STRATEGIC STUDIES QUARTERLY - FEATURE ARTICLE

Artificial Intelligence: A Threat to Strategic Stability

James S. Johnson

Abstract

AI-augmented conventional capabilities might affect strategic stability between great military powers. The nuanced, multifaceted possible intersections of this emerging technology with a range of advanced conventional weapons can compromise nuclear capabilities, thus amplifying the potentially destabilizing effects of these weapons. This article argues that a new generation of artificial intelligence–enhanced conventional capabilities will exacerbate the risk of inadvertent escalation caused by the commingling of nuclear and nonnuclear weapons. The increasing speed of warfare will also undermine strategic stability and increase the risk of nuclear confrontation.

*****

The hyperbole surrounding artificial intelligence (AI) makes it easy to overstate the opportunities and understate the challenges posed by the development and deployment of AI in the military sphere.[1] Commingling and entangling nuclear and nonnuclear capabilities and the increasing speed of warfare may well undermine strategic stability.[2] From what we know today about emerging technology, new iterations of AI-augmented advanced conventional capabilities will compound the risk of military escalation,[3] especially inadvertent and accidental escalation.[4] While the potential escalation risks posed by advances in military technology have been discussed lightly in the literature, the potential of military AI to compound the risk and spark inadvertent escalation is missing.[5] This article addresses *how* and *why* AI could affect strategic stability between nuclear-armed great powers (especially China and the United States) and the multifaceted possible intersections of this disruptive technology with advanced conventional capabilities.[6]

Toward this end, the article conceptualizes and defines military-use AI and identifies a broad portfolio of nonnuclear weapons with "strategic effects"[7] along with their attendant enabling systems, including specific AI innovations that pose the greatest risks to nuclear stability.[8] Rather than provide a net assessment of all of the possible ways AI could influence strategic stability, the article instead examines the possible stability enhancing and destabilizing effects in the nuclear domain using two examples: swarming autonomous weapon systems (AWS) and hypersonic weapons.[9]

Conceptualizing Military Artificial Intelligence

Four core themes help conceptualize military-relevant AI.[10] First, AI does not exist in a vacuum. That is, in isolation AI will unlikely be a strategic game changer. Instead, it will mutually reinforce the destabilizing effects of existing advanced capabilities, thereby increasing the speed of warfare and compressing the decision-making time frame. Second, AI's impact on stability, deterrence, and escalation will likely be determined as much by a state's perception of its functionality than what it is capable of doing. In the case of nuclear policy, deterrence, and strategic calculations more broadly, the perception of an adversary's capabilities and intentions is as important as its actual capability. In addition to the importance of military force postures, capabilities, and doctrine, the effects of AI will therefore also have a strong cognitive element, increasing the risk of inadvertent escalation as a result of misperception and misunderstanding. For the foreseeable future, military AI will include a fair degree of human agency, especially in the safety-critical nuclear domain. Thus, strategic calculations on the use of force made in collaboration with machines at various levels will continue to be informed and shaped by human perceptions.

Third, the increasingly competitive and contested nuclear multipolar world order will compound the destabilizing effects of AI and, in turn, increase escalation risks in future warfare between great military powers—especially China and the United States. Moreover, the potential operational and strategic advantages offered by AI-augmented capabilities could prove irresistible to nuclear-armed strategic rivals. Thus motivated, adversaries could eschew the limitations of AI, compromising safety and verification standards to protect or attempt to capture technological superiority on the future digitized battlefield.[11] Finally, and related, against this inopportune geopolitical backdrop, the perceived strategic benefits of AI-powered weapons will likely attract states as a means to sustain or capture the technological upper hand over rivals. The most pressing risk posed to nuclear security is, therefore, the premature adoption of unsafe, error-prone, unverified, and unreliable AI technology in the context of nuclear weapons, which could have catastrophic implications.[12]

Military AI applications can be broadly categorized into those that have utility at a predominately operational or strategic level of warfare.[13] At the operational level, applications include autonomy[14] and robotics (especially drone swarming); multi-actor interaction during red teaming and war gaming; big data–driven modeling;[15] and intelligence analysis to locate and monitor mobile missiles, submarines, mines, and troops movement.[16] At a strategic level, applications include (1) intelligence, surveillance, and reconnaissance (ISR) and command, control, communications, and intelligence (C3I) systems (especially in complex, adversarial, and cluttered environments);[17] (2) enhanced missile defense with machine-learning-augmented automatic target recognition (ATR) technology (i.e., improving target acquisition, tracking, guidance systems, and discrimination);[18] conventional precision missile munitions (including but not limited to hypersonic variants) able to target strategic weapons; (3) increased speed and scope of the observation, orientation, decision, and action (OODA) loop decision-making to augment air defense and electronic warfare (especially in antiaccess/area-denial [A2/AD] environments); and (4) AI-enhanced offensive and defensive cyber capabilities (e.g., machine learning techniques to infiltrate and uncover network vulnerabilities and to manipulate, spoof, and even destroy these networks).[19]

While the potential strategic effects of military AI are not unique or exclusive to this technology, the confluence of several trends weighs heavily on the pessimistic side of the instability-stability ledger: the rapid technological advancements and diffusion of military AI; the inherently destabilizing characteristics of AI technology (especially heightened speed of warfare, explainability, and vulnerability to cyberattack); the multifaceted possible intersections of AI with nuclear weapons; the interplay of these intersections with strategic nonnuclear capabilities; and the backdrop of a competitive multipolar nuclear world order, which may entice states to prematurely deploy unverified, unreliable, and unsafe AI-augmented weapons into combat situations. The historical record demonstrates that security competition—motivated by the desire to control warfare—tends to be ratcheted up because of the complexity of military technology and operations over time.[20] As a result, the Clausewitzian conditions of "fog and friction" will likely become a ubiquitous outcome of the uncertainties created by increasingly complex and inherently escalatory technologies.

From this perspective, the acceleration of modern warfare, the shortening of the decision-making time frame, and the commingling of military systems have occurred within the broader context of the computer revolution (e.g., remote sensing, data processing, acoustic sensors, communications, and cyber capabilities).[21] These overarching trends do *not rely on AI* and would have likely occurred whether AI were involved or not. AI is best understood, therefore, as a potentially powerful force multiplier of these developments. Put another way, military AI, and the advanced capabilities it enables, is a natural manifestation—rather than the cause or origin—of an established trend, potentially leading states to adopt destabilizing launch postures due to the increasing speed of war and commingling.[22]

The following three case studies ground the discussion of the core themes related to AI and the risk of inadvertent escalation to illustrate how and why military AI applications fused with nonnuclear weapons might cause or exacerbate escalation risks in future warfare. They also illuminate how these AI-augmented capabilities would work and, despite the risks associated with the deployment of these systems, why militaries might deploy them nonetheless. Because military commanders are concerned with tightly controlling the rungs on the "escalation ladder," they should, in theory, be against delegating too much decision-making authority to machines—especially involving nuclear weapons.[23] Competitive pressures between great military powers and fear that others will gain the upper hand in the development and deployment of military AI (and the advanced weapon systems AI could empower) might overwhelm these concerns, however. By way of a caveat, the cases do not assume that militaries will necessarily be able to implement these augmented weapon systems in the near term. Disagreements exist among AI researchers and analysts about the significant operational challenges faced by states in the deployment of AI-augmented weapon systems.

Autonomous Weapons, Swarming, and Instability

The proliferation of a broad range of AI-augmented autonomous weapon systems (most notably drones used in swarming tactics) could have far-reaching strategic implications for nuclear security and escalation in future warfare.[24] Several observers anticipate that sophisticated AI-augmented AWSs will soon be deployed for a range of ISR and strike missions.[25] Even if AWSs are used only for conventional operations, their proliferation could nonetheless have destabilizing implications and increase the risk of inadvertent nuclear escalation. For example, AI-augmented drone swarms may be used in offensive sorties targeting ground-based air defenses and by nuclear-armed states to defend their strategic assets (i.e., launch facilities and their attendant C3I and early-warning systems), exerting pressure on a weaker nuclear-armed state to respond with nuclear weapons in a use-them-or-lose-them situation.

Recent advances in AI and autonomy have substantially increased the perceived operational value that military great powers attach to the development of a range of AWSs,[26] potentially making the delegation of lethal authority to AWSs an increasingly irresistible and destabilizing prospect.[27] That is, in an effort to defend or capture the technological upper hand in the possession of cutting-edge war-fighting assets vis-à-vis strategic rivals' traditionally conservative militaries, states may eschew the potential risks of deploying unreliable, unverified, and unsafe AWS. Today, the main risk for stability and escalation is the technical limitations of the current iteration of AI machine learning software (i.e., brittleness, explainability, unpredictability of machine learning, vulnerability to subversion or "data poisoning," and the fallibility of AI systems to biases).[28] To be sure, immature deployments of these nascent systems in a nuclear context would have severe consequences.[29]

Conceptually speaking, autonomous systems will incorporate AI technologies such as visual perception, speech, facial recognition, and decision-making tools to execute a range of core air interdiction, amphibious ground assaults, long-range strike, and maritime operations independent of human intervention and supervision.[30] Currently, only a few weapon systems select and engage their targets without human intervention. Loitering attack munitions (LAM)—also known as "loitering munitions" or "suicide drones"—pursue targets (such as enemy radars, ships, or tanks) based on preprogrammed targeting criteria and launch an attack when their sensors detect an enemy's air defense radar.[31] Compared to cruise missiles (designed to fulfill a similar function), LAMs use AI technology to shoot down incoming projectiles faster than a human operator ever could and can remain in flight (or loiter) for much longer periods. This attribute could complicate the ability of states to reliably and accurately detect and attribute autonomous attacks.[32]

A low-cost lone-wolf unmanned aerial vehicle (UAV) would, for example, not pose a significant threat to a US F-35 stealth fighter, but hundreds of AI machine learning autonomous drones in a swarming sortie may potentially evade and overwhelm an adversary's sophisticated defense capabilities—even in heavily defended regions such as China's east and coastal regions.[33] Moreover, stealth variants of these systems[34]—coupled with miniaturized electromagnetic jammers and cyberweapons—may be used to interfere with or subvert an adversary's targeting sensors and communications systems, undermining its multilayered air defenses in preparation for drone swarms and long-range stealth bomber offensive attacks.[35] In 2011, for example, MQ-1 and MQ-9 drones in the Middle East were infected with hard-to-remove malicious malware, exposing the vulnerability of US subset systems to offensive cyber.[36] This threat might, however, be countered (or mitigated) by the integration of future iterations of AI technology into stealth fighters such as the F-35.[37] Manned F-35 fighters will soon be able to leverage AI to control small drone swarms in close proximity to the aircraft performing sensing, reconnaissance, and targeting functions, including countermeasures against swarm attacks.[38] In the future, extended endurance of UAVs and support platforms could potentially increase the ability of drone swarms to survive these kinds of countermeasures.[39]

Several prominent researchers have opined that, notwithstanding the remaining technical challenges as well as the legal and ethical feasibility,[40] we can expect to see operational AWSs in a matter of years.[41] According to former US deputy secretary of defense Robert Work, the United States "will not delegate lethal authority to a machine to make a decision" in the use of military force. [42] Work adds, however, that such self-restraint could be tested if a strategic competitor (especially China and Russia) "is more willing to *delegate authority* to machines than we are and, as that competition unfolds, we'll have to make decisions on how we can best compete" (emphasis added).[43] In short, pre-delegating authority to machines, and taking human judgment further out of the crisis decision-making process, might severely challenge the safety, resilience, and credibility of nuclear weapons in future warfare.[44]

The historical record is replete with examples of near nuclear misses, demonstrating the importance of human judgment in mitigating the risk of miscalculation and misperception (i.e., of another's intentions, redlines, and willingness to use force) between adversaries during crises.[45] Despite these historical precedents, the risks associated with unpredictable AI-augmented autonomous systems operating in dynamic, complex, and possibly a priori unknown environments remain underappreciated by global defense communities.[46] Eschewing these risks, China and Russia plan to incorporate AI into unmanned aerial and undersea vehicles for swarming missions infused with AI machine learning technology.[47] Chinese strategists have reportedly researched data-link technologies for "bee swarm" UAVs, particularly emphasizing network architecture, navigation, and anti-jamming military operations for targeting US aircraft carriers.[48]

Drones used in swarms are *conceptually* well suited to conduct preemptive attacks and nuclear ISR missions against an adversary's nuclear and nonnuclear mobile missile launchers and nuclear-powered ballistic missile submarines (SSBN), along with their attendant enabling facilities (e.g., C3I and early warning systems, antennas, sensors, and air intakes).[49] The Defense Advanced Research Projects Agency (DARPA), for example, is developing an autonomous surface vehicle (ASV) double outrigger, Sea Hunter, currently being tested by the US Navy to support antisubmarine warfare operations (i.e., submarine reconnaissance).[50] Some observers have posited that autonomous systems like Sea Hunter may render the underwater domain transparent, thereby eroding the second-strike deterrence utility of stealthy SSBNs. The technical feasibility of this hypothesis is highly contested, however.[51]

On the one hand, several experts argue that deployed in large swarms, these platforms could transform antisubmarine warfare, rendering at-sea nuclear deterrence vulnerable. On the other hand, some consider such a hypothesis technically premature because (1) it is unlikely that sensors on board AWSs would be able to reliably detect deeply submerged submarines; (2) the range of these sensors (and the drones themselves) would be limited by battery power over extended ranges;[52] and (3) given the vast areas traversed by SSBNs on deterrence missions, the chance of detection is negligible even if large numbers of autonomous swarms were deployed.[53] Thus, significant advances in power, sensor technology, and communications would be needed before these autonomous systems have a game-changing strategic impact on deterrence.[54] However, irrespective of the veracity of this emerging capability, the *mere perception* that nuclear capabilities face new strategic challenges would nonetheless elicit distrust between nuclear-armed adversaries—particularly where strategic force asymmetries exist. Moreover, DARPA's Sea Hunter demonstrates how the emerging generation of autonomous weapons is expediting the completion of the iterative targeting cycle to support joint operations, thus increasing the uncertainty about the reliability and survivability of states' nuclear second-strike capability and potentially triggering use-them-or-lose-them situations.

Conceptually speaking, the most destabilizing impact of AI on nuclear deterrence would be the synthesis of autonomy with a range of machine-learning-augmented sensors, undermining states' confidence in the survival of their second-strike capabilities and in extremis triggering a retaliatory first strike.[55] Enhanced by the exponential growth in computing performance and coupled with advances in machine learning techniques that can rapidly process data in real time, AI will empower drone swarms to perform increasingly complex missions, such as hunting hitherto hidden nuclear deterrence forces.[56] In short, the ability of future iterations of AI able to predict based on the fusion of expanded and dispersed data sets and then to locate, track, and target strategic missiles such as mobile

ICBM launchers in underground silos, on board stealth aircraft, and in SSBNs is set to grow.[57]

The following four scenarios illustrate the possible strategic operations AI-augmented drone swarms would execute.[58] First, drone swarms could be deployed to conduct nuclear ISR operations to locate and track dispersed (nuclear and nonnuclear) mobile missile launchers and their attendant enabling C3I systems.[59] Specifically, swarms incorporating AI-infused ISR, autonomous sensor platforms, ATR, and data analysis systems may enhance the effectiveness and speed of sensor drones to locate mobile missiles and evade enemy defenses.

Second, swarming could enhance legacy conventional and nuclear weapons delivery systems (e.g., ICBMs and SLBMs), possibly incorporating hypersonic variants (discussed below).[60] AI applications will likely enhance the delivery system targeting and tracking and improve the survivability of drone swarms against the current generation of missile defenses.

Third, swarming tactics could bolster a state's ability to disable or suppress an adversary's defenses (e.g., air, missile, and antisubmarine warfare defenses), clearing the path for a disarming attack.[61] Drone swarms might be armed with cyber or EW capabilities (in addition to antiship, antiradiation, or regular cruise and ballistic missiles) to interfere with or destroy an adversary's early warning detection and C3I systems in advance of a broader offensive campaign.[62] Conversely, drone swarms might enhance states' missile defenses as countervails to these offensive threats. For example, swarms could form a defensive wall to absorb incoming missile salvos, intercepting them or acting as decoys to throw them off course with mounted laser technology.[63]

Finally, in the maritime domain, unmanned underwater vessels (UUV), unmanned surface vessels (USV), and UAVs supported by AI-enabled intra-swarm communication and ISR systems could be deployed simultaneously in both offensive and defensive antisubmarine warfare operations to saturate an enemy's defenses and to locate, disable, and destroy its nuclear-armed or nonnuclear attack submarines.[64] Despite continued advances in sensor technology design (e.g., reduced size and extended detection ranges) to overcome quieting challenges, other technical challenges still remain. These include communicating underwater between multiple systems, processing power requirements, generating battery life and energy, and scaling the system.[65]

While some experts do not expect a technically reliable and effective capability of this kind will be operational for at least a decade, others are more optimistic.[66] From a tactical perspective, drone swarms would not need ocean-wide coverage (or full ocean transparency) to effectively detect and track submarines. According to UK rear admiral John Gower, a relatively even spread of sensors might be sufficient to enable "a *viable search and detection plan* . . . conceived for the open ocean" (emphasis added).[67] Moreover, advances in mobile sensing platforms could enable drones in swarms to locate submarines through chokepoints (or gateways) as they emerge from ports. Due to the current slowness of drones with extended sea ranges, however, trailing them autonomously seems implausible.[68] Future iterations of machine-learning-augmented UUVs and USVs may eventually complement, and perhaps replace entirely, the traditional role of general-purpose nuclear-powered submarines (SSN) and manned surface vehicles in tracking and trailing submarines of adversaries at chokepoints while simultaneously mounting sparsely distributed and mobile distributed network systems (DNS) sensors on UUVs.[69]

If a state views the credibility of its survivable nuclear weapons (especially nuclear-armed submarines) to be at risk,[70] conventional capabilities such as drone swarms will likely have a destabilizing effect at a strategic level.[71] Thus, even if swarm sorties were not intended as (or indeed technically capable of) a disarming first strike, the perception alone of the feasibility of such an operation would be destabilizing nonetheless. Moreover, the speed of AI could put the defender at a distinct disadvantage, creating additional incentives to strike first (or preemptively) technologically superior military rivals. Consequently, the less secure a nation considers its second-strike capabilities to be, the more likely it is to countenance the use of autonomous systems within its nuclear weapons complex to bolster the survivability of its strategic forces. According to analyst Paul Scharre, "winning in swarm combat may depend upon having the best algorithms to enable better coordination and *faster reaction times*, rather than simply the best platforms" (emphasis added).[72]

Combining speed, persistence, scope, coordination, and battlefield mass, AWSs will offer states attractive asymmetric options to project military power within contested A2/AD zones.[73] Enhanced by sophisticated machine learning neural networks, China's manned and unmanned drone teaming operations could potentially impede future US freedom of navigation operations in the South China Seas.[74] Its air- and sea-based drones linked to sophisticated neural networks could, for example, support the People's Liberation Army's manned and unmanned teaming operations. Were China to infuse its cruise missiles and hypersonic glide capabilities with AI and autonomy, close-range encounters in the Taiwan Straits and the East and South China Seas would become more complicated, accident-prone, and destabilizing—at both a conventional and nuclear level.[75] China is reportedly developing and deploying UUVs to bolster its underwater monitoring and antisubmarine capabilities as part of a broader goal to establish an "underwater Great Wall" to challenge US undersea military primacy. US AI-enhanced UUVs could, for example, theoretically threaten China's nuclear ballistic and nonnuclear attack submarines.[76]

The deployment of new military technology in the nuclear domain, therefore, affects states differently depending on the relative strength of their strategic force structure. Thus, even if US UUVs were programmed only to threaten China's nonnuclear attack fleets, Chinese commanders might nonetheless fear that their country's nascent and relatively small—compared to US and Russian SSBN fleets—sea-based nuclear deterrent could be neutralized more easily.[77] Moreover, advances in machine learning sensor technology for enabling more accurate detection of Chinese SSBNs would likely reinforce Beijing's concerns that it was being targeted by a militarily superior power—especially the United States. To test the veracity of this scenario, a better understanding of Chinese thinking on the utility of its nuclear and nonnuclear capabilities—and how it could inform China's attitude to escalation risk—would be required.

Perceived as a relatively low-risk force majeure with ambiguous rules of engagement, and absent a robust normative and legal framework, autonomous weapons will likely become an increasingly attractive asymmetric to erode a militarily superior adversary's deterrence and resolve.[78] In sum, notwithstanding the remaining technical challenges (especially the demand for power), swarms of robotic systems fused with AI machine learning techniques may presage a powerful interplay of increased range, accuracy, mass, coordination, intelligence, and speed in a future conflict.[79]

Hypersonic Boost-Glide Technology and Missile Defense

Multiple advanced nonnuclear weapons could potentially threaten a wide range of strategic targets. In particular, technological advances in hypersonic boost-glide weapons—especially deployed in conjunction with cruise missiles, missile defense capabilities, and drone swarm support—could target an adversary's high-value assets such as radars, antisatellite weapons, mobile missile launchers, C3I systems, and transporter-erector-launchers (TEL) used to undergird both nuclear and conventional missiles. In the future, swarms of AI-augmented UAVs could be used to locate and track dispersed targets such as mobile missile launchers and suppress enemy air defenses, clearing the path for swarms of hypersonic autonomous delivery systems armed with conventional or nuclear payloads.[80] The development and deployment of offensive-dominant weapons such as hypersonic boost-glide weapons,[81] capable of threatening dual-use targets, could eventually exacerbate the problem of target ambiguity, increase the risks of inadvertent escalation, and, in turn, lower the nuclear threshold.[82]

It is noteworthy that Chinese, US, and Russian doctrinal texts share a common view of the potential utility of conventional hypersonic weapons to put at risk targets that hitherto only nuclear weapons could threaten, thereby bolstering strategic deterrence.[83] Moreover, in a future conflict between the US and China or the US and Russia, all sides would have strong incentives to attack the others' dual-use C3I and ISR capabilities early on and preemptively.[84] Chinese analysts view hypersonic cruise missiles, for example, as an effective means to enhance China's nuclear deterrence posture, penetrate US missile defenses, and preempt hypersonic (notably the X-37 unmanned spacecraft) scenarios.[85]

The maneuverability of hypersonic weapons could compound these dynamics, adding destination ambiguity to the destabilizing mix. In contrast to ballistic missiles, the unpredictable trajectories of hypersonic weapons will make using this weapon for signaling intent highly problematic and potentially escalatory. Furthermore, the challenge of determining an attacker's intentions would be complicated if an adversary's dual-use ISR, early warning, or C3I systems were targeted early on in a conflict. Adversaries unable to ascertain the intended path or ultimate target of a bolt-from-the-blue hypersonic strike will likely assume the worst (i.e., it was in a use-it-or-lose-it situation), inadvertently escalating a situation intended initially only to signal intent. Against the backdrop of geopolitical competition and uncertainty, the reciprocal fear of surprise attack will likely heighten the risk of miscalculation, with potentially escalatory implications.[86]

For example, if China's early warning systems detected a hypersonic weapon launched from the US, Beijing would not be sure whether China was the intended target ("destination ambiguity"). Even if it became clear that China was the intended target, Beijing would still not know what assets the US intended to destroy ("target ambiguity") or whether the weapon was nuclear or conventionally armed ("warhead ambiguity"). China's AI-augmented—and likely dual-use—early warning systems would be a mixed blessing for strategic stability, however. Perhaps Beijing's confidence in the survivability of its nuclear forces could have a stabilizing effect. Then again, allowing China to detect an incoming weapon much earlier in a conflict might exacerbate warhead and target ambiguity, thus generating inadvertent escalatory risks. If China made improvements to its missile early warning system in preparation for the adoption of a launch-under-attack nuclear posture (like Russia and the United States), then the early detection of a US boost-guide attack would become even more critical.[87]

According to analyst James Acton, enabling capabilities are critical for the successful employment of hypersonic weapons.[88] In particular, military operations that require rapid decision-making (i.e., to locate, track, and accurately execute an attack) will generally place higher demands on enabling capabilities to plan and execute a strike (especially ISR) than preemptive or surprise attacks. To date, however, command and control, ISR, intelligence collation and analysis, and battle damage assessment remain undeveloped, lagging the progress made in hypersonic weapon technology.[89] AI technology is expected to accelerate progress for hypersonic weapons and other long-range (conventional and nuclear-armed) precision munitions in all of these critical enabling capabilities:[90] (1) autonomous navigation and advanced vision-based guidance systems,[91] (2) ISR systems for targeting and tracking (especially mobile) targets, (3) missile release and sensor systems, (4) AI machine learning systems to decipher patterns from large data sets to support intelligence analysis for identifying and tracking targets,[92] (5) pattern interpretation to cue decision support systems for enabling "fire and forget" missiles,[93] and (6) escalation prediction.[94] For example, several states (notably China and Russia) are developing machine learning approaches to build control systems for hypersonic glide vehicles (HGV), which because of their high velocity cannot be operated manually.

These autonomous variants could also enhance hypersonic missile defenses, strengthening their resilience against countermeasures such as jamming and spoofing.[95] Conceptually, within a matter of minutes, AI machine learning systems can generate a hypersonic flight plan for human review and approval, and in real-time, self-correct a missile in flight to compensate for unexpected flight conditions or a change in the target's location.[96] Theoretically, this AI augmentation would enable swarms of hypersonic autonomous delivery systems to circumvent some of the remaining technical challenges that militaries face in tracking and targeting an adversary's mobile missile forces. Specifically, it would allow tracking a moving target and communicating this information back to commanders in real time, and then cueing a rapid surprise or preemptive attack *before* the mobile launchers can be relocated.[97]

A large volume of Chinese open sources reveals prolific indigenous research into the integration of AI-powered machine learning techniques, especially deep neural networks, to address the technical challenges associated with the high-speed and heat-intensive reentry dynamics of hypersonic weapons (i.e., heat control, maneuverability, stability, and targeting).[98] Particularly, Chinese analysts anticipate that AI will resolve many of the intractable issues associated with hypersonic glide vehicles' high flight envelope, including complex flight environments, severe nonlinearity, intense and rapid time variance, and the dynamic uncertainty during the dive phase of the delivery. They broadly concur with their Western counterparts that much like other AI-augmented strategic nonnuclear capabilities (i.e., drone swarms, cyber and EW capabilities, missile defense, and antisubmarine capabilities), hypersonic weapons—by increasing the speed of warfare—are inherently destabilizing.

Chinese efforts to apply AI machine learning techniques to enhance hypersonic weapons can be understood as part of a broader strategic goal of developing "intelligent" autonomous weapons, and their enabling systems, for the future multidimensional and multidomain battlefield environment.[99] Because of the many intersections AI-enhanced hypersonic weapons could have with nuclear security (especially the penetration of US missile defenses), together with the strong likelihood Chinese hypersonic weapons will carry dual payloads,[100] an appreciation of the interaction between these capabilities and implications for nuclear, conventional, and cross-domain deterrence will be a critical task for analysts and policy makers.[101] Similar to the cyber capabilities, AWSs, and other advanced automated weapon systems that AI could empower, hypersonic weapons could significantly accelerate the pace of conflict and compress the decision-making time frame. In sum, as a powerful enabler and force multiplier, AI could disrupt information flows and effective communication (both between adversaries and allies and within military organizations) and, consequently, complicate escalation management during future crisis or conflict—especially involving China and the United States.[102] Furthermore, the disruption of communications might also undermine nuclear deterrence and therefore increase the odds of brinkmanship and incentives to act first and preemptively during a crisis.

Conclusion

A new generation of AI-augmented advanced conventional capabilities will exacerbate the risk of inadvertent escalation caused by the commingling of nuclear and strategic nonnuclear weapons (or conventional counterforce weapons) and the increasing speed of warfare, thereby undermining strategic stability and increasing the risk of nuclear confrontation. This conclusion is grounded in the overarching findings that relate to *how* and *why* AI could affect strategic stability between great military powers— especially China and the United States.

If a state perceives that the survivability of its nuclear forces were at risk, advanced conventional capabilities (e.g., autonomous drone swarms and hypersonic weapons) augmented with AI machine learning techniques will have a destabilizing impact at a strategic level of conflict. AI's effect on strategic stability will likely be determined by states' perceptions of its operational utility rather than actual capability. If an adversary underestimated the potential threat posed by nascent and especially poorly conceptualized accident-prone autonomous systems, the consequences would be severely destabilizing.

Despite the speed, diverse data pools, and processing power of algorithms compared to humans, complex AI-augmented systems will still depend on the assumptions encoded into them by human engineers to simply extrapolate inferences—potentially erroneous or biased—from complexity, resulting in unintended outcomes. One of the most significant escalatory risks caused by AI is likely to be, therefore, the perceived pressure exerted on nuclear powers in the use of AI-augmented conventional capabilities to adopt unstable nuclear postures (such as launch on warning, rescinding no-first-use pledges, or nuclear war fighting), or even to exercise a preemptive first nuclear strike during a crisis. In extremis, human commanders might lose control of the outbreak, course, and termination of warfare.

Further, a competitive and contested multipolar nuclear environment will likely exacerbate the potentially destabilizing influence of AI, increasing that risk of inadvertent escalation to a nuclear level of conflict between great military powers. In today's multipolar geopolitical order, therefore, relatively low-risk and low-cost AI-augmented AWS capability—with ambiguous rules of engagement and absent a robust normative and legal framework—will become an increasingly enticing asymmetric option to erode an advanced military's deterrence and resolve. By disrupting effective and reliable flows of information and communication between adversaries and allies and within military organizations, AI-augmented conventional weapon systems (i.e., C3I, early warning systems, and ISR) could complicate escalation management during future crisis or conflict—especially involving China and the United States.

A prominent theme that runs through the scenarios in this article—and central to understanding the potential impact of AI for strategic stability and nuclear security—is the concern that AI systems operating at machine speed will push the pace of combat to a point where machine actions surpass the cognitive and physical ability of human decision-makers to control or even comprehend events. Effective deterrence depends on the clear communication of credible threats and consequence of violation between adversaries, which assumes the sender and recipient of these signals share a common context allowing for mutual interpretation.[103]

For now, it remains axiomatic that human decisions escalate a situation; however, military technology like AI that enables offensive capabilities to operate at higher speed, range, and lethality will move a situation more quickly up the escalation rungs, crossing thresholds that can lead to a strategic level of conflict. These escalatory dynamics would be greatly amplified by the development and deployment of AI-augmented tools functioning at machine speed. Military AI could potentially push the pace of combat to a point where the actions of machines surpass the cognitive and physical ability of human decision-makers to control (or even fully understand) future warfare. Thus, until experts can unravel some of the unpredictable, brittle, inflexible, unexplainable features of AI, this technology will continue to outpace strategy, and human error and machine error will likely compound one another—with erratic and unintended effects.

James S. Johnson

Dr. James Johnson is a postdoctoral research fellow at the James Martin Center for Nonproliferation Studies (CNS) at the Middlebury Institute of International Studies, Monterey. He holds a PhD in politics and international relations from the University of Leicester, where he is also an honorary visiting fellow with the School of History and International Relations. Dr. Johnson is fluent in Mandarin and has published widely in the fields of security and strategic studies, Sino-American security relations, nuclear nonproliferation and arms control, emerging technology (especially AI), Chinese foreign policy, and East Asian security. He is the author of *The US-China Military and Defense Relationship during the Obama Presidency* (Palgrave Macmillan, 2018). His latest book project is entitled *Artificial Intelligence and the Future of Warfare: USA, China, and Strategic Stability*.

Notes

1. Recent progress in AI falls into two distinct fields: (1) "narrow" AI and specifically machine learning and (2) "general" AI, which refers to AI with the scale and fluidity akin to the human brain. Narrow AI is already used in the private sector, particularly in data-rich research fields and applied sciences (e.g., predictive analytics for market research, consumer behavior, logistics, and quality control systems). The distinction between narrow and general AI might, however, be less of an absolute, or binary, measure than one of degree. Breakthroughs in narrow AI have generally led to speculation on the arrival of artificial general intelligence. Most experts agree, however, that the development of general AI is at least several decades away, if at all. Stuart Armstrong, Kaj Sotala, and Seán S. ÓhÉigeartaigh, "The Errors, Insights and Lessons of Famous AI Predictions—and What They Mean for the Future," *Journal of Experimental and Theoretical Artificial Intelligence* 26, no. 3 (2014): 317–42, DOI: 10.1080/0952813X.2014.895105.

[2] "Entanglement" in this context 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. "Strategic stability" as a concept in political science has been defined in many ways. Colby Elbridge and Michael Gerson, eds., *Strategic Stability: Contending Interpretations* (Carlisle, PA: Army War College, 2013), https://publications.armywarcollege.edu/.

[3] Military-use AI, and the advanced capabilities it enables, can be conceptualized as a natural manifestation (rather than the cause or origin) of an established trend in emerging technology toward commingling and increasing the speed of warfare, which could lead states to adopt destabilizing launch postures. Hans M. Kristensen, Matthew McKinzie, and Theodore A. Postol, "How US Nuclear Force Modernization Is Undermining Strategic Stability: The Burst-Height Compensating Super-Fuze," *Bulletin of the Atomic Scientists*, 1 March 2017, https://thebulletin.org/.

[4] "Inadvertent escalation" refers to a situation where one state takes an action that it does not believe the other side will (or should) regard as escalatory but occurs *unintentionally* nonetheless. See Barry R. Posen, *Inadvertent Escalation: Conventional War and Nuclear Risks* (Ithaca, NY: Cornell University Press, 1991); Forrest E. Morgan et al., *Dangerous Thresholds: Managing Escalation in the 21st Century* (Santa Monica, CA: RAND Corporation, 2008), https://www.rand.org/; and Lawrence Freedman, *Evolution of Nuclear Strategy*, 3rd ed. (London: Palgrave Macmillan, 2003), especially chap. 14.

[5] Notable exceptions include Vincent Boulanin, ed., *The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk*, vol. I, *Euro-Atlantic Perspectives* (Stockholm: SIPRI Publications, May 2019), https://www.sipri.org/; Edward Geist and Andrew J. Lohn, *How Might Artificial Intelligence Affect the Risk of Nuclear War?* (Santa Monica, CA: RAND Corporation, 2018), https://www.rand.org/; Kareem Ayoub and Kenneth Payne, "Strategy in the Age of Artificial Intelligence," *Journal of Strategic Studies* 39, nos. 5–6 (2016): 793–819, DOI: 10.1080/01402390.2015.1088838; Technology for Global Security (T4GS) and the Center for Global Security Research (CGSR), "AI and the Military: Forever Altering Strategic Stability," T4GS Reports, 13 February 2019, https://www.tech4gs.org/; Jürgen Altmann and Frank Sauer, "Autonomous Weapon Systems and Strategic Stability," *Survival* 59, no. 5 (2017): 121–27, DOI: 10.1080/00396338.2017.1375263; and James S. Johnson, "Artificial Intelligence and Future Warfare: Implications for International Security," *Defense and Security Analysis* 35, no. 2: 147–69, DOI: 10.1080/14751798.2019.1600800.

[6] Thomas J. Christensen, "The Meaning of the Nuclear Evolution: China's Strategic Modernization and U.S.-China Security Relations," *Journal of Strategic Studies* 35, no. 4 (August 2012): 467–71; and Fiona S. Cunningham and M. Taylor Fravel, "Assuring Assured Retaliation: China's Nuclear Posture and U.S.-China Strategic Stability," *International Security* 40, no. 2 (Fall 2015): 40–45, https://www.belfercenter.org/.

[7] Examples of strategic capabilities include kinetic long-range nuclear and conventional munitions (e.g., ICBMs), long-range penetrating bombers, and shorter-range tactical (or theater) weapons that are or can be forward deployed. A range of technologically advanced (offensive and defensive) nonnuclear (kinetic and nonkinetic) weapons designed to reduce the vulnerability of states to nuclear attack can also have strategic effects. For example, offensive cyber and counterspace (i.e., ASATs) have recently emerged as strategic capabilities. Defense systems (e.g., ballistic missile defense systems)

can also be viewed as strategic in as much as they are intended (or able) to impair the ability of a state to respond at a strategic level.

8. The author acknowledges that new military terms or concepts do not necessarily represent operational or deployable capabilities.

9. For the impact of AI and machine learning technology on the cyber (nonkinetic) domain, see James S. Johnson, "The AI-Cyber Nexus: Implications for Military Escalation, Deterrence, and Strategic Stability," *Journal of Cyber Policy* 4, no. 3 (2019): 442–60, DOI: 10.1080/23738871.2019.1701693.

10. See James S. Johnson, "Artificial Intelligence and Future Warfare: Implications for International Security," *Defense and Security Analysis* 35, no. 2 (2019): 147–69, DOI: 10.1080/14751798.2019.1600800.

11. Edward Geist and Andrew J. Lohn, *How Might Artificial Intelligence Affect the Risk of Nuclear War?* (Santa Monica, CA: RAND Corporation, 2018), https://www.rand.org/; and Ayoub and Payne, "Strategy in the Age of Artificial Intelligence," 799–819.

12. The DOD has long recognized these kinds of concerns. For example, the Air Force's Tacit Rainbow anti-radiation missile program, which incorporated elements of unmanned aerial vehicles (UAV) and cruise missiles, was canceled in 1991 in large part because of the risk of error posed by autonomous systems used in offensive missions.

13. The line between core AI and "AI-related" technology is a blurred one. For the purposes of this article, core AI technology includes machine learning (and deep learning and deep networks subset), modelling, automated language and image recognition, voice assistants, and analysis support systems. Also, AI-related (and AI-enabling) technology includes autonomous vehicles, big data analytics, 5G networks, supercomputers, smart vehicles, smart wearable devices, robotics, and the Internet of Things, to name a few.

14. "Autonomy" in the context of military applications can be defined as the condition or quality of being self-governing to achieve an assigned task based on a system's own situational awareness (integrated sensing, perceiving, and analyzing), planning, and decision-making. That is, autonomy is fundamentally a software endeavor. Software (i.e., AI machine learning techniques for sensing, modeling, and decision-making) rather than hardware separates existing armed unmanned and remote-controlled weapon systems (e.g., the US MQ-9 Reaper, the Israeli Guardium, and the Russian Platform-M). A distinction is often made between automatic, automated, and autonomous systems, although these terms are sometimes used interchangeably. For the purposes of this article, it is necessary to acknowledge that this debate exists. See Department of Defense Directive (DODD) 3000.09, *Autonomy in Weapon Systems*, 21 November 2012, https://fas.org/.

15. For example, AI is enabling scientists to model nuclear effects to confirm the reliability of nuclear stockpiles without nuclear testing.

16. For example, the US National Geospatial Intelligence Agency has reportedly used AI to support military and intelligence analysis.

17. A recent Stockholm International Peace Research Institute (SIPRI) report found that autonomy is used in at least 56 military systems to collect and process various types of information, especially related to targeting and command and control. Vincent Boulanin and Maaike Verbruggen, *Mapping the Development of Autonomy in Weapon Systems* (Stockholm, Sweden: SIPRI, 2017), 28, https://www.sipri.org/.

18. Since the 1970s, air defense systems have been using an AI technology to augment automatic target recognition to detect, track, prioritize, and select incoming air threats.

[19] Daniel S. Hoadley and Nathan J. Lucas, *Artificial Intelligence and National Security* (Washington, DC: Congressional Research Service, 2018), https://kr.usembassy.gov/.

[20] Langdon Winner, *Autonomous Technology: Technics-out-of-Control as a Theme in Political Thought* (Cambridge, MA: MIT Press, 1977), https://ratical.org/.

[21] Lieber A. Keir and Daryl G. Press, "The New Era of Counterforce: Technological Change and the Future of Nuclear Deterrence," *International Security* 41, no. 4 (2017): 9–49; and Kenneth Payne, "Artificial Intelligence: A Revolution in Strategic Affairs?," *Survival* 60, no. 5 (2018): 7–32, DOI: 10.1080/00396338.2018.1518374.

[22] Kristensen, McKinzie, and Postol, "Nuclear Force Modernization."

[23] Herman Kahn, *On Escalation: Metaphors and Scenarios* (New York: Praeger, 1965).

[24] Recent studies generally agree that AI machine learning systems are an essential ingredient to enable fully autonomous systems. See Stuart Russell and Peter Norvig, *Artificial Intelligence: A Modern Approach*, 3rd ed. (Harlow, Essex: Pearson Education, 2014), 56; and Michael Horowitz, Paul Scharre, and Alex Velez-Green, *A Stable Nuclear Future? The Impact of Automation, Autonomy, and Artificial Intelligence* (Philadelphia: University of Pennsylvania, 2017).

[25] See Robert J. Bunker, *Terrorist and Insurgent Unmanned Aerial Vehicles: Use, Potentials, and Military Applications* (Carlisle, PA: Strategic Studies Institute and US Army War College Press, 2015), https://www.hsdl.org/; Zachary Kallenborn and Philipp C. Bleek, "Swarming Destruction: Drone Swarms and Chemical, Biological, Radiological, and Nuclear Weapons," *The Nonproliferation Review* 25, nos. 5–6 (2018): 523–43, DOI: 10.1080/10736700.2018.1546902; and Bryan Clark, *The Emerging Era in Undersea Warfare* (Washington, DC: Center for Strategic and Budgetary Analysis, 2015), https://csbaonline.org/.

[26] AI and autonomy—together with automatic and automated—are often used interchangeably. Autonomous systems are best understood as a key subset of AI technologies—especially machine learning.

[27] To date, no state has formally declared an intention to build entirely autonomous weapon systems. Currently, only the United States, the United Kingdom, and Israel have used armed drones operationally.

[28] Machine learning is a concept that encompasses a wide variety of techniques designed to identify patterns in and also "learn" and make predictions from data sets. Successful learning depends on having access to vast pools of reliable data about past behavior and successful outcomes. The "neural network" approach to AI represents only a small segment of the improvements in AI techniques. AI also includes, for example, language processing, knowledge representation, and inferential reasoning, which are being actualized by the rapid advancements in software, hardware, data collection, and data storage. Jürgen Schmidhuber, "Deep Learning in Neural Networks: An Overview," *Neural Networks* 61 (2015): 85–117, http://www2.econ.iastate.edu/.

[29] Will Knight and Karen Hao, "Never Mind Killer Robots—Here Are Six Real AI Dangers to Watch out for in 2019," *MIT Technology Review*, 7 January 2019, https://www.technologyreview.com/.

[30] The US DOD has developed directives restricting development and use of systems with particular autonomous capabilities; "humans" must be kept in the loop and directly make the decisions for all applications of lethal force.

31. LAMs are hybrid offensive capabilities between guided munitions and unmanned combat aerial systems. To date, the only known operational LAM is Israel's Harop (or Harpy 2), combining a human-in-the-loop and fully autonomous mode.

32. For example, the terrorist group ISIS used remotely controlled aerial drones in its military operations in Iraq and Syria. Ben Watson, "The Drones of ISIS," *Defense One*, 12 January 2017, https://www.defenseone.com/.

33. There are instances when a lone-wolf drone can pose a serious threat to an F-35; a single drone can destroy an F-35 on the ground. For example, an unmanned aerial system could be employed to place spike strips on a runway to deflate aircraft tires, deliver debris to damage jet engines, drop explosives on other targets, or even in a Kamikaze role during the critical takeoff or landing phases of flight, increasing the chances of damage or a catastrophic crash. Thomas S. Palmer and John P. Geis, "Defeating Small Civilian Unmanned Aerial Systems to Maintain Air Superiority," *Air and Space Power Journal* 31, no. 2 (Summer 2017): 105, https://www.airuniversity.af.edu/.

34. China, the United States, the United Kingdom, and France have developed and tested stealthy UAV prototypes.

35. The Russian military, for example, reportedly deployed jammers to disrupt GPS-guided unmanned air vehicles in combat zones including Syria and Eastern Ukraine.

36. Noah Shachtman, "Computer Virus Hits US Drone Fleet," *Wired,* 7 October 2011, https://www.wired.com/

37. AI-infused algorithms able to integrate sensor information, consolidate targeting, automate maintenance, and merge navigation and sensor information are currently being developed and tested to anticipate the kinds of high-intensity future threat environments posed by drone swarming.

38. Currently, small drone technology does not enable drones to fly at speeds where they could be, or remain, in close proximity to the aircraft. Most existing concepts involve either medium-sized (e.g., MQ-9) drones acting as wingmen to a fighter jet (e.g., F-35), and thus in close proximity, or small drones released as a payload that does not remain in close proximity to the fighter, with little to no guidance from the mother ship. The author thanks the anonymous reviewer for making this point.

39. A combination of restrictions outlined in DODD 3000.09, *Autonomy in Weapons Systems*, as well as the cultural and bureaucratic norms and practices in the US armed services, will likely stymie efforts to incorporate AI-enabled systems. This will particularly apply in situations where the demand increases for manpower skilled in fields such as computer science (especially AI machine learning), engineering, and the sciences.

40. While recent breakthroughs in AI have made possible the automation of several tasks previously considered complex (e.g., dependable vehicle control and air traffic control), there remain technical limits on what computers and robots can achieve autonomously. Boulanin, *Impact of Artificial Intelligence*, vol. 1, chap. 3.

41. The moral and ethical considerations related to the use of autonomous control weapons and autonomous targeting are complex and highly contested; humans creating technology to attack a human is inherently problematic.

42. "WATCH: David Ignatius and Pentagon's Robert Work on the Latest Tools in Defense," *Washington Post Live* (blog), 30 March 2016, https://www.washingtonpost.com/.

43. "WATCH: David Ignatius and Pentagon's Robert Work," video. Kalashnikov, a Russian defense contractor, has reportedly built an unmanned ground vehicle (the

Soratnik) and plans to develop a broad range of autonomous systems infused with sophisticated AI machine learning algorithms.

44. UAVs used in swarming operations do not necessarily need to be "fully autonomous"; humans could still decide to execute a lethal attack.

45. Patricia Lewis et al., *Too Close for Comfort: Cases of Near Nuclear Use and Options for Policy* (London: Chatham House, Royal Institute of International Affairs, 2014), https://www.chathamhouse.org/.

46. Modeling interactions with other agents (especially humans) in either a competitive or a collaborative context is inherently problematic because human behavior is often unpredictable. Andrew Ilachinski, *AI, Robots, and Swarms: Issues, Questions, and Recommended Studies* (Arlington, VA: Center for Naval Analyses, January 2017), xv, https://www.cna.org/.

47. This Russian unmanned submarine is known by the Pentagon as "Kanyon"; its onboard nuclear warheads are considered capable of destroying ports and cities.

48. Elsa B. Kania, *Battlefield Singularity: Artificial Intelligence, Military Revolution, and China's Future Military Power* (Washington, DC: Center for a New American Security, DC: November 2017), 23, https://s3.amazonaws.com/.

49. Currently, the types of airborne drones that militaries are considering using in swarms are small and thus limited in range. Supplying sufficient power for swarms of UAVs or unmanned underwater vessels (UUV) for extended periods would require significant improvements in battery technology, air-independent propulsion, or fuel-cell technology. Further, many states' nuclear-related facilities (except the SSBNs) are located well inland, which (for now) makes drones ill-suited to attack these targets unless lifted in by a different platform. Electric storage battery power capacity is, however, rapidly improving, and experts predict a tenfold increase in power and endurance within the next decade. Leslie F. Hauck and John P. Geis II, "Air Mines: Countering the Drone Threat to Aircraft," *Air and Space Power Journal* 31, no. 1 (Spring 2017): 26–40, https://www.airuniversity.af.edu/.

50. Joseph Trevithick, "Navy's Sea Hunter Drone Ship Has Sailed Autonomously to Hawaii and Back amid Talk of New Roles," *The Drive*, 4 February 2019, https://www.thedrive.com/.

51. While there are a number of technologies under development specifically designed to track SSBMs (e.g., the DOD's Sea Hunter, a prototype autonomous surface vehicle), these programs remain immature.

52. Unlike standard UUVs that are typically tethered and have a very short range, underwater gliders (e.g., US Liquid Robotics Wave Rider SV3), while slow, can roam over long distances for months at a time.

53. Jonathan Gates, "Is the SSBN Deterrent Vulnerable to Autonomous Drones?," *The RUSI Journal* 161, no. 6 (2016): 28–35, DOI: 10.1080/03071847.2016.1265834.

54. Drones (including UAVs, UUVs, and unmanned surface vessels or USVs) might nonetheless have a significant qualitative impact on antisubmarine warfare. For example, drone swarms deployed to chokepoints (or gateways) or to an adversary's docking exit routes could act as a layered physical barrier, deterring or denying an opponent's submarine the ability to operate in certain military zones (i.e., A2/AD zones).

55. Given the current limits on drone range (i.e., battery power) and limited payload, it is unlikely that drone technology will mature sufficiently to represent a credible threat to states' nuclear assets (or other hardened targets) in the near term (i.e., within five

years)—unless, for example, UAVs are able to infiltrate hardened targets via an air duct or other like passage.

56. Tom Simonite, "Moore's Law Is Dead. Now What?," *MIT Technology Review*, 13 May 2016, https://www.technologyreview.com/. In addition to UAVs, emerging space technologies will soon enable drone-like surveillance from space incorporating similar machine learning techniques. Larger satellite constellations coupled with smaller individual satellites are expected to provide continuous coverage over large geographical ranges.

57. Elias Groll, "How AI Could Destabilize Nuclear Deterrence," *Foreign Policy*, 24 April 2018, https://foreignpolicy.com/.

58. The value of AWSs in these scenarios does not mean that they are the only or necessarily most effective way to fulfill these missions. Gates, "Is the SSBN Deterrent Vulnerable?," 28–35.

59. In 2011, students at the Massachusetts Institute of Technology presented the fully autonomous, fixed-wing Perdix UAV capable of between-drone communication at the 2011 Air Vehicle Survivability Workshop. In addition to the US, Russia, South Korea, and China are also actively pursuing drone swarm technology programs. Kallenborn and Bleek, "Swarming Destruction," 1–2.

60. At least two nuclear-armed states are considering the possibility of using UAVs or UUVs for nuclear delivery. Russia, in 2015, revealed the development of a large nuclear-armed UUV, Poseidon (also known as Status-6). The US is also developing a nuclear-capable long-range bomber, the B-21 Raider, that could potentially be used to operate remotely while carrying nuclear payloads. Other unmanned combat aerial vehicle (UCAV) prototypes (e.g., Northrop Grumman X47B, the Dassault nEUROn, and the BAE Systems Taranis) could also feasibly be used in nuclear attacks. Boulanin, *Impact of Artificial Intelligence*, vol. 1, 56–57.

61. Mike Pietrucha, "The Need for SEAD Part 1: The Nature of SEAD," *War on the Rocks*, 17 May 2016, https://warontherocks.com/.

62. Polat Cevik et al., "The Small and Silent Force Multiplier: A Swarm UAV-Electronic Attack," *Journal of Intelligent and Robotic Systems* 70 (April 2013): 595–608, https://doi.org/10.1007/s10846-012-9698-1.

63. While the Missile Defense Agency (MDA) is developing lasers for drones, the size of a drone needed to power a laser of meaningful power would be very large. The likelihood, therefore, we will see lasers on drones in the near term is considered low. The MDA estimates that the first prototype laser for a fighter-sized platform will likely be completed in approximately two years. The US MDA recently requested a significant budget to develop a drone-mounted laser program. Jen Judson, "MDA Awards Contracts for a Drone-Based Laser Design," *Defense News*, 11 December 2017, https://www.defensenews.com/.

64. The US Defense Advanced Research Projects Agency (DARPA) is currently developing an antisubmarine warfare continuous trail unmanned vehicle capability, the Anti-Submarine Warfare Continuous Trail Unmanned Vessel (ACTUV) program, to track quiet diesel-electric submarines with USVs from the surface.

65. Unmanned drone platforms are capable of carrying several types of sensors, and the swarming machine-learning systems to control them are either available today or in advanced stages of development. These sensors include active and passive sonar, magnetic anomaly detectors (MAD), light detection and ranging (LIDAR) for wake detection, thermal sensors, and laser-based optical sensors capable of piercing seawater.

66. Sebastian Brixey-Williams, "Will the Atlantic Become Transparent?," 2nd ed., *British Pugwash*, November 2016, 2–6, https://britishpugwash.org/.

67. John Gower, "Concerning SSBN Vulnerability—Recent Papers," British American Security Information Council (BASIC), *Analysis* (blog), 10 June 2016, https://basicint.org/.

68. It might be possible for a handoff to occur between drones in a grid to monitor a submarine as it moves, but doing so in extended ranges and duration would be cumbersome and slow.

69. To date, the US Navy has deployed and tested DNSs in littoral waters. For example, PLUSNet (persistent littoral undersea surveillance network) is a joint project between the US Navy's Office of Naval Research (ONR) and DARPA that began in 2005.

70. Whether autonomous underwater vehicles involved in a future swarm attack on a nuclear-armed submarine were armed or programmed merely to track and monitor a submarine, the destabilizing effects on deterrence would likely be similar. Altmann and Sauer, "Autonomous Weapon Systems," 131.

71. In an asymmetric encounter involving adversaries who do not possess AWS capabilities, the escalatory cycles described above would unlikely occur. Sauer, 132.

72. Paul Scharre, "Counter-Swarm: A Guide to Defeating Robotic Swarms," *War on the Rocks*, 31 March 2015, https://warontherocks.com/.

73. China's military has incorporated a range of advanced UAVs into all four services of its force structure.

74. In early 2018, China began construction of the world's largest test site for unmanned UAVs for war and peacetime surveillance operations in the South China Sea. For example, the Haiyi (or "Sea Wing") UUV glider has been used in several scientific missions in the South China Sea. "Sea Wing Series of Underwater Gliders Achieves the Largest Model of Swarms Simultaneously Observing," Shenyang Institute of Automation, 24 August 2017.

75. Reports indicate that China is engaged in the development of several potentially destabilizing capabilities including research into the use of AI and autonomy in prompt and high-precision (cruise and ballistic) missile systems, space planes, and a variety of hypersonic boost-glide variants. Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China, 2019* (Washington, DC: Department of Defense, 2019), https://media.defense.gov/.

76. A range of autonomous ground and underwater vehicles is already in development globally with varying degrees of success.

77. Chinese reports from the 2016 seizure of a US UUV indicate that this action was taken because of the perceived threat to Chinese SSBNs in the region.

78. Paul Scharre, *Autonomous Weapons and Operational Risk: Ethical Autonomy Project* (Washington, DC: Center for a New American Security, February 2016), https://s3.amazonaws.com/.

79. Supplying sufficient power for swarms of UAVs (or UUVs) for an extended period would require significant improvements in either battery technology, air-independent propulsion, or fuel cell technology. It may also require the development of some form of energy storage mechanism that has yet to be envisaged. Gates, "Is the SSBN Deterrent Vulnerable?," 28–35.

80. Currently, ballistic missiles mounted with hypersonic boost-glide vehicles can only maneuver while inside the atmosphere, and the density of the atmosphere at the

turning point dictates their rate of turn. Tight turns are only possible near the ground and in close proximity to the target.

81. Russia, China, and the United States have been most active in the development of hypersonic weapons. To date, however, no state has emerged as the dominant leader in this nascent technology. James M. Acton, ed., *Entanglement: Russian and Chinese Perspectives on Non-Nuclear Weapons and Nuclear Risks* (Washington, DC: Carnegie Endowment for International Peace, 2017), 54, https://carnegieendowment.org/.

82. Currently, the drag associated with hypersonic glide vehicles remaining in the atmosphere will require new propulsion technologies and innovation in ablative materials to absorb the increased heat, both of which are not expected to emerge in the near term. The author would like to thank an anonymous reviewer for making this point.

83. A particular concern identified by Russian and Chinese analysts is the possibility that a combination of US ballistic missile defense and high-precision conventional weapons (such as hypersonic weapons) could permit the US to attempt a disarming first strike without crossing the nuclear Rubicon.

84. Avery Goldstein, "First Things First: The Pressing Danger of Crisis Instability in U.S.-China Relations," *International Security* 37, no. 4 (2013): 67–68, https://muse.jhu.edu/.

85. This view in large part reflects a misperception held by Chinese analysts that the US's hypersonic and conventional prompt global strike programs are guided by clearly defined and coherent military (versus technological) objectives targeting China. As a result, Beijing would more likely perceive an ambiguous situation as an attack on its nuclear arsenals.

86. James Johnson, "The End of Military-Techno *Pax Americana*? Washington's Strategic Responses to Chinese AI-Enabled Military Technology," *The Pacific Review*, 2019, https://doi.org/10.1080/09512748.2019.1676299.

87. Analysts have noted that there are calls within China to adopt a launch-on-warning strategy and that it is developing the technology to enable this capability. See Acton, *Entanglement*, 79.

88. James M. Acton, *Silver Bullet? Asking the Right Questions about Conventional Prompt Global Strike* (Washington, DC: Carnegie Endowment for International Peace, 2013), xiv, https://carnegieendowment.org/.

89. Assessing the precise status of US-enabling capabilities is challenging because they are so highly classified. Acton, 88–90.

90. Because ICBMs and SLBMs depend on automation to set their flight trajectory and navigate to their target, they already operate de facto autonomously once launched. Thus, while autonomy enhances the strategic value of missile delivery systems, it is not an operational prerequisite—except perhaps in the underwater domain where munitions cannot be easily operated remotely.

91. Existing navigation systems tend to rely heavily on pre-mapping for navigating autonomously and identifying paths and obstacles; however, navigation systems will need to incorporate advanced vision-based guidance and built-in pre-mapping systems. Advances in machine learning techniques could significantly improve the vision-based guidance systems of these subsystems and, in turn, enable autonomy. Acton, *Silver Bullet?*, 114.

92. For example, the DOD Defense Innovation Unit plans to partner with the Joint Artificial Intelligence Center to mine large data sets across multiple aircraft platforms and ground vehicles to develop analytics and predictive maintenance applications for the US Air Force and Army.

93. So-called fire-and-forget (or semiautonomous) missiles allow the onboard sensors and computer to guide a missile to its target without further operator communications following initial target selection and fire authorization.

94. Chinese analysts have begun research into the use of big data and deep-learning AI techniques to enhance the processing speed and intelligence analysis of satellite images in support of the military's early warning capabilities, enabling a "prediction revolution" in future warfare.

95. Boulanin, *Impact of Artificial Intelligence*, 56.

96. US government–funded Sandia National Laboratories, which has made and tested hypersonic vehicles for more than 30 years, recently established an academic research coalition, Autonomy New Mexico, whose mission is to create artificially intelligent aerospace systems. Bioengineer, "Future Hypersonics Could Be Artificially Intelligent," Bioengineer.org, 18 April 2019, https://bioengineer.org/.

97. Austin Long and Brendan Rittenhouse Green, "Stalking the Secure Second Strike: Intelligence, Counterforce, and Nuclear Strategy," *Journal of Strategic Studies* 38, nos. 1–2 (2015): 37–73, DOI: 10.1080/01402390.2014.958150.

98. Researchers from China's People's Liberation Army (PLA) force, the College of Mechatronic Engineering and Automation of the National University of Defense Technology, Harbin University, and the Beijing Institute of Tracking and Telecommunications Technology have collaborated to address the technical challenges faced in control dynamics with HGVs.

99. These include, for example, drone swarms, robotics, precision guidance munitions, early warning systems, and cyber and electronic warfare capabilities.

100. While it is technically feasible, the United States does not currently see any role for unmanned bombers in nuclear weapons delivery.

101. Office of the Secretary of Defense, *Missile Defense Review* (Washington, DC: Department of Defense, 2019), https://media.defense.gov/.

102. Samuel Osborne, "Future War with Russia or China Would Be 'Extremely Lethal and Fast,' US Generals Warn," *Independent*, 6 October 2016, https://www.independent.co.uk/.

103. Jon R. Lindsay and Erik Gartzke, eds., *Cross-Domain Deterrence: Strategy in an Era of Complexity* (New York: Oxford University Press, 2019), 19.

Disclaimer and Copyright

The views and opinions in *SSQ* are those of the authors and are not officially sanctioned by any agency or department of the US government.