Strategic Stability and Emerging Russian and Chinese Technologies:

Hypersonic Weapons, Quantum Technologies, and Artificial Intelligence

Juljan Krause,[ab] Kimberly Peh,[b1] and Spenser Warren[ab2]

[a] University of California Institute on Global Conflict and Cooperation

[b] Lawrence Livermore National Laboratory Center for Global Security Research

Introduction

How will emerging advanced technologies affect international stability? Technologies like artificial intelligence, synthetic biology, automation, and autonomous unmanned systems are deemed revolutionary because the unprecedented speed, information, and scale of influence they bring supposedly create a "functionally different" environment which states cannot ignore.[3] New capabilities come with new sources of data that decision-makers need to grapple with. As a recent report from the Center for Strategic and International Studies (CSIS) states, "The increased amount of information itself poses another challenge insofar as processing and deriving useful knowledge from the raw data can be overwhelming for analysts".[4] This intricate problem challenges the idea that more information is always better. Rather, the increase in information demands the need to consume, interpret, and utilize data in different and more effective ways. Yet, despite the changes that may follow the development of advanced technologies, defined here as those which have "not yet been overtly significantly deployed by any nation's military",[5] a fundamental difficulty with studying their impacts is that, by definition, their effects have yet to be seen or fully explored.

Research on this question runs the risk of being overly speculative or repetitive of work that dangerously reduces the impact of technologies to physical properties alone. To avoid both

[1] This work was performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under Contract DE-AC52-07NA27344. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States government or Lawrence Livermore National Security, LLC, and shall not be used for advertising or product endorsement purposes.

[2] Author names are listed in alphabetical order.

[3] Rebecca Hersman et al., "Under the Nuclear Shadow: Situational Awareness Technology and Crisis Decisionmaking," Center for Strategic & International Studies, March 2020, https://www.csis.org/analysis/under-nuclear-shadow-situational-awareness-technology-and-crisis-decisionmaking, 8; Harald Andas, "Emerging technology trends for defence and security," *Norwegian Defence Research Establishment* 20/01050; and Mircea Udrescu and Eugen Siteanu, "Emerging technologies: Innovation, demassification, effectiveness, revolutions in military affairs," *Land Forces Academy Review* 226.4.104 (2021): 299-308.

[4] Hersman et al 2020, 2.

[5] Christopher Chyba, "New technologies & strategic stability," *Daedalus* 149.2 (2020): 152.

shortfalls, we synthesize the debate and outline an analytic framework that focuses on the mechanisms linking technology and stability to guide thinking on this topic.[6]

This approach leads us to identify three sets of mechanisms: whether technologies change states' real or perceived (dis)advantages; influence the level of uncertainty; and affect communication between states. These mechanisms are derived from taking a broad view of stability, which we take to mean the robustness of the prevailing situation to escalatory pressures.[7] Scholars and practitioners typically define stability through its parts: strategic stability, the lack of incentives for states to use force, especially nuclear weapons, against each other; crisis stability, the lack of incentives for states to use nuclear weapons first in a crisis; and arms race stability, the lack of incentives for states to compete through the building of weapons to overcome advantages others might gain from nuclear use. However, each of these definitions is contested and, therefore, complicates building knowledge founded on shared premises.[8] Thus, we adopt a broad view of stability to overcome this definitional problem. The result of this effort is a framework based on the three mechanisms that is not intended to be determinative but serves as a guide to help evaluate the up or downward pressures technologies may have on state behaviors.

The bulk of this brief discusses three key advanced technologies that are currently being developed by Russia and China. These technologies are: hypersonics, artificial intelligence, and quantum technology (see Glossary on quantum technology). This section lays out the current developments in each country to help outline where each country is concentrating its efforts and the level of emphasis each is placing on the different technologies. Here, we narrow in on Russia and China because these are the most likely nuclear-armed countries to make progress in the technological areas we are concerned with, excluding the United States.

Following the discussion and contextualization of Russia and China's technological developments, this brief finally concludes with an application of the framework to illuminate how advancements across the three technologies in Russia and China may influence stability. The tables below preview our key findings.

[6] This approach has two advantages. First, a focus on mechanisms helps anchor our analyses analytically. Research on the effect of technology on stability is not new and has been growing in the light of increasing interest in emerging (disruptive) technologies. As such, theoretical links between mechanisms can be distilled from the literature and used to understand the impacts of currently emerging technologies on stability. Second, this approach ensures that our discussion remains at the strategic level. Stability is a strategic outcome and is influenced by a large confluence of variables like arms control regimes, leaders' perceptions and beliefs, and organizational or bureaucratic cultures within states. However, the immediate effects of technology, such as, speed, range, and accuracy, manifest at the operational level. Hence, without active efforts to maintain discussion at the strategic level, studies sometimes theorize from the operational level and make only cursory links from these operational effects to the strategic outcome. As Chyba notes, despite the speed which hypersonic glide vehicles offer, it is unclear if such change in speed truly changes strategic decisions considering that existing submarine-launched and intercontinental ballistic missiles are already traveling at hypersonic speeds. Put differently, notwithstanding the changes which advanced technologies may introduce at the operational level, their relationship with strategic outcomes remain to be explained because operational-level effects may not translate directly to strategic-level consequences. See Chyba 2020.

[7] Chyba 2020, 151.

[8] Sarah Bidgood, "What we talk about when we talk about US-Russia strategic stability," *Journal for Peace and Nuclear Disarmament* 6.1(2023): 9-27; and Elbridge A. Colby, and Michael S. Gerson, "Strategic Stability: Contending Interpretations," (Carlisle, PA: U.S. Army War College Press, 2013).

Key Findings

Russia	*Change real or perceived (dis)advantages?*	*Influence the levels of uncertainty?*	*Affect communication between states?*
Hypersonic Weapons	**Absence of significant (dis)advantage:** These weapons do not significantly enhance Russian counterforce or counter-NC3 capabilities. Moreover, they neither improve Russian accuracy nor threaten space-based NC3 capabilities. However, hypersonic weapons may strengthen Russian warfighting capabilities to some extent. They may penetrate missile defenses or target critical naval assets more effectively. That said, their use would not be fundamentally different from the use of other Russian nonstrategic nuclear weapons. Tsirkon may threaten American conventional deterrence, eroding intrawar deterrence and escalation management abilities in the naval domain, although the underperformance of Russian hypersonics in Ukraine will likely mitigate these risks by lowering Russian perceptions of their ability. Kinzhal's only truly new ability is its hypersonic velocity. Tsirkon and Avangard combine hypersonic speeds with maneuverability. This speed-maneuverability combination would make each far more challenging to track and hit than Kinzhal or existing systems.	**Potential arms racing or competition in space:** Russia's ASAT weapons pose threats to American NC3 assets in space because it can strike targets, including components of the U.S. NC3 system, in the GEO. Meanwhile, there is no clarity on the nuclear nature of the weapons within the U.S. Intelligence Community.	

Russia	*Change real or perceived (dis)advantages?*	*Influence the levels of uncertainty?*	*Affect communication between states?*
Quantum Technologies	**Capabilities are rudimentary and unlikely to have strategic impacts**	**Potential competition in the development of quantum technology:** How Russia would integrate quantum technologies into its military systems or doctrine remains unknown.	

Russia	*Change real or perceived (dis)advantages?*	*Influence the levels of uncertainty?*	*Affect communication between states?*
AI/ML	**Real advantages can be gained if Russia commits to the development of AI. However, improvements to the survivability of Russia's nuclear arsenal could enhance stability:** AI development is slow, and a mix of strengths and limitations confound Russia's advancements in this area. However, Russia has seen some success in developing AI-enabled EW systems. This capability could enhance Russia's ability to target satellites, degrading American and allied decision-making capabilities during a conflict. The integration of AI into air and missile defenses could also improve the survivability of Russia's nuclear arsenal and increase the effectiveness of its conventional forces. AI is likely to be integrated into Russian early warning systems, which Russian leaders believe would make the nuclear arsenal less vulnerable. Russia may also use autonomous weapons to defend missile silos, which could make silos less vulnerable to saboteurs. AI is also perceived as a tool for finding and exploiting vulnerabilities in adversarial IT systems.	**Doubts in the veracity of information can lead to overall skepticism in attempts to communicate intents and signals:** Russian strategists see AI as a tool of manipulation, enhancing the ability to generate deep fakes and other forms of believable misinformation that confuses adversarial militaries, erode trust in adversary governments, and complicate adversary decision-making.	

China	*Change real or perceived (dis)advantages?*	*Influence the levels of uncertainty?*	*Affect communication between states?*
Hypersonic Weapons	**Real advantages can be achieved if development is successful:** If developed, China's hypersonic FOBS armed with a traditional nuclear-armed reentry vehicle would pose problems due to its ability to strike from vectors where the radars are not looking. Chinese hypersonic weapons alone will have limited impact on American nuclear deterrence because they are poor options for counterforce or counter-NC3 strikes. However, they will likely have significant impacts on American warfighting capabilities in the Pacific should strategic deterrence fail. In addition, Chinese hypersonics can blunt the U.S.'s regional missile defenses, undermining the U.S.'s ability to defend allies in the region and hampering its ability to manage escalation in a regional conflict and degrade intrawar deterrence.	**Uncertainty around China's goals generally raises skepticism in its developments:** While most experts consider China's pursuit of hypersonic weapons to be primarily defensive, China may have secondary offensive intentions—including a desire to achieve regional conventional superiority to prevent an American intervention in the case of regional aggression.	

China	*Change real or perceived (dis)advantages?*	*Influence the levels of uncertainty?*	*Affect communication between states?*
Quantum Technologies	**Significant benefits can be obtained, especially with remarkable progress in some areas:** Quantum computers are likely to improve the Chinese C2 system, which can enhance real-time planning and decision support. On the battlefield, China could also gain an advantage if its automated decision support systems can resolve issues across multiple domains quickly. At present, China is the only power that has access to a quantum satellite, which is a remarkable engineering feat. China has also made impressive progress in developing ground-to-ground repeaters, which can help China and partners (e.g., North Korea) evade sanctions. The goal of Chinese efforts in the advancement of quantum communication is to make progress towards building a rudimentary quantum internet. Success in this area would frustrate the U.S. and allies' intelligence services. In the long term, a Chinese quantum navigation system would help establish a more effective network whilst effectively protecting its networks against cyberattacks.	**Potential problems can arise from entanglement and a lack of clarity in China's plans:** For Chinese strategists, there is no technology that, in principle, is not dual use. There is little information in the public domain on the leadership's and the PLA's vision regarding the strategic implications of quantum technologies for Chinese doctrine, or their operational integration with the Chinese military.	

China	*Change real or perceived (dis)advantages?*	*Influence the levels of uncertainty?*	*Affect communication between states?*
AI/ML	**Real or perceived disadvantages in this area could lead either to restraint or efforts to compensate for weakness:** While China considers AI paramount to its strategic aim to surpass the U.S. militarily, much of the projects and priority areas are aspirational in character. Many Chinese commentators seem to agree that AI will erode strategic stability and complicate China's deterrence relationship with the U.S. Recent analyses of Chinese publications suggest that the Chinese establishment fears that emerging technologies such as AI could undermine "China's second-strike capability and require a reassessment of how asymmetric strategic stability may be restored."	**Potential problems can arise from opacity in China's plans:** The People's Liberation Army (PLA) typically refers to AI-enabled systems in terms of "intelligentized warfare", but the Chinese leadership remains purposefully vague and obscure in its definition of "intelligence," and "intelligentization."	**Preemption can happen due to China's eagerness to integrate AI and automate processes:** AI is assumed to increase risks of miscalculation. The number of preemptive strikes may rise if AI-enabled systems are less risk-averse than human decision-makers.

Framework

Many scholars have studied the effects of specific technologies like artificial intelligence, cyber weapons, and autonomous weapons systems (AWS).[9] Others have engaged the discussion more broadly, evaluating *when* and *whether* technologies matter in influencing escalation. For example, Favaro and Williams argue that the role technologies play in influencing escalation take place prior to crises when their potential advantages prompt leaders to become more confident about the odds of attaining military success.[10] Talmadge implies that the literature overstates the effect of technology and argues, instead, that technologies are only sometimes necessary and hardly sufficient for driving escalation in intra-war settings.[11] Evidently, the debate lacks neither attention nor arguments that seek to specify the relationship between technologies and stability.[12]

As such, rather than add to the number of theoretical arguments, we propose a framework to guide thinking on how emerging technologies influence escalation. This paper is not the first to develop a framework to facilitate this analysis. Chyba, for example, put forth a framework that assesses the effect in three ways: the speed of technological diffusion, the effect of technologies on deterrence and defense, and their impact on crisis decision-making.[13] While useful, Chyba's framework and many arguments in the existing debate can still be better integrated and coalesced into higher-order mechanisms, thereby allowing for a joint understanding of such pressures that drive escalation, be it in the areas of arms racing, crises, or war.

We distill three first-order questions pertaining to technology and stability from this literature. Specifically, how will these technologies:

1. change states' real or perceived (dis)advantages?
2. influence the levels of uncertainty which states have to deal with?
3. affect communication between states?

[9] James Acton, "Cyber warfare & inadvertent escalation," *Daedalus* 149.2 (2020): 133-149; Jürgen Altmann & Frank Sauer, "Autonomous weapon systems and strategic stability," *Survival* 59.5 (2017): 117-142; Michael C. Horowitz, "Do emerging military technologies matter for international politics," *Annual Review of Political Science* 23: 385-400; James Johnson, "Artificial Intelligence & future warfare: Implications for international security," *Defense & Security Analyses* 35.2 (2019): 147-169.

[10] Marina Favaro and Heather Williams, "False sense of supremacy: Emerging technologies, the war in Ukraine, and the risk of nuclear escalation," *Journal for peace and nuclear disarmament* 6.1 (2023): 28-46.

[11] Caitlin Talmadge, "Emerging technology and intra-war escalation risks: Evidence from the Cold War, implication for today," *Journal of Strategic Studies* 42.6 (2019): 864-887; see also Todd S. Sechser, Neil Narang, and Caitlin Talmadge, "Emerging technologies and strategic stability in peacetime, crisis, and war," *Journal of Strategic Studies* 42.6 (2019): 727-735.

[12] Brad Roberts, "Emerging and Disruptive Technologies, Multi-domain Complexity, and Strategic Stability: A Review and Assessment of the Literature," *Center for Global Security Research*, (February 2021).

[13] Chyba, 2020.

In the following, we elaborate each of these questions in turn.

1) Changing states' real or perceived (dis)advantages

A chief concern with emerging technologies is their potential ability to enable states to implement offensive campaigns more easily.[14] For instance, technologies such as drones can reduce political costs of military action by allowing states to initiate crises and launch strikes with fewer casualties.[15] Moreover, compared with the increasing costs of such manned aerial vehicles as the F-35, which today, costs around $100 billion,[16] drones are cost effective given the ability to buy them "off-the-shelf" and construct them with relatively cheap and easily attainable materials.[17]

In addition to lowering the threshold for conflict initiation, drones also benefit states by allowing them to probe the target's resolve since the removal of direct human engagement implies that operations can be kept at the gray-zone level. States can also perhaps avoid attribution, which is made possible by the relatively widespread use of drones by a variety of states and non-state actors.[18] Given these military advantages, states with the upper hand in the development of such technologies may re-evaluate the viability of conflict as a foreign policy, which increases the likelihood of aggressive action. In fact, these advantages need not be real. In the case of Russia's invasion of Ukraine, for example, Favaro and Williams note that it is the *perception* of military advantage which has led Russia to believe that it has the ability to "impose and absorb costs".[19] Hence, technologies may increase the attractiveness of conflict as a foreign policy option even if the advantages are merely perceived and will not necessarily materialize.

Separate from intentional escalation, which originates from states' deliberate effort to destabilize the status quo, this confidence and readiness to use and benefit from emerging technologies can also result in inadvertent escalation. Results from a wargame show that players value cyber capabilities and can become overconfident about their utility and advantages. Indeed, in the presence of both cyber capabilities and vulnerabilities, teams have used cyber exploits to overcome weaknesses in the system. Players explain that *because* of the vulnerability, they must use the cyber exploit to "gain advantage" or assume compromises and overcome threats to the Nuclear Command, Control, and Communications (NC3).[20] These justifications reveal the level of confidence players have in such technologies, going as far as believing that their cyber capabilities can compensate for weaknesses in the system.[21]

[14] Talmadge, 2019.
[15] Vincent Boulanin, Lora Saalman, Petr Topychkanov, Fei Su, and Moa Peldán Carlsson, "AI, Strategic Stability and Nuclear Risk," *Stockholm International Peace Research Institute* (June 2020): 116; On drone warfare, see Sarah E. Kreps, "Drone Warfare," in *Understanding war and peace 2nd edition*, ed. Dan Reiter (Cambridge: Cambridge University Press, 2023), 371-404.
[16] Udrescu and Siteanu 2021, 306.
[17] Altmann and Sauer 2017, 126; Johnson 2019, 153.
[18] Boulanin et al. 2020, 117-118; Johnson 2019, 153.
[19] Favaro and Williams 2023, 32.
[20] Jacquelyn Schneider, Benjamin Schechter, and Rachael Shaffer, "Hacking nuclear stability: Wargaming technology, uncertainty, and escalation," *International Organization* 77 (2023): 655.
[21] Ibid., 657.

Such (over)confidence in cyber capabilities, however, increases the potential for inadvertent escalation – especially when teams with vulnerabilities exercise restraint mostly in low-intensity situations and become *more* willing to leverage exploits and de-emphasize weaknesses in more intense cases.[22] Worse still, teams with cyber vulnerabilities demonstrate a willingness to "sacrifice safety and control" by relying on "dead hand orders" and automation to send a stronger deterrence signal.[23] In other studies, scholars observe that in severe cases of disadvantages, states may even rely more on nuclear capabilities to overcome unfavorable shifts in the conventional balance of power.[24] Thus, even if unintended, confidence in the abilities of technologies to strengthen deterrence and a readiness to take risks to address vulnerabilities can drive up tensions and perceptions of threat in times of crisis, thereby prompting an escalation.[25]

2) Influencing the levels of uncertainty

Uncertainty is one of the most widely argued causes of arms races and wars. Some scholars argue that because states can never be certain about other states' intentions, they must assume the worst and undertake such actions as arms building to deter aggression or prepare for war.[26] Others argue that uncertainty about the costs of war to each side can prevent states from negotiating and settling on a deal which could have overcome disagreements without resorting to war.[27] Still others argue that uncertainties, or disagreements, around relative capabilities can lead to wars when states, driven by mutual optimism and confidence in their own abilities, seek to demonstrate their strengths or change the status quo.[28]

Technologies and their developments can change the level of uncertainty in at least two ways. In the case of emerging technologies, for which the effects and use remain largely unknown, states may be particularly inclined to make worst-case assumptions about adversaries' progress and how they plan to use these technologies,[29] and thus, be motivated to develop their own capabilities and perpetuate the security dilemma.[30] Arms races epitomize such action-reaction cycles and hence, are unsurprising outcomes following the development of arms and emergence of new technologies.

[22] Ibid., 649; 657.
[23] Ibid., 653.
[24] Henrik Stålhane Hiim, M. Taylor Fravel, and Magnus Langset Trøan, "The dynamics of an entangled security dilemma," *International Security* 47.4 (2023): 149.
[25] Acton 2020.
[26] John J. Mearsheimer, *The Tragedy of Great Power Politics*, (New York: W.W. Norton & Company, 2001); and Sebastian Rosato, *Intentions in Great Power Politics: Uncertainty and the Roots of Conflict*, (Yale University Press, 2021).
[27] James D. Fearon, "Rationalist Explanations for War," *International Organization* 49.3 (1995): 379-414; see also Robert Powell, "War as a Commitment Problem," *International Organization* 60.1 (2006): 169-203.
[28] Geoffrey Blainey, *The Causes of War* (London: Macmillan, 1973); Kristopher W. Ramsay, "Information, Uncertainty, and War," *Annual Review of Political Science* 20 (2017): 505-527; Stephen Van Evera, *Causes of War: Power and the roots of conflict*, (Ithaca: Cornell University Press, 2001).
[29] Chyba 2020: 154; Hiim et al. 2023.
[30] The term, "security dilemma", was coined by John Herz. It occurs when states' accumulation of power for security-reasons drives other states to do the same. This cycle of action-reaction can become self-perpetuating and, thus, drive and intensify competition between states. See Shiping Tang, "The Security Dilemma: A Conceptual Analysis", *Security Studies* 18.3 (2009): 587-623.

It is less relevant whether states have plans of using such technologies offensively; the threats they make possible can ratchet up the competitive pressures between states. As Altmann and Sauer illustrate in the case of autonomous weapons systems: "Russia was reportedly alarmed when the idea of using stealthy drones for missile defence was floated in the US. Swarms of AWS could be used to attack nuclear-weapon delivery systems, command and control systems, and sensitive infrastructure components such as antennas, sensors or air intakes. *Even though an attacker might have little interest or confidence in the success of a disarming first strike of this type, the fact that such strikes were now possible would in itself increase nervousness and distrust between nuclear-armed adversaries*."[31]

A second source of uncertainty stems from the entanglement between nuclear and conventional capabilities and systems, which is not new considering the availability of dual capable aircraft and systems throughout the Cold War and beyond.[32] Uncertainty derived from such entanglement can be destabilizing because states may not be able to discern whether an attack is targeted at nuclear or conventional assets or characterize if a weapon or delivery system carries a nuclear warhead. In response, target states may overreact by stepping up the escalation ladder, even preemptively launching nuclear strikes before aggressors do, or conversely, underreact and encourage attackers to believe that the target state lacks resolve.[33] Whether or not technologies will exacerbate or ameliorate uncertainty due to entanglement will partially depend on states' ability to signal their intent or successfully characterize the nature of the attack. Both can be difficult to achieve against the backdrop of distrust and efforts to degrade target states' NC3 and quality of information through dis- and mis-information campaigns.[34] This issue is only amplified by the increase in speed of many emerging technologies that may drastically reduce windows of opportunity for communication and decision-making. However, enhanced situational awareness aided by big data and artificial intelligence may mitigate some of these challenges – if states can fruitfully utilize the large amounts of information.[35]

[31] Altman and Sauer 2017, 131, emphasis added.

[32] According to James Johnson, entanglement "refers to dual-use delivery systems that can be armed with nuclear and nonnuclear warheads; the commingling of nuclear and nonnuclear forces and their support structures; and nonnuclear threats to nuclear weapons and their associated command, control, communications, and intelligence (C3I) systems." James Johnson, "Artificial intelligence: A threat to strategic stability," *Strategic Studies Quarterly* (Spring 2020), 31; see also James M. Acton, "Escalation through entanglement: How the vulnerability of command-and-control systems raises the risks of an inadvertent nuclear war," *International Security* 43.1 (2018): 56-99.

[33] James M. Acton, "Is it a Nuke? Pre-launch ambiguity and inadvertent escalation", *Carnegie Endowment for International Peace*, (April 9, 2020), https://carnegieendowment.org/research/2020/04/is-it-a-nuke-pre-launch-ambiguity-and-inadvertent-escalation?lang=en; Johnson, 2020, 26; Robert Legvold, "The challenges of a multipolar nuclear world in a shifting international context," *American Academy of Arts & Sciences* (2020), https://www.amacad.org/publication/nuclear-weapons-changing-global-order/section/3; Jeffrey Taylor, "Deterring Russian Nuclear Threats with Low-Yield Nukes May Encourage Limited Nuclear War," *Journal of Advanced Military Studies* 13 (2022): 207-229.

[34] Boulanin et al. 2020, 119-120.

[35] Hersman et al. 2020, 7. However, the authors of the report are generally more pessimistic about the emerging strategic situational awareness capabilities due to the various pathways to escalation. See pages 6-7. See also Huangqing Chen, Tingquan Lim and Taotao Jiang, "Function Analysis of Command and Control System in Intelligent War," *Journal of Physics: Conference Series* 1684(2020): 4-5.

3) Affecting communication between states

In addition to signaling and characterization problems, stability between states can break down if states, more fundamentally, cannot communicate effectively. Communication between states, including belligerents, is crucial for addressing misunderstandings and accidents, thereby preventing inadvertent escalation from occurring even during wars.[36] However, the integration of artificial intelligence and other advanced weapons systems into decision-making processes can undermine communication by compressing timeframes for information exchange and deliberation.

In China, for instance, active plans are in place to integrate artificial intelligence into operations and decision-making processes, as we discuss in more detail below. This "intelligentization" of warfare can reduce time and opportunities for communication, especially in light of efforts to allow such intelligent systems to inform and even intervene in combat,[37] because there will be limited room for call backs. More generally, because errors are inherent in predictive models, states may end up finding themselves in unexpected crises or conflicts from launching unwarranted preventive strikes.[38] A recent study, moreover, finds that large language model agents in wargames consistently choose to escalate in arms races and conflicts, including choosing to deploy nuclear weapons in some scenarios.[39] While the authors recognize that this tendency to escalate may be due to the literature's bias toward studying escalation (rather than de-escalation), it is questionable that future training data will beget different results given the persistent lack of attention to the study of de-escalation, particularly in intra-war dynamics.[40] Overall, with pressures to gain advantages over adversaries and the reduced reaction times accorded by many advanced technologies, escalation may become more likely as states proceed to shoot first and ask questions later.

In the rest of this brief, we describe three Russian and Chinese emerging technologies: hypersonic weapons, artificial intelligence, and quantum computing. This discussion contextualizes the technological developments in each country and provides the necessary knowledge for analyzing their effects on stability.

[36] Rose Gottemoeller and Daniil Zhukov, "Nuclear risk reduction centers: A stable channel in unstable times," *Stanley Center for Peace and Security*, (October 2023), https://stanleycenter.org/wp-content/uploads/2023/10/English-Nuclear-Risk-Reducation-Centers-A-Stable-Channel-in-Unstable-Times.pdf; Leah Walker, "The role of crisis communications in the Russo-Ukrainian War," *Institute for Security + Technology* , (May 18, 2022), https://securityandtechnology.org/blog/the-role-of-crisis-communications-in-the-russo-ukrainian-war/.

[37] Chen et al, 2020; Elsa B. Kania, "Minds at war: China's pursuit of military advantage through cognitive science and biotechnology," *Prism* 8.3 (2019): 83-101, https://ndupress.ndu.edu/Portals/68/Documents/prism/prism_8-3/prism_8-3_Kania_82-101.pdf.

[38] Boulanin et al. 2020.

[39] Juan-Pablo Rivera, Gabriel Mukobi, Anka Reuel, Max Lamparth, Chandler Smith, and Jacquelyn Schneider, "Escalation risk from language models in military and diplomatic decision-making," *arXiv*, (January 7, 2024), https://arxiv.org/pdf/2401.03408.

[40] Maximillian Hoell, Kimberly Peh, Ryan Christenson, Daniel Kroth, Quinn Urich, Raymond Hughes, Ross Buchanan, and Daeyeon Lee, "Escalation, De-escalation, and Intra-war deterrence," Workshop Summary, *Lawrence Livermore National Laboratory Center for Global Security Research*, (April 3-4, 2024), https://cgsr.llnl.gov/content/assets/docs/Intrawar-Deterrence-Workshop-Summary.pdf.

Emerging Technologies in Russia and China

Russia

Hypersonics

During his annual address to the Federal Assembly on March 1, 2018, Vladimir Putin announced a series of novel nuclear weapons.[41] These weapons included both hypersonic weapons and nuclear-powered weapons. Some weapons may include integrated AI capabilities for enhanced guidance, as discussed later in this brief.

The five novel systems include the Avangard Hypersonic Glide Vehicle, Kinzhal Hypersonic Aeroballistic Missile, Tsirkon Hypersonic Cruise Missile, Burevestnik Nuclear-Powered Cruise Missile, and Poseidon Nuclear-Powered Uncrewed Underwater Vehicle. All three hypersonic weapons are dual-capable systems that could deliver a conventional or nuclear warhead. Burevestnik or Poseidon could do so in theory but are likely nuclear-only systems.

Novel weapons provide Russia with a hedge against future American missile defenses and counterforce capabilities.[42] These weapons are part of a broader modernization wave intended to guarantee Russian nuclear modernization for the coming decades. While current American capabilities are insufficient to threaten the survivability of the Russian arsenal, several strategists worry about the combination of a more robust national missile defense and greater precision-strike capabilities due to investment in Prompt Global Strike.[43] They also provide Russia with status symbols, which are greatly valued by its leadership in view of Russia's engagement in a status competition with the United States, China, and others. One of the few areas where they can compete with the United States and China is the development of nuclear technologies. Russian policymakers believe that these systems simultaneously enhance future Russian security and provide concrete status symbols, allowing them to address two goals of the Russian leadership.

Russia has fielded the three hypersonic weapons: Kinzhal in December 2017, Avangard in December 2019, and Tsirkon in December 2022.[44] Russia has used conventional variants of two—Kinzhal and Tsirkon—in Ukraine. Vladimir Putin announced that Russia completed testing on Burevestnik in October 2023, although some experts remain skeptical.[45] Russian

[41] Vladimir Putin, "Presidential address to the Federal Assembly," Office of the President of Russia, 12 February 2018, http://en.kremlin.ru/events/president/news/56957.
[42] Spenser A. Warren, "Security, power, and prestige: Understanding the determinants of Russian nuclear modernization under Vladimir Putin." (Ph.D. Diss: Indiana University Bloomington, 2023).
[43] Charles K. Bartles, "Russian threat perception and the ballistic missile defense system," The Journal of Slavic Military Studies 30.2 (2017): 152-169.
[44] Guy Faulconbridge, "Putin deploys Zircon hypersonic cruise missiles to Atlantic," Reuters, 4 January 2023, https://www.reuters.com/world/europe/putin-sends-off-frigate-armed-with-new-hypersonic-cruise-missile-2023-01-04/; Michael Kofman, "Beyond the hype of Russia's hypersonic weapons," The Moscow Times, 16 January 2020, https://www.themoscowtimes.com/2020/01/15/russias-hypersonic-weapons-a68907; Tass, "Kinzhal complex substantially boosts Russia's Aerospace Force capabilities—commander," 1 March 2018, https://tass.com/defense/992375.
[45] Timothy Wright, "Russia's claims to have tested nuclear-powered cruise missile," International Institute for Strategic Studies, 13 October 2023, https://www.iiss.org/online-analysis/missile-dialogue-initiative/2023/10/russia-claims-to-have-tested-nuclear-powered-cruise-missile/.

media reports that Poseidon will enter into service in 2025, where it will be deployed on Belgorod-class SSNs assigned to the Russian Pacific Fleet.[46]

These weapons are technological marvels if Russian claims about their characteristics are accurate. Yet their impacts on deterrence and warfighting should be mixed. At the strategic level, these weapons do not change the strategic status quo.[47] None significantly enhances Russian counterforce or counter-NC3 capabilities. Russia could use any in a strike against American NC3 assets on Earth, and Avangard could strike American missile silos in the continental United States. However, existing Russian weapons could do so with the same effectiveness.

Novel weapons do not improve Russian accuracy.[48] The most accurate of these weapons, Avangard, has an accuracy consistent with existing Russian ICBMs. Kinzhal's accuracy may be lower than that of other Russian air-based nuclear weapons. These weapons may allow Russia to circumvent American missile defenses, but that does not alter the status quo, as Russian forces are already capable of overcoming American missile defenses.

These weapons also do not threaten space-based NC3 capabilities. None can reach space except Avangard. Even then, Avangard separates from a boosting missile near the Karman Line and maneuvers through the atmosphere to reach its target, relying on air resistance to glide to its destination. This trajectory makes it a poor choice for a counter-NC3 strike targeting assets in space, especially since other conventional or nuclear warheads could reach these targets more reliably.

A greater threat to American NC3 assets in space is the possible space-based Russian anti-satellite (ASAT) weapon covered in the intelligence announced by Representative Mike Turner in February 2024.[49] Reporting suggests the U.S. Intelligence Community remains divided over the nuclear nature of the weapon. It may include a nuclear weapon that damages satellites with the release of gamma radiation following a detonation. Alternatively, it may be a nuclear-powered weapon that uses a conventional kinetic kill vehicle, electronic warfare, or other smaller satellites to strike and damage space assets. Russia has invested in each of these before, including recent investment in an air-based ASAT weapon that launches interceptor satellites into the path of satellites in Low-Earth Orbit (LEO).[50]

[46] Tass, "Submarine force armed with Poseidon torpedoes to come into operation in Kamchatka in 2025," 3 April 2023, https://tass.com/defense/1598329.
[47] Spenser A. Warren, "Avangard and transatlantic security," Center for Strategic and International Studies, 23 September 2020, https://www.csis.org/blogs/post-soviet-post/avangard-and-transatlantic-security.
[48] See Jill Hruby, "Russia's new nuclear weapon delivery systems: An open-source technical review," (Washington: Nuclear Threat Initiative, 2019); Natalie G. Montoya, "No winning moves: Calculated casualties and damages of a nuclear attack on the United States by Russia for first and second strike scenarios" (BSE Thesis: Massachusetts Institute of Technology, 2021).
[49] Erin Banco, Alexander Ward, and Lee Hudson, "The 'disturbing' intel roiling the Hill is about Russian nukes in space," Politico, 14 February 2024, https://www.politico.com/news/2024/02/14/house-intel-national-security-threat-russia-space-power-00141473.
[50] Bart Hendrickx, "Burevestik: A Russia air-launched anti-satellite system," The Space Review, 27 April 2020, https://thespacereview.com/article/3931/1. While the air-launched ASAT system is called Burevestnik, it is unrelated to the nuclear-powered cruise missile. Russia has given the name Burevestnik, the Russian name for the stormy petrel and roughly translated as storm-bringer, to several weapon systems in the past.

Regardless of whether the new ASAT system under development is a nuclear weapon or nuclear-powered weapon, it could pose a significant threat to American NC3 assets in space, threatening both deterrence and warfighting capabilities while increasing crisis instability.[51] The novel threat posed by this system would be its ability to strike targets in Geosynchronous Orbit, including critical components of the American NC3 system. Ground-based ASAT weapons can only reliably strike targets in LEO. The ability to strike targets in geosynchronous orbit (GEO) exists even if the weapon is not nuclear. A non-nuclear option could be more dangerous than a nuclear one, as certain non-nuclear ASAT technologies could strike specifically American space assets, whereas the gamma radiation from a nuclear detonation would destroy both American and Russian satellites indiscriminately.

Hypersonic weapons may strengthen Russian warfighting capabilities to some extent. These weapons may better penetrate missile defenses or target critical naval assets more effectively. They could also have other uses, including the delivery of low-yield nuclear warheads for escalation management or battlefield purposes. In this regard, however, their use would not be fundamentally different from the use of other Russian nonstrategic nuclear weapons.

Kinzhal has proven effective at overcoming rudimentary air and missile defenses while older missiles struggled against them. However, the weapon remains vulnerable to more advanced systems such as Patriot.[52] Tsirkon is likely a more effective weapon for avoiding missile defenses. Kinzhal's only truly new ability is its hypersonic velocity, which decreases as it approaches targets. Tsirkon combines hypersonic speeds with maneuverability, as does Avangard. This speed-maneuverability combination would make each far more challenging to track and hit than Kinzhal or existing systems.

Russia is not producing Avangard in large enough numbers to have a significant battlefield impact yet.[53] Previous Kinzhal and Tsirkon uses did not drastically change battlefield or political outcomes. Tsirkon may have a greater impact in the event of a naval war. The missile is designed to strike critical sea-based targets, primarily destroyers equipped with Aegis missile defenses and aircraft carriers.[54] Poseidon may also carry out such functions, but its slower speed and positioning in the Sea of Okhotsk—where it is likely to stay to enjoy the protections of Russian bastion defense—make it an inferior option relative to Tsirkon.

[51] Spenser A. Warren, “Is Russia looking to put nukes in space? Doing so would undermine global stability and ignite an anti-satellite arms race,” The Conversation, 17 February 2024, https://theconversation.com/is-russia-looking-to-put-nukes-in-space-doing-so-would-undermine-global-stability-and-ignite-an-anti-satellite-arms-race-223702.
[52] Maria Kostenko and Nick Patton Walsh, “Ukraine says it used US-made Patriot system to intercept Russian hypersonic missile,” CNN, 6 May 2023, https://www.cnn.com/2023/05/06/europe/us-patriot-system-ukraine-hypersonic-missile-intl-hnk/index.html.
[53] Kofman, “Beyond the hype of Russia’s hypersonic weapons;” Warren, “Avangard and Transatlantic security.”
[54] Michael Kofman et al., “Russian military strategy: Core tenets and operational concepts,” Center for Naval Analyses, 19 October 2021, https://www.cna.org/reports/2021/10/russian-military-strategy-core-tenets-and-concepts; Warren, “Understanding the determinants of Russian nuclear modernization.”

Quantum Computing

The Russian government and Russian industry have recently invested resources in quantum technologies, focusing on the development of a wide range of new quantum computing technologies.[55] Russia's Quantum Technologies Roadmap, initiated in 2019, tasked Rosatom, Russian Railways, and Rostec with developing advanced quantum computing, communications, and sensing capabilities, respectively, setting aside over 50 billion Rubles—approximately 691 million in US dollars—for this research.[56]

A combination of Russian private and state-run companies is collaborating on efforts to increase the use of quantum technology in artificial intelligence. According to state-affiliated media, these companies include Sberbank, the Russian Direct Investment Fund, telecommunications firm Mobile TeleSystems, and tech companies Yandex and VKontakte.[57]

The Quantum Technologies Roadmap calls for the creation of a 30-100 qubit computer by 2024 and a 1000 qubit computer by 2030.[58] These goals are unrealistic, and Russian quantum developments have been more modest, lagging behind China and the United States. By the end of 2021, Russian scientists at Rosatom developed a prototype 4-qubit ion quantum computer.[59] Rosatom demonstrated a 16-qubit ion quantum computer in 2023.[60]However, qubit counts are not good predictors of quantum advantage and require a consideration of complementary metrics to evaluate their performance accurately. The Russian government launched the Quantum Technologies Roadmap in 2019 with the intention of maintaining national security and promoting technological independence.[61] In comments to a forum on future technology in Moscow, Vladimir Putin tied the development of quantum technologies to national security and sovereignty, claiming that remaining dependent on quantum technologies in other countries "means a serious threat to national security, as well as weakening, and even loss of the country's sovereignty."[62]

How Russia would integrate quantum technologies into its military systems or doctrine remains unknown. Current Russian abilities are rudimentary, with minimal, if any, strategic impact. Russia will likely remain incapable of creating significant quantum technologies for the foreseeable future.

[55] A.K. Fedorov et.al., "Quantum technologies in Russia," Quantum Science and Technology 4.4 (2019): 10.1088/2058-9565/ab4472.
[56] Johnny Kung and Muriam Fancy, "A quantum revolution: Report on global policies for quantum technology," Canadian Institute for Advanced Research, August 2021, https://cifar.ca/wp-content/uploads/2021/05/QuantumReport-EN-May2021.pdf.
[57] Ekaterina Blinova, "Future technologies forum: Russia races against time pushing quantum computing," Sputnik, July 14, 2023, https://sputnikglobe.com/20230714/future-technologies-forum-russia-races-against-time-pushing-quantum-computing-1111878551.html.
[58] Kung and Fancy, "Report on global policies for quantum technology."
[59] Dan O'Shea, "Russia reaches milestone on quantum computing roadmap," Inside Quantum Technology, December 30, 2021, https://www.insidequantumtechnology.com/news-archive/russia-reaches-milestone-on-quantum-computing-roadmap/.
[60] Blinova, "Russia races against time pushing quantum computing."
[61] Kung and Fancy, "Report on global policies for quantum technology."
[62] Blinova, "Russia races against time pushing quantum computing."

AI

Russia has a significant interest in the military applications of artificial intelligence (AI). Speaking to a group of students on September 1, 2017, Vladimir Putin remarked, "Artificial intelligence is the future…for all humankind. It comes with colossal opportunities, but also threats that are difficult to predict. Whoever becomes the leader in this sphere will become the ruler of the world." [63] The Russian leadership sees both military and economic opportunities in AI. Russian efforts to integrate AI into its military capabilities are focused on providing Russia with the ability to disrupt or destroy adversary command, control, and communications (C3) systems and capabilities and to establish information superiority during the early stages of a war.[64] While Russia sees AI as strategically important, AI investment, development, and integration continue to lag behind the United States and other countries.

It is important to note that the Russian military sees AI as a potential force amplifier, enhancing already established warfighting methods and capabilities rather than revolutionizing warfare.[65] Russia is integrating AI into uncrewed aerial and underwater vehicles–including the Poseidon unmanned underwater vehicles (UUV)–as well as air defense systems, although these advancements have happened at a slow and incremental rate.[66] Russian efforts to develop AI capabilities and integrate them into weapons systems and military doctrine will be assisted by the clarity of AI goals, the existence of several AI initiatives, and a technologically skilled population, but simultaneously constrained by limited private sector AI development, lack of sufficient capital or the government or private sector, and high levels of corruption in both private and public sector firms developing AI technologies.[67] Despite this technologically literate population and the legacy of a strong Soviet education system, Russia faces a lack of adequately trained AI experts and the loss of many of the few who do receive adequate training to higher-paying jobs elsewhere.[68] Government agencies such as Rostec have prioritized the research and development of other technologies, while Russia's business environment limits private-sector investment.[69] State-owned companies, primarily the Sberbank, have filled the gap by driving Russian investment in AI.[70]

[63] Russia Today, "'Whoever leads in AI will rule the world': Putin to Russian children on knowledge day," September 1, 2017, https://www.rt.com/news/401731-ai-rule-world-putin/.
[64] Margarita Konaev, "Military applications of artificial intelligence: The Russian approach," In Samuel Bendett et al., "Advanced military technology in Russia: Capabilities and implications," Chatham House, September 2021, 63-74, https://www.chathamhouse.org/sites/default/files/2021-09/2021-09-23-advanced-military-technology-in-russia-bendett-et-al.pdf.
[65] Konaev, "Military applications of artificial intelligence."
[66] Katarzyna Zysk, "Defence innovation and the 4th industrial revolution in Russia." Journal of Strategic Studies 44.4 (2021): 543-571.
[67] Keith Dear, "Will Russia rule the world through AI? Assessing Putin's rhetoric against Russia's reality." The RUSI Journal 164.5-6 (2020): 36-60.
[68] Jeffrey Edmonds et al., "Artificial intelligence and autonomy in Russia," Center for Naval Analyses, May 12, 2021, https://www.cna.org/reports/2021/05/Artificial-Intelligence-and-Autonomy-in-Russia.pdf; Stephanie Petrella, Chris Miller, and Benjamin Cooper, "Russia's artificial intelligence strategy: The role of state-owned firms," Orbis 2021 65.1 (2021) 75-100.
[69] Petrella, Miller, and Cooper, "Russia's artificial intelligence strategy."
[70] Edmonds et.al., "Artificial intelligence and autonomy in Russia;" Petrella, Miller, and Cooper, "Russia's official artificial intelligence strategy."

Russian AI development lags the United States, China, and others. Data from 2019 placed Russia 12th on the list of countries with the most AI patents registered and 14th on the list of countries ranked by inventor nationality.[71] These problems have been on display in Russia's war in Ukraine, with Russia only using limited AI capabilities, including drones with AI technology.[72] Despite previous claims suggesting high levels of AI integration, Russian drone forces in Ukraine have mostly lacked AI capabilities.[73]

While Russia has had challenges developing AI technologies and integrating them into military systems, it has reportedly had some success developing AI-enabled electronic warfare (EW) systems. The RB-109A Bylina EW system likely includes an automated decision-support system that can identify and select C3 targets, decide how to suppress a particular target best, and determine which jamming station to use for that suppression.[74] Bylina was one of four EW systems spotted in the Donbas during the summer of 2018, likely testing the system's capabilities, and the Ministry of Defense approved a plan to deliver completed Bylina systems to military units by 2025.[75] The integration of AI into EW could enhance Russia's ability to target communications and navigation satellites, degrading American and allied decision-making capabilities during a conflict.[76] Further advances in AI-enabled EW could increase the risk posed by Russian EW capabilities to American NC3 systems.

Russian strategists perceive AI as an important tool for enhancing its nuclear deterrent, although many plans for integrating AI into nuclear, missile defense, and early warning systems remain uncompleted. AI is likely to be integrated into Russian early warning systems to improve threat assessment and damage prediction, with reports suggesting that Russia plans to integrate AI technology into upgraded radar stations as it modernizes its missile attack warning system.[77] Russian leaders believe that improved warning systems would make the nuclear arsenal less vulnerable to an American first strike, allowing Russia to launch a retaliatory strike before an American attack significantly degraded the Russian arsenal. AI also overlaps with the development of novel nuclear weapons and other aspects of Russia's ongoing nuclear modernization. Avangard, Kinzhal, and Sarmat include AI-assisted guidance systems, as would Burevestnik and Poseidon upon development.[78] In theory, these guidance systems could make novel nuclear weapons more reliable, increasing the likelihood that they reach their target and possibly mitigating the effects of a potential attack against the space-based global navigation satellite system (GLONASS).

[71] UK Government and Intellectual Property Office, Artificial Intelligence: A Worldwide Overview of AI patents and Patenting by the UK AI sectors, June 2019; World Intellectual Property Office, 'Technology trends: Artificial Intelligence," 2019; https://www.wipo.int/tech_trends/en/artificial_intelligence/story.html.
[72] Ingvild Bode and Anna Nadibaidze, "AI and drones in the Russian invasion of Ukraine: Challenging the expectations," AutoNorms, April 4, 2022, https://www.autonorms.eu/ai-and-drones-in-the-russian-invasion-of-ukraine-challenging-the-expectations/.
[73] Anna Nadibaidze, "Russia's 'low-tech' war on Ukraine discredited its military modernization narrative," Network for Strategic Analysis, March 3, 2023, https://ras-nsa.ca/russias-low-tech-war-on-ukraine/.
[74] Konaev, "Military applications of artificial intelligence."
[75] Konaev, "Military applications of artificial intelligence."
[76] Konaev, "Military applications of artificial intelligence."
[77] Edmonds et al., "Artificial intelligence and autonomy in Russia."
[78] Edmonds et al., "Artificial intelligence and autonomy in Russia."

Russia may use autonomous weapons to defend missile silos.[79] If effective, these weapons could make silos less vulnerable to saboteurs, although questions regarding their capabilities arise due to the underperformance of supposedly autonomous systems in Ukraine. AI could be integrated into Russian air and missile defenses in the future, as Russian strategists believe AI would enhance the ability of air and missile defense systems to detect and counter an incoming attack.[80] Similar to AI-enhanced early warning, integrating AI into air and missile defenses could make the Russian nuclear arsenal more survivable in the face of an American missile or aerospace attack. Enhancing these defenses could also increase the effectiveness of Russian conventional forces, degrading the ability of the United States or others to launch strategic attacks against conventional forces or gain air superiority.

Finally, AI is an important tool in Russia's information warfare arsenal. Russian strategists view AI as useful for both the cyber-psychological and cyber-technical facets of cyber warfare, itself considered a subset of information warfare in Russian strategic thought.[81] For the former, Russian strategists see AI as a tool of manipulation, enhancing the ability to generate deep fakes and other forms of believable misinformation that confuses adversarial militaries, erode trust in adversary governments, and complicate adversary decision-making.[82] Regarding the latter, AI is perceived as a tool for finding and exploiting vulnerabilities in adversarial information technology (IT) systems, making it easier to engage in cyber espionage, plant malware, or destroy critical systems and infrastructure.[83]

China

Hypersonics

China has developed or is developing multiple hypersonic weapons. The YJ-21 is a hypersonic anti-ship cruise missile that could target an adversary's naval capabilities in the West Pacific. The DF-17 is a Medium-Range Ballistic Missile (MRBM) with a range of approximately 1,000 to 1,500 miles that is designed to boost hypersonic glide vehicles (HGVs).[84] The DF-27 is a more advanced variant of the DF-17 that can strike targets at a range of 5,000 to 8,000 kilometers and can carry multiple warheads.[85] In 2023, Chinese leaders claimed the DF-27 had been under operational deployment for over four years, though the weapon does not have as long of a track

[79] Justin Haner and Denise Garcia, "The artificial intelligence arms race: Trends and world leaders in autonomous weapons development." Global Policy 10.3 (2019): 331-337.
[80] Edmonds et al., "Artificial intelligence and autonomy in Russia."
[81] Edmonds et. al., "Artificial intelligence and autonomy in Russia;" Rod Thornton and Marina Miron, "Towards the 'Third revolution in military affairs: The Russian military's use of AI-enabled cyber warfare,'" The RUSI Journal 165.3 (2020): 12-21.
[82] Thornton and Miron, "The Russian military's use of AI-enabled cyber warfare."
[83] Thornton and Miron, "The Russian military's use of AI-enabled cyber warfare."
[84] Kelley M. Sayler, "Hypersonic weapons: Background issues for Congress," Congressional Research Service, March 17, 2022, 16.
[85] Kartik Bommakanti, "Advances in Chinese missile defence and hypersonic capabilities," Observer Research Foundation, June 19, 2023, https://www.orfonline.org/expert-speak/advances-in-chinese-missile-defence-and-hypersonic-capabilities.

record of successful tests as the DF-17.[86] The DF-41 is an ICBM that China has successfully tested and could boost a nuclear-armed HGV.

China has also tested or deployed multiple HGVs that a missile such as the DF-17, DF-27, or DF-41 could boost. Among the potential HGVs that these missiles could carry is the DF-ZF HGV. The Chinese military tested the vehicle at least nine times between 2014 and 2022 and reportedly fielded the vehicle in 2020.[87] Defense officials have publicly claimed the HGV has a range of approximately 1,200 miles and is capable of performing extreme maneuvers during its flight.[88] U.S. defense officials claim that China has also tested another nuclear capable HGV prototype, the Starry Sky-2, that can reach a speed of Mach 6 while performing in-flight maneuvers.[89]

In addition to these systems, China tested a Fractional Orbital Bombardment System (FOBS) capable of delivering a nuclear-capable hypersonic weapon in July 2021.The weapon reportedly flew more than 40,000 kilometers before impacting inside China, where it missed its intended target but did come close to striking it.[90] If developed, China's hypersonic FOBS is not a completely new system, but an evolution of existing hypersonic technologies.[91]

Incorporating a hypersonic reentry vehicle would increase the potential strategic impact of a FOBS. A FOBS armed with a traditional nuclear-armed reentry vehicle would pose problems for radar systems tasked with tracking incoming missile threats due to its ability to strike from vectors where the radars are not looking.[92] For example, China may attempt to strike the United States from the south, as the majority of early warning systems are focused on missile threats coming over the North Pole.[93] These issues are compounded by the inclusion of an HGV as a reentry vehicle, as an HGV can strike targets far from the FOBS's orbital flight path, complicating interception even if radar systems are able to identify and track the FOBS during orbit.[94] While a FOBS strike over the South Pole may be more difficult to track than a missile strike over the North Pole, it would not be completely invisible. American space-based infrared sensors could detect both the launch and deorbit of a FOBS, providing the United States with warning of an impending strike and the ability to determine the vector of the missile.[95]

As with Russia, many experts argue that China's pursuit of hypersonic weapons is an attempt to counter the combined threat of American missile defense and counterforce capabilities in an

[86] Bommakanti 2023.
[87] Sayler 2022, 16-17.
[88] Sayler 2022, 16-17.
[89] Sayler 2022, 17.
[90] Emma Helfrich and Tyler Rogoway, "More details on China's exotic orbital hypersonic weapon come to light," The Warzone, November 20, 2022, https://www.twz.com/more-details-on-chinas-exotic-orbital-hypersonic-weapon-come-to-light.
[91] Helfrich and Rogoway 2022.
[92] Jeffrey Lewis, "China's orbital bombardment system is big, bad news—but not a breakthrough," Foreign Policy, October 18, 2021, https://foreignpolicy.com/2021/10/18/hypersonic-china-missile-nuclear-fobs/.
[93] Sanne Verschuren. "China's hypersonic weapons tests don't have to be a Sputnik moment," War on the Rocks, October 29, 2021, https://warontherocks.com/2021/10/chinas-hypersonic-missile-tests-dont-have-to-be-a-sputnik-moment/.
[94] Helfrich and Sayler 2022.
[95] Verschuren 2021.

attempt to maintain Chinese nuclear deterrence into the future.[96] Chinese leaders perceive the combination of future American missile defenses—which they expect to become more robust in the following decades—and American investment in conventional prompt global strike as a future threat to China's nuclear arsenal. Like Moscow, Beijing worries the United States may be able to destroy a significant portion of its nuclear arsenal or NC3 capabilities with a counterforce strike, allowing its more robust missile defenses to absorb a Chinese retaliatory strike.

While most experts consider China's pursuit of hypersonic weapons to be primarily defensive, China may have secondary offensive intentions—including a desire to achieve regional conventional superiority to prevent an American intervention in the case of regional aggression—and current Chinese intentions, even if defensive, may not hold into the future. China may desire to achieve nuclear superiority vis-à-vis the United States, using its arsenal for strategic and prestige purposes in an attempt to place China at the center of the global order and in the dominant position of international politics.[97] Beijing may see hypersonic weapons as part of such a strategy.

However, Chinese hypersonic weapons alone will have limited impact on American nuclear deterrence, with strategic hypersonic weapons being poor options for counterforce or counter-NC3 strikes. While hypersonic weapons, especially a hypersonic FOBS, produces novel ways for China to circumvent American BMD and can help guarantee Chinese nuclear deterrence into the future, they do not provide fundamentally new capabilities. China is already capable of overwhelming American missile defenses. Additionally, China's emerging FOBS capability is likely too inaccurate to serve as a good first-strike weapon targeting American nuclear forces or NC3 infrastructure.[98] A far greater counterforce or counter-NC3 threat would be China's nuclear expansion or Chinese investment in ASAT capabilities, respectively.

While China's hypersonic weapons may not threaten American nuclear deterrence, they will likely have significant impacts on American warfighting capabilities in the Pacific should strategic deterrence fail. Chinese hypersonic weapons are largely regionally focused.[99] Regional capabilities such as the DF-17 could target American bases in the Pacific, while the YJ-21 is focused on combating American naval capabilities in the region.[100] Strikes against these targets could degrade American forces, hamper crucial logistics, or disrupt communications. Chinese hypersonic weapons, like Russia's Tsirkon, may be particularly hazardous for American carrier

[96] Eleni Ekmektsioglou, "Hypersonic weapons and escalation control in East Asia," *Strategic Studies Quarterly* 9.2 (2015): 43-68; Lewis 2021; Joshua H. Pollack, "Boost-glide weapons and US-China strategic stability," *Nonproliferation Review* 22.2 (2015): 155-164; Sayler 2022; Verschuren 2021; Warren and Ganguly Forthcoming.
[97] See Brad Roberts, et al., *China's emergence as a second nuclear peer: Implications for U.S. nuclear deterrence strategy* (Livermore, CA: Lawrence Livermore National Laboratory Center for Global Security Research, 2023).
[98] Sidarth Kaushal and Sam Cranny-Evans, "China's new hypersonic capability," RUSI, October 26, 2021, https://rusi.org/explore-our-research/publications/commentary/chinas-new-hypersonic-capability.
[99] Ekmektsioglou 2015; Michael T. Klare. "An 'arms race in speed,'" *Arms Control Today* 49.5 (2019): 6-13.
[100] Mark Montgomery and Bradley Bowman, "The US is failing to quickly field hypersonic missile defense," Defense News, January 19, 2024, https://www.defensenews.com/opinion/2024/01/19/the-us-is-failing-to-quickly-field-hypersonic-missile-defense/.

groups. China may intend to use the DF-27 against carrier groups based as far out as Hawaii, with Chinese leaders claiming the ability to destroy carrier groups with certainty.[101]

While American national missile defenses may be insufficient to counter a Chinese retaliatory second strike, regional missile defenses may have some effectiveness at blunting a Chinese missile strike against bases or naval assets in the region. Chinese hypersonics should significantly decrease this effectiveness. Such a decrease would make the defense of American allies such as Taiwan, Japan, or the Philippines far more difficult. It would also decrease American deterrence by denial capabilities, hampering the ability of the United States to manage escalation in a regional conflict and degrading intrawar deterrence.

Quantum technology

China's quantum policy has its origins in the "Big Data Strategy" that the leadership announced in 2014.[102] Initially, plans to progress quantum technologies were embedded in broader strategies such as "Made in China 2025", which aimed for technology leadership in AI and ML (machine learning) by the end of 2025. At the time, quantum technologies were first and foremost considered to support progress in making headway in the core areas of the Made in China plan, especially advanced information technologies, robotics and automation.[103]

Following the surprise launch of *Micius*, China's quantum satellite in 2016 (see below), quantum technologies, above all quantum communications, have been enjoying increased attention from the top of the Chinese leadership. In 2020, China's news agency *Xinhua* published an official statement of the 24th Collective Study of the Political Bureau of the Central Committee, in which Xi Jinping "emphasized a profound understanding of the great significance of advancing the development of quantum science and technology, and strengthened the strategic planning and system layout of quantum science and technology development."[104] Since then, China has been pursuing its quantum program at full throttle.

It is important to note that Chinese thinking on the strategic value of emerging technologies such as quantum does not align with the Western concept of "dual use." For Chinese strategists, there is no technology that, in principle, is not dual use. China pursues a policy of "civil-military

[101] Iain Boyd, "China's hypersonic missiles threaten US power in the Pacific—An aerospace engineer explains how the weapons work and the unique threats they pose," The Conversation, May 24, 2023, https://theconversation.com/chinas-hypersonic-missiles-threaten-us-power-in-the-pacific-an-aerospace-engineer-explains-how-the-weapons-work-and-the-unique-threats-they-pose-206271.

[102] Lindsay Gorman, "China's Data Ambitions: Strategy, Emerging Technologies, and Implications for Democracies," Commentary from the Center for Innovation, Trade, and Strategy (Washington DC: National Bureau of Asian Research, August 14, 2021), https://www.nbr.org/publication/chinas-data-ambitions-strategy-emerging-technologies-and-implications-for-democracies/.

[103] Scott Kennedy, Made in China 2025, Center for Strategic and International Studies, June 1, 2015, https://www.csis.org/analysis/made-china-2025.

[104] Xinhua.Net, "During the Twenty-Fourth Collective Study of the Political Bureau of the Central Committee, Xi Jinping Emphasized a Profound Understanding of the Great Significance of Advancing the Development of Quantum Science and Technology, and Strengthened the Strategic Planning and System Layout of Quantum Science and Technology Development.," *Xinhua.Net*, October 17, 2020, High Level edition, http://www.xinhuanet.com/politics/2020-10/17/c_1126623288.htm.

fusion" [军民融合] by which all emerging technologies are to support the leadership's core objective to turn the PLA into a world-class military by 2050.[105] Ultimately, civil-military fusion is to support Xi Jinping's grand project of "national rejuvenation," and establish China as a hegemon in the international system.[106]

To this end, quantum technologies are an opportunity for China to present to the world a genuinely Chinese technology that does not duplicate or imitate Western innovation. A consultancy business estimates public Chinese investment in quantum technologies to have exceeded $15 billion in 2022.[107] However, this figure is disputed. Exact figures are hard to come by but it must be assumed that China has amped up investment over the past years. Since the beginning of the 2020s, Chinese media have repeatedly claimed the country had become "a global leader in the fields of 5G, artificial intelligence, big data, internet of things, robotics, quantum computing, and outer space research" to the effect that national rejuvenation is going to "have a profound impact on [the] world".[108] While China seems to be excelling at signaling scientific leadership in quantum technologies, there is little, if any, information in the public domain that would speak to the leadership's and the PLA's vision regarding the actual strategic implications of quantum technologies for Chinese doctrine, or their operational integration with the Chinese military.[109]

Quantum computing and warfare

Even modest first-generation, noisy quantum computers of a small number of qubits would significantly improve China's warfighting capabilities. In the military domain, quantum computers will support wargaming and simulations, logistics and supply chain management and optimization, efficient energy use and predictive maintenance.[110]

Quantum computers are also likely to improve the Chinese Command and Control (C2) system. This is because quantum computers will outperform "classical" systems in key domains such as number-crunching or finding optimal paths out of many alternatives. Where a Chinese quantum computing system is faster in resolving large chunks of unstructured intelligence, surveillance and reconnaissance data, real-time scenario planning and decision support are going to vastly improve.[111]

[105] Emily Weinstein, "Don't Underestimate China's Military-Civil Fusion Efforts," *Foreign Policy*, June 28, 2024, https://foreignpolicy.com/2021/02/05/dont-underestimate-chinas-military-civil-fusion-efforts/.
[106] Avery Goldstein, "China's Grand Strategy under Xi Jinping: Reassurance, Reform, and Resistance," *International Security* 45, no. 1 (2020): 164–201, https://doi.org/10.1162/isec_a_00383.
[107] "Quantum technology sees record investments, progress on talent gap," *McKinsey Digital*, April 24, 2023, https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/quantum-technology-sees-record-investments-progress-on-talent-gap
[108] Digby Wren, "National Rejuvenation to Have a Profound Impact on World," *China Daily*, September 8, 2021, https://www.chinadaily.com.cn/a/202109/08/WS6137f4e9a310efa1bd66dfb9.html.
[109] "The Chinese Industrial Base and Military Deployment of Quantum Technology" (Washington DC: RAND Corporation, 2024), https://doi.org/10.7249/CTA3189-1.
[110] Michal Krelina, "Quantum technology for military applications," EPL Quantum Technology 8 (2021), 26.
[111] ATARC, "Applied quantum computing for today's military," ATARC Quantum Working Group, 2021.

However, fault-tolerant standalone quantum computers are notoriously difficult to build. This is because both the good and the bad, i.e. the processing power and the error rates of quantum computers scale exponentially—more qubits on a chip mean more noise and adverse quantum effects. Some qubit modalities require cryogenic cooling, which confines them to high-security laboratories, while all approaches suffer from short fidelity due to the extremely short lifespans of qubits (they are said to "decohere" quickly). By and large, the U.S. (and in some respect, Europe) seems to be leading in the development of quantum computers while China has not been able to announce major breakthroughs in this domain over the past couple of years, at least not publicly. That said, as of late, China seems to have refocused efforts in this area. Chinese media have recently reported the successful development of a 72-qubit superconducting quantum computer, which would push China ahead of U.S. industrial rivals such as Alphabet and IBM.[112] Estimates suggest that today, China spends four times as much on developing quantum computing capabilities as US industry.[113]

"Classical", digital computing works sequentially while quantum computers can hold many different states in parallel, which gives a quantum computer an advantage where a machine needs to resolve large amounts of data, or find the right solution among a vast number of possible candidates. This feature creates two distinct military vulnerabilities for the U.S. once quantum computers mature: they are going to break established encryption protocols whilst improving the speed of semi-automated decision-making processes. The former problem is largely being addressed by designing new classes of encryption protocols that even quantum computers find difficult to tackle. This is the field of post-quantum cryptography, which has received significant attention since the standardization of new lattice-based approaches by the National Institute of Standards and Technology (NIST) in 2023.

The second problem is a much bigger challenge should China be able to embed AI and ML in a quantum layer so that training data can be absorbed much more quickly and predictions made faster.[114] While the military leadership is unlikely to wholly surrender decision-making powers to machines, China could gain advantages if their automated decision support systems can aggregate large amounts of data more efficiently and in real-time, especially where large feeds from combats in multiple theaters must be resolved quickly. Progress of this sort would likely increase strategic instability by eroding crisis stability.

Satellite-based quantum communications

Quantum communication is the transmission of information over secure quantum channels that protect communication against eavesdropping thanks to a quantum layer that allows for the

[112] Xinhua, "China's 3rd-gen superconducting quantum computer goes into operation," China Daily, 7 January 2024, https://www.chinadaily.com.cn/a/202401/07/WS6599f6f2a3105f21a507ae67.html.
[113] Wilson Beaver, "The urgency of the quantum computing race with China," The Heritage Foundation, 14 September 2023, https://www.heritage.org/technology/commentary/the-urgency-the-quantum-computing-race-china.
[114] J.R. Wilson, "The future of artificial intelligence and quantum computing," Military + Aerospace, 25 August 2020, https://www.militaryaerospace.com/computers/article/14182330/future-of-artificial-intelligence-and-quantum-computing.

secure exchange of keypairs. Various protocols exist, the most prominent being Quantum Key Distribution (QKD), first introduced conceptually in 1984.[115]

Quantum communication is "information-theoretically" secure. This means that the mathematics of the protocols are such that eavesdropping is impossible without causing the quantum states of photon pairs to collapse, thus inevitably raising an alarm. The absolute security of the protocol applies to all current and future iterations of it.

However, significant challenges remain and serious vulnerabilities emerge from the difficulties around implementing the protocols in real-world systems. While the quantum element of the system is information-theoretically secure, quantum hackers have successfully compromised endpoints and connectors where quantum communication systems connect with digital hardware and infrastructure.[116] Here, the problems are manifold and currently offset the advantages of quantum-securing the exchange of keypairs. At present, the National Security Agency (NSA) and the Government Communications Headquarters (GCHQ) in the UK see little value in these protocols and consider the direct military and security implications for the U.S. and Allied Forces manageable.[117]

This being said, the implications of a complete and comprehensive Chinese quantum communication system are considerable. The signal quality of intercept communication would surely drop whilst providing the Chinese leadership with unprecedented capabilities for cyber offense.

The issue is exacerbated by a Chinese leadership position in satellite-based quantum communications. Unlike electrical signals and radio waves, quantum signals cannot be amplified: the "no-cloning theorem" in quantum mechanics shows that amplification would inadvertently collapse the quantum system. This property of quantum bits, such as photons that are used in quantum communication, requires the development of complex quantum repeaters and memory systems. On Earth, quantum signals have a maximum reach of approximately 100 kilometers before they die out.

This gives satellite-based quantum communications, where photons are subject to significantly less disturbance and noise, an immediate advantage. At present, China is the only power that has access to a quantum satellite. *Micius* was launched in 2016.[118] Whilst facing its own challenges,

[115] Charles H. Bennett and Gilles Brassard, "Quantum cryptography: Public key distribution and coin tossing," Proceedings of IEEE International Conference on Computers, Systems and Signal Processing (1984): 175-179; Bennett et al., "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels," Physics Review Letters (1993): 1895-1899; Sheng-Kai Liao et al., "Satellite-to-ground quantum key distribution," Nature 549 (2017): 43-47; Xiao-Ling Pang et al., "Hacking quantum key distribution via injection locking," Physical Review Applied 13 (2020); Valerio Scarani, "The security of practical quantum key distribution," Reviews of Modern Physics 81.3 (2009): 1301-1350.

[116] Pang et al., "Hacking quantum key distribution."

[117] "GCHQ (NCSC) White Paper," Quantum Security Technologies, 24 March 2020, https://www.ncsc.gov.uk/whitepaper/quantum-security-technologies; NSA / Central Security Service, "Quantum Key Distribution and Quantum Cryptography," n.d., https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/.

[118] Marcus Strom, "Chinese quantum satellite Micius breaks record for distribution distance of quantum entangled photons," The Sydney Morning Herald, 15 June 2017, https://www.smh.com.au/technology/chinese-quantum-satellite-micius-breaks-record-for-distribution-distance-of-quantum-entangled-photons-20170615-gwrh0u.html.

such as an error rate of more than 95 percent, the satellite avoids the installation of costly repeaters every 100 kilometers or so and is a remarkable engineering feat.

China has also made impressive progress in developing ground-to-ground repeaters. Recent successes include hybrid setups, which combine satellite and ground repeaters, in which communication was achieved over a distance of 4,600 kilometers.[119] Applications range from securing government communication to providing the infrastructure for future financial and cryptocurrency trade networks, which are surely of interest to regimes that are keen to evade Western sanctions such as that of North Korea.

The ultimate goal of Chinese efforts in this domain is to make progress towards building a rudimentary quantum internet that can be connected and decoupled from the Internet as Chinese decision makers deem appropriate.[120] U.S. and allied intelligence services are going to have a much harder job gathering intelligence once China can easily decouple parts of its internet infrastructure.

What is more, novel domestic quantum communication systems would greatly support Chinese "harvest now, decrypt later" cyber activities that see vast amounts of encrypted data siphoned off the internet in the hope to quantum-decrypt such data at a later stage.[121] China is likely to already hold large amounts of sensitive public and private sector data harvested from Western sources. Of little use now they will become important assets once quantum decryption becomes possible. At the same time, future quantum communication networks will protect domestic Chinese data from similar harvesting attempts by non-Chinese entities.

While early-generation quantum communication systems are surely clunky, hardware-intensive and expensive to develop and service, as the NSA and GCHQ have pointed out in their joint statement, the wholesale dismissal of these systems seems somewhat myopic. No matter how small, any chance for China to obtain leverage over a comprehensive advanced communication system that the U.S. and its allies choose not to develop should be a cause of concern.

Quantum navigation and underwater warfare

Quantum communication networks, i.e. early-generation, mid-range quantum computers that are connected over secure quantum channels, should significantly enhance Chinese positioning, navigation and timing (PNT) systems. This would be a capability that is separate from but complementary to BeiDou, China's own Global Navigation Satellite System (GNSS), which Western commentators already consider largely superior to the Global Positioning System (GPS).[122]

[119] Yu-Ao Chen, "An integrated space-to-ground quantum communication network over 4,600 kilometres," Nature 589 (2021): 214-219.
[120] Koji Azuma et al., "Quantum repeaters: From quantum networks to the quantum internet," Review of Modern Physics 95 (2023).
[121] David Lague, "U.S. and Chinarace to shield secrets from quantum computers," Reuters, 14 December 2023, https://www.reuters.com/investigates/special-report/us-china-tech-quantum/.
[122] Sarah Sewall, Tyler Vandenberg, and Kaj Malde, "China's BeiDou: New dimensions of great power competition" (Cambridge, MA: Harvard Belfer Center for Science and International Affairs, 2023).

Quantum navigation is especially useful in GNSS-denying, -degrading or challenging environments, such as underground and underwater, or where GNSS signals are jammed. Quantum sensors would increase the survival rate of Chinese capabilities against attacks on BeiDou satellites. Chinese inertial navigation systems (INS) that would compensate for a loss of GNSS, would also benefit enormously from quantum sensors. Research suggests that even the most advanced INS drift by approximately 1.5 kilometers per hour for aircraft, and 1.8 kilometers per day for submarines and ships, to which quantum sensors could offer a 50-fold improvement.[123] Some commentators even suggest a 1,000-fold improvement in the self-positioning of submerged submarines.[124]

Long-term, a Chinese quantum navigation system would significantly enhance clock precision and synchronization, thus making for a better and more effective network with fewer satellites whilst effectively protecting its networks against cyberattacks. In the increasingly important space domain, fewer satellites dramatically reduce the attack surface of Chinese C2 systems.

Quantum technology prototypes are typically clunky and heavy. Given their size, submarines seem the most likely assets to accommodate additional quantum capabilities, at least in the near and medium terms. Chinese quantum-enhanced submarines would certainly be a significant challenge to US submarine dominance in the Pacific Region where improved Chinese sensors and submarines prove a growing problem already.[125]

To effectively deny Chinese submarine capabilities, superconducting quantum interference devices, appropriately abbreviated SQUIDS, seem a plausible response.[126] Installed along coast lines, for instance, SQUIDS are extremely sensitive magnetometers that improve detection ranges from several hundred meters to six kilometers or more.[127]

Quantum radar

A quantum radar offers three distinct advantages over its "classical" counterpart: i) a higher signal-to-noise ratio, which makes the radar better withstand jamming attacks or other electronic countermeasures; ii) possible non-detection if the number of employed photons is below enemy detection barriers; and iii) potential target identification and illumination.[128]

The prospect of a Chinese quantum radar detecting U.S. stealth bombers proved a major concern in November 2018 when news broke about experimental successes at China Electronics Technology Group Corporation (CETC), one of China's leading defense manufacturers, to build

[123] Daniel Choi, Quantum technology and the military–revolution or hype?: The impact of emerging quantum technologies on future warfare (Quantico, VA: Marine Corps University Press, 2023).
[124] Parker, Commercial and military applications and timelines for quantum technology.
[125] Alastair Gale, "The era of total U.S. submarine dominance over China is ending," The Wall Street Journal, 20 November 2023, https://www.wsj.com/world/china/us-submarine-dominance-shift-china-8db10a0d.
[126] Dietmar Drung et al., "Highly sensitive and easy-to-use SQUID sensors," IEEE Transactions on Applied Superconductivity 17 (2007): 699-704.
[127] Krelina, "Quantum technology for military applications," 38.
[128] Jeffrey H. Shapiro, "The quantum illumination story," IEEE Aerospace and Electronic Systems Magazine 35 (2020): 8-20; Ricardo Gallego Torrome, Nadya Bekhti-Winkel, and Peter Knott, "Introduction to quantum radar," arXiv preprint, 2021, https://arxiv.org/pdf/2006.14238.pdf.

a quantum radar prototype.[129] Similar announcements thereafter would gain significant traction in the media.

Initial concern about Chinese progress in this domain, however, seemed unwarranted. By and large, the advantages of a quantum radar remain conceptual and theoretical. Especially a long-range surveillance quantum radar will be prohibitively expensive to build and maintain. This is due to the exponential speedup of photon resources required as the radar extends.[130] Some commentators express doubts about effective anti-jamming also, citing examples of smart techniques that can compromise a quantum radar just as much as established radar systems, yielding no advantage for the significantly more expensive quantum system. Research in this domain is very much ongoing, with Chinese media every now and then reissuing claims that a stealth-detecting quantum radar was near completion.[131]

AI

This section summarizes how the Chinese political and military leadership, and Chinese academics and commentators, think about the use of AI for military purposes and how they envision the integration of AI-enabled systems for the purpose of winning major future wars. The significant technical differences between AI, ML, systems with autonomous capabilities (SACs)[132] and algorithmic decision-making notwithstanding, this section collects them under the umbrella term of AI. This is to mirror how Chinese experts and military officials themselves employ, and at times conflate, these concepts.[133]

The People's Liberation Army (PLA) typically refers to AI-enabled systems in terms of "intelligentized warfare" [智能化作战].[134] The Chinese leadership remains purposefully vague and obscure in its definition of "intelligence," and "intelligentization."[135] However, in its defense strategy, the Chinese Ministry of National Defense points to advancing the "integrated development of mechanization and informationization, speed[ing] up the development of

[129] Martin Giles, "The US and China are in a quantum arms race that will transform warfare," MIT Technology Review, 3 January 2019, https://www.technologyreview.com/2019/01/03/137969/us-china-quantum-arms-race/.
[130] Fred Daum, "Quantum radar cost and practical issues," IEEE Aerospace and Electronic Systems Magazine 35 (2020): 8-20.
[131] See, for example, Stephen Chen, "Chinese team says quantum physics project moves radar closer to detecting stealth aircraft," South China Morning Post, 3 September 2021, https://www.scmp.com/news/china/science/article/3147309/chinese-team-says-quantum-physics-project-moves-radar-closer.
[132] NATO Allied Command Transformation, *Autonomous Systems: Íssues for Defence Policymakers*, ed. Andrew P Williams and Paul D Scharre (Norfolk, Va.: NATO HG SACT, 2016), https://www.act.nato.int/images/stories/media/capdev/capdev_02.pdf.
[133] Ryan Fedasiuk, "Chinese Perspectives on AI and Future Military Capabilities," CSET Policy Brief (Washington DC: Center for Security and Emerging Technology, August 2020), https://cset.georgetown.edu/publication/chinese-perspectives-on-ai-and-future-military-capabilities/.
[134] Michael Dahm, "Chinese Debates on the Military Utility of Artificial Intelligence," *War on the Rocks* (blog), June 5, 2020, https://warontherocks.com/2020/06/chinese-debates-on-the-military-utility-of-artificial-intelligence/.
[135] Sam Bresnick, "China's Military AI Roadblocks: PRC Perspectives on Technological Challenges to Intelligentized Warfare," Issue Brief (Washington DC: Center for Security and Emerging Technology, June 2024), 4, https://cset.georgetown.edu/publication/chinas-military-ai-roadblocks/.

intelligent military, [and] creat[ing] a modernized military force structure with Chinese characteristics"[136] as the key parameters of intelligentized warfare. Whilst avoiding exact definitions, Chinese commentators typically describe "intelligent," or "intelligentized warfare" as a novel type of war that combines human and machine intelligence, and they forecast extensive use of AI-enabled systems across most, if not all, military applications.[137]

The Chinese military establishment therefore considers AI of critical importance in its force planning for future wars as being wide-ranging confrontations between large-scale opposing "operational systems [作战体系]," rather than between units and services.[138] For China, AI is a central piece in the larger puzzle that is "systems on systems warfare"[139]; a theory of victory that places heavy emphasis on force integration as well as combining kinetic and non-kinetic means.[140]

China's rapid ascent towards becoming a science and technology superpower, paired with a strong industrial base, access to cheap energy as well as the CCP's (Chinese Communist Party) close ties with the country's private sector, increasingly allow for quick scale-ups of innovation in emerging technologies, especially AI.[141] Robust data on Chinese investment levels are hard to come by. However, a 2023 study of U.S. and Chinese procurement activity in 2020 suggests that American and Chinese military forces "are devoting comparable levels of attention to a similar suite of AI applications."[142] Since then China has certainly not slowed down. For this reason, a growing number of voices warn publicly against underestimating Chinese progress in this domain.[143]

Recent organizational challenges within the PLA reflect Xi Jinping's commitment to making the Chinese military "world-class" [世界一流军队] by 2050.[144] The PLA's Strategic Support Force (SSF), which used to oversee AI development efforts alongside information and cyberwarfare

[136] Ministry of National Defense, "Defense Policy - Ministry of National Defense," Defense Policy, accessed June 21, 2024, http://eng.mod.gov.cn/xb/DefensePolicy/index.html.
[137] Kevin Pollpeter and Amanda Kerrigan, "The PLA and Intelligent Warfare: A Preliminary Analysis" (Arlington VA: Center for Naval Analyses, October 2021), https://www.cna.org/reports/2021/10/The-PLA-and-Intelligent-Warfare-A-Preliminary-Analysis.pdf.
[138] Jeffrey Engstrom, *Systems Confrontation and System Destruction Warfare: How the Chinese People's Liberation Army Seeks to Wage Modern Warfare* (Santa Monica CA: RAND Corporation, 2018), 3, https://doi.org/10.7249/RR1708.
[139] Ibid.
[140] For reasons of tractability and to stick to the brief, this section does not consider the role of AI in purely non-kinetic Chinese information warfare campaigns, a domain that is of immense importance to the Chinese leadership and would demand a separate report to do justice to the complexity of the topic.
[141] The Economist, "China Has Become a Scientific Superpower," *The Economist*, June 12, 2024, https://www.economist.com/science-and-technology/2024/06/12/china-has-become-a-scientific-superpower.
[142] Margarita Konaev et al., "U.S. and Chinese Military AI Purchases" (Center for Security and Emerging Technology, August 2023), 1, https://doi.org/10.51593/20200090.
[143] "Preserving U.S. Military Advantage Amid Rapid Technological Change" (Center for a New American Security, March 12, 2024), https://www.cnas.org/publications/congressional-testimony/preserving-u-s-military-advantage-amid-rapid-technological-change.
[144] "Testimony before the U.S.-China Economic and Security Review Commission. Hearing on Trade, Technology, and Military-Civil Fusion: Chinese Military Innovation in Artificial Intelligence" (Washington DC, June 7, 2019), https://www.uscc.gov/sites/default/files/June%207%20Hearing_Panel%201_Elsa%20Kania_Chinese%20Military%20Innovation%20in%20Artificial%20Intelligence_0.pdf.

capability planning, was recently split into three dedicated units: the Information Support Force, Cyberspace Force, and Aerospace Force are now standalone units under the Central Military Commission.[145]

Akin to the global dissemination of AI applications across the public and private sectors, the Chinese military adopts AI to automate repetitive and somewhat mundane tasks to free up human and financial resources. Efforts focus on health monitoring, personnel management, and predictive maintenance in the logistics and supply chain management for combat units.[146] This is where AI has proved successful and implementable.

Estimates suggest that the PLA spends a minimum of $1.6 billion annually on AI-related R&D (research and development). In 2020, a bulk of investment went into developing new intelligence and surveillance systems also. AI-enabled target recognition and fire control research were other important domains over the past couple of years; developing semi-automated undersea capabilities that could challenge U.S. dominance in this domain were also a priority.[147]

A large number of official Mandarin-language defense magazines and journals regularly add to the long list of applications that the PLA hopes to realize over the next two decades.[148] The below collects the most relevant priority areas that the PLA and Party leadership are pursuing in various projects, as reflected in open-source publications.

Summarily, Chinese strategists hold AI to be playing a crucial role in facilitating human-machine teaming over flexible computer networks across domains. There is also widespread agreement among Chinese experts that AI will realize efficiency gains by improving target tracking and the speed of force deployment.[149]

ML and Deep Learning

For the PLA, ML and Deep Learning serve the dual purpose of making existing systems better while also providing new capabilities altogether. Objectives are automated fault-prediction for better maintenance, novel algorithms for remote-sensing, and Natural-Language Processing (NLP) for the analysis of military intelligence. Neural networks are hoped to enhance precision in Automatic Target Recognition (ATR), and improve the modeling and simulation of wargames, as well as missile guidance.[150]

[145] Bresnick, "China's Military AI Roadblocks: PRC Perspectives on Technological Challenges to Intelligentized Warfare," 10.
[146] Ryan Fedasiuk and Emily Weinstein, "AI in the Chinese Military," in *Chinese Power and Artificial Intelligence* (Routledge, 2022), 175.
[147] Ryan Fedasiuk, Jennifer Melot, and Ben Murphy, "Harnessed Lightning: How the Chinese Military Is Adopting Artificial Intelligence" (Center for Security and Emerging Technology, October 2021), https://doi.org/10.51593/20200089.
[148] https://libguides.gwu.edu/c.php?g=258984&p=1728996
[149] Fedasiuk, "Chinese Perspectives on AI and Future Military Capabilities."
[150] "Testimony before the U.S.-China Economic and Security Review Commission. Hearing on Trade, Technology, and Military-Civil Fusion: Chinese Military Innovation in Artificial Intelligence."

Network integration

The PLA places heavy emphasis on integrating AI with future "ubiquitous networks" (泛在网络)" that are supposed to close the time lag between threat perception and action.[151] AI is hoped to considerably shorten the OODA (observe-orient-decide-act) loop as AI-enabled systems will "raise situational awareness, and assist commanders in formulating judgments, planning missions, generating action plans, controlling operations, and making decisions"[152] over tightly integrated control networks. The integration of 5G and AI-enabled communication hardware is hoped to provide the communications backbone for joint and multi-domain operations.

Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR)

The gradual replacement of human operators with AI-enabled systems and SACs promises a significant speedup of decision-making processes, and a qualitative improvement thereof. This is due to, Chinese commentators argue, better data on battleground depth and complexities that can be aggregated faster, and, ultimately, allow for improved targeting and strike capabilities. Some Chinese experts speak of a "1+1>2" effect, meaning the "next-generation kill chain will be greater than the sum of its parts."[153]

Unmanned Systems

Analysis suggests the development of unmanned and semi-autonomous vehicles are at the top of the PLA's priority areas.[154] Chinese commentators envision a "seamless integration" of AI-enabled systems for ISR. Success in the battlefield and the ability to offset the enemy's counter attacks will be determined by the speed, accuracy and reliability of novel SACs. In this context, reports of a machine gun-equipped robot dog have recently surfaced. The robot is supposed to replace "our (human) members to conduct reconnaissance and identify (the) enemy and strike the target," a Chinese serviceman said.[155] Undersea capabilities are also at the top of the agenda.

While China considers AI paramount to its strategic aim to surpass the U.S. militarily, much of the above cited projects and priority areas are aspirational in character, and development is marked by varying degrees of success. The PLA faces a series of obstacles in realizing the full

[151] Michael Dahm, "Chinese Debates on the Military Utility of Artificial Intelligence," *War on the Rocks* (blog), June 5, 2020, https://warontherocks.com/2020/06/chinese-debates-on-the-military-utility-of-artificial-intelligence/.
[152] Jeremy Rausch et al., *China's Military Decision-Making in Times of Crisis and Conflict*, ed. Roy Kamphausen (Seattle WA, Washington DC: The National Bureau of Asian Research, 2023), 70, https://www.nbr.org/wp-content/uploads/pdfs/publications/chinas-military-decision-making_sep2023.pdf.
[153] Bresnick, "China's Military AI Roadblocks: PRC Perspectives on Technological Challenges to Intelligentized Warfare," 12.
[154] Fedasiuk and Weinstein, "AI in the Chinese Military."
[155] Brad Lendon and Nectar Gan, "China's Military Shows off Rifle-Toting Robot Dogs," *CNN*, May 28, 2024, https://www.cnn.com/2024/05/28/china/china-military-rifle-toting-robot-dogs-intl-hnk-ml/index.html.

potential of machine intelligence, many of which are outlined in a June 2024 CSET report.[156] Chinese academics are quoted as saying that "compared with other military powers in the world, military intelligence in China is still in its infancy."[157] Such critical reflections align with views in the West: with a view to automation and autonomy in the UK's Armed Forces, a retired British General recently commented that "the irony here is that we talk as if AI is everywhere in defence, when it is almost nowhere."[158] Significant gaps between aspiration and reality in AI development are not exclusive to the PLA.

The challenges and obstacles that China is facing can be broadly summarized as follows:

- The PLA and China's military-industrial complex lack the right standards and robust evaluation practices and processes to make AI-enabled systems safe and deployable. Interoperability issues are of chief concern. Sources speak of "scattered and chaotic conditions'" within the PLA that make milestones a moving goalpost and the overall objective of building future-proof applications fit for system-on-system warfare difficult to achieve;[159]

- Entrenched problems in China's domestic supply chain harm sensor development, integration and deployment for ISR;

- Data collection and management practices are not fit for purpose so that AI-enabled intelligence analysis remains underdeveloped. Both in terms of quantity and quality, the PLA does not have sufficiently developed corpuses of training data available to see the U.S. eye to eye in the training of military AI;

- For the PLA, AI is somewhat a double-edged sword as it may widen the attack surface for U.S.-led cyber attacks;

- Not unlike across other militaries, some of the senior PLA leadership place little trust in AI-enabled systems. Explainability gaps plague the development of trustworthy AI not just in China but globally.[160] The bulk of comments from within the Chinese research community revolve around the stubborn problem of explainability in AI-enabled decision-making, which hinder uptake and erode confidence among service personnel in a system's reliability and performance metrics.

Chinese academic and military commentators largely employ the term "strategic stability" in ways similar to U.S. and allied policymakers, i.e. as comprising first-strike, crisis, and arms race

[156] Bresnick, "China's Military AI Roadblocks: PRC Perspectives on Technological Challenges to Intelligentized Warfare."
[157] Bresnick, 14.
[158] The Economist, "How AI Is Changing Warfare," *The Economist*, June 20, 2024, https://www.economist.com/briefing/2024/06/20/how-ai-is-changing-warfare.
[159] Bresnick, "China's Military AI Roadblocks: PRC Perspectives on Technological Challenges to Intelligentized Warfare," 26.
[160] Juljan Krause, "Trusted Autonomous Systems in Defence: A Policy Landscape Review," The Policy Institute (London: King's College London, November 2021), https://doi.org/10.18742/pub01-063.

stability.[161] A majority of Chinese commentators seem to agree that AI will erode strategic stability and complicate China's deterrence relationship with the U.S.[162] Recent analyses of Chinese publications suggest that the Chinese establishment fears that emerging technologies such as AI could undermine "China's second-strike capability and require a reassessment of how asymmetric strategic stability may be restored."[163]

Concerns in this context are plentiful. AI is assumed to increase risks of miscalculation and, ultimately, escalation whilst making Chinese forces more vulnerable to U.S. strikes that may overwhelm Chinese air defenses.[164] The number of preemptive strikes may rise if AI-enabled systems are less risk-averse than human decision-makers.

Bearing in mind the aforementioned obstacles alongside other technical as well as organizational issues, the PLA "sees itself as the weaker side in the overall military balance."[165] Given its deeply entrenched views on war being a "systems-on-systems" confrontation, internally the Chinese leadership does not hold the PLA having made sufficient progress in AI against the U.S. Armed Forces, its chief benchmark. However, the field of machine intelligence is moving fast, and the steady rise of academic output from Chinese scientists that are affiliated with the country's defense sector attests to China's concerted efforts to close this gap.

Conclusion

We have laid out a framework of analysis based on three high-order explanations linking technologies and stability and discussed the developments of hypersonics, quantum technologies, and AI in Russia and China. Putting them together shows that the sources of (in)stability differ between the two countries and across technologies.

Risks of instability related to technological developments in Russia mostly rest in uncertainty around the nature of its ASAT weapons and its muddying the information environment with the assistance of AI. States can never be certain of others' intentions,[166] but the level of uncertainty can increase if receivers can barely trust the signals and messages communicated by senders. Uncertainty could also rise considering that the U.S. intelligence community remains unsure about the nuclear nature of Russia's ASAT weapons. Warhead ambiguity, that is, whether a weapon is carrying a nuclear warhead, can drive escalation by leading target states to react preemptively or preventively to avoid the worst outcome in times of conflict. The dual-capability of Russia's hypersonic weapons may also contribute to instability in the event of a crisis. The

[161] Li Bin and Tong Zhao, eds., *Understanding Chinese Nuclear Thinking* (Washington DC: Carnegie Endowment for International Peace, 2016), https://carnegie-production-assets.s3.amazonaws.com/static/files/ChineseNuclearThinking_Final.pdf.
[162] Fedasiuk, "Chinese Perspectives on AI and Future Military Capabilities."
[163] Alison A Kaufman and Brian Waidelich, "PRC Writings on Strategic Deterrence: Technological Disruption and the Search for Strategic Stability" (Arlington VA: Center for Naval Analyses, February 2023), iii, https://www.cna.org/reports/2023/04/PRC-Writings-on-Strategic-Deterrence.pdf.
[164] Fedasiuk, "Chinese Perspectives on AI and Future Military Capabilities."
[165] Mark Cozad et al., *Gaining Victory in Systems Warfare: China's Perspective on the U.S.-China Military Balance* (RAND Corporation, 2023), https://www.rand.org/pubs/research_reports/RRA1535-1.html.
[166] Rosato 2021.

improvements these weapons may provide to Russia may have some impact on intrawar deterrence, making Russia escalation more likely. This is most pronounced in the Kremlin's perception of Tsirkon as a potential tool for striking carrier groups, potentially American conventional deterrence in a crisis or limited regional war. The actual performance of Russian hypersonic weapons in Ukraine, where they have proven to be vulnerable to Patriot, will likely erode this perception somewhat, limiting how destabilizing Tsirkon can be. Although Russia has devoted resources to the development of its hypersonics capabilities, the potential advantages that can be obtained at the strategic nuclear level appear minimal because much of what these technologies can do can already be achieved by Russia's existing weapons. Thus, it is unlikely that developments in this area would drastically change the calculations in Moscow, barring changes in its political goals. In fact, strategic stability may strengthen if developments in AI or hypersonic weapons leads to greater survivability in Russia's nuclear arsenal, reinforcing mutual deterrence between Russia and the United States. Russian quantum abilities are also unlikely to be destabilizing, as Russia remains far behind other countries in both quantum investment and quantum capabilities.

In China's case, however, all three pathways of instability exist, and advantages gained by China may put the United States in a bad position should advancements come through. With success in the area of hypersonics, China can weaken the United States's warfighting capabilities in the Pacific by interrupting communications, for example, and threaten the credibility of the U.S.'s extended deterrence given the doubts East Asian allies might have of the U.S.'s ability to defend both itself and its allies. In quantum technologies, China has already demonstrated some remarkable success, and plans to leverage such capabilities can enhance China's abilities both strategically and operationally. However, real or perceived disadvantages in its AI developments may induce caution in China given the high value it places on AI and how its leadership perceives AI as a key factor in gaining advantages militarily. That said, the direction in which this disadvantage may influence stability is indeterminate. Such disadvantages can similarly precipitate crises and encourage recklessness if China believes its nuclear deterrence and retaliatory capabilities to be at a greater risk. China's eagerness to integrate AI throughout its military can furthermore introduce instability by severely compressing timescales and raising the likelihood of preemptive nuclear strikes if it trusts AI to inform or implement the "launch under attack" retaliatory option.

Different from Russia, where uncertainty in its developments and plans may derive from its relative lack of interest in technological breakthroughs,[167] opacity around China's technological developments, goals, and plans may be somewhat deliberate. Indeed, China understands transparency differently than the United States and sees nuclear ambiguity, for example, as a crucial part of maintaining deterrence.[168] As such, general uncertainty and skepticism surround China's actions, which create pressures for arms racing to guard against deception or changes to

[167] Ross Buchanan, Ryan Christernson, Daniel Kroth, Kaitlyn Lenkeit, Madeleine Lambert, Kimberly Peh, and Brandon Kirk Williams, "Techno-Optimism, Geopolitics, and the Future of AI," Workshop Summary, (Livermore, CA: Lawrence Livermore National Laboratory Center for Global Security Research, 2024), https://cgsr.llnl.gov/content/assets/docs/Techno-Optimism-Geopolitics-and-the-Future-of-AI-Workshop-Summary.pdf.

[168] Li Bin, "Appendix 3A. China and Nuclear Transparency," in Transparency in Nuclear Warheads and Materials: The Political and Technical Dimensions, edited by Nicholas Zarimpas, 50-57, (Oxford University Press: 2003), https://www.sipri.org/sites/default/files/files/books/SIPRI03Zarimpas/SIPRI03Zarimpas03A.pdf.

China's declared stance, including on the purpose of its technological developments. To complicate matters, China sees all technologies as dual use. As mentioned, the Chinese leadership is outspoken about its technology policy of "military-civil fusion" for making progress towards "national rejuvenation." This view of technologies entangles nuclear and conventional capabilities, which can easily lead to escalation due to conflicting views on the nature of the attack and target.

The concluding thoughts here illustrate how the framework assists in understanding the effects of technology. It should at least be clear from this discussion that advanced technologies do not uniformly lead to stability or instability, and the same technology may not always result in similar outcomes. Hence, simply starting from the characteristics of each technology, which most analyses do, may not be the best way to approach this issue. Moreover, depending on the level of development and each country's plan to use these weapons, the extent of the effect on stability may differ too. Thus, context matters, and it needs to be a factor when considering how technologies relate with strategic outcomes.

GLOSSARY

The term “quantum technologies” typically comprises four specific technology clusters. While complementary, they can be implemented separately and independently.

Quantum computing: the manipulation of the states of quantum objects (“qubits”) for the purpose of encoding information. “State” means the electromagnetic spin of electrons or the polarization of photons. While “classical” computers encode information physically by amplifying electrical signals, i.e. charges to micro-transistors, the computational load of a quantum computer is realized by manipulating the state-spaces of qubits. While the processing power of “classical” digital computers is a linear function of the number of micro-transistors placed on a chip, the processing power of a quantum computer grows exponentially in the number of qubits, which makes it a much more powerful machine for certain classes of problems.

Quantum communications: several protocols exploit the characteristic features of photons to securely exchange key pairs for the purpose of encrypting messages. The nature of quantum channels is such that eavesdropping is impossible without raising an alarm, which makes the technology extremely secure, at least in principle. It is important to note that the actual message that is to be exchanged will still need to be transmitted digitally; the quantum element only relates to the exchange of key pairs.

Quantum sensing, imaging and metrology: the most developed if not prominently discussed domain of quantum technologies. Near-term, quantum sensing and imaging have the most tangible effects on improving or extending weapon systems and other military technologies.