the Bulletin of Atomic Scientists from 2016 to 2025. Lin was a member of President Obama’s Commission on Enhancing National Cybersecurity (2016) and the Aspen Commission on Information Disorder (2020). He was a professional staff member and staff scientist for the House Armed Services Committee, where his portfolio included defense policy and arms control issues. He received his doctorate in physics from MIT.

Stanford University, Stanford, CA, USA, email: herblin@stanford.edu.

Acknowledgments: We are grateful for the support of the Stanton Foundation for this project and its resulting contributions.

Image: DMA Social Media by Katie Lange.⁴⁰

40 For image, see <https://www.dvidshub.net/image/4889623/titan-missile-museum>.

