Artificial Intelligence, Drone Swarming and Escalation Risks in Future Warfare

James Johnson

[abstract]

The rapid proliferation of a new generation of artificial intelligence (AI)-augmented and -enabled autonomous weapon systems (AWS), most notably drones used in swarming tactics, could have a significant impact on deterrence, nuclear security, escalation, and strategic stability in future warfare. James Johnson argues that emerging iterations of AWS fused with AI systems will presage a powerful interplay of increased range, accuracy, mass, coordination, intelligence, and speed in a future conflict. In turn, the risk of escalatory use-them-or-lose-them situations between nuclear-armed military powers and the attendant dangers posed by the use of unreliable, unverified and unsafe AWS will increase, with potentially catastrophic strategic outcomes.

[end abstract]

The proliferation of a broad range of artificial intelligence (AI)-augmented autonomous weapon systems (AWS) could have significant strategic implications for nuclear security and escalation in future warfare. Several observers anticipate that sophisticated AI-augmented AWS will soon be deployed for a range of ISR and strike missions.[1] Experts generally agree that AI machine-learning systems are an essential ingredient to enable fully autonomous systems.[2] Even if AWS are used only for conventional operations, their proliferation could nonetheless have destabilising implications and increase the risk of inadvertent nuclear escalation.[3] For example, AI-augmented drone swarms may be used in offensive sorties targeting ground-based air defences by nuclear-armed states to defend their strategic assets (for example, launch

[1] 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); Zachary Kallenborn and Philipp C Bleek, 'Swarming Destruction: Drone Swarms and Chemical, Biological, Radiological, and Nuclear Weapons', *Nonproliferation Review* (Vol. 25. No. 5–6, 2018), pp. 523–43.

[2] See Stuart Russell and Peter Norvig, *Artificial Intelligence: A Modern Approach*, Third Edition (Harlow: Pearson Education, 2014), p. 56.

[3] This article is adapted from sections of a forthcoming article by the author with *Strategic Studies Quarterly* entitled, 'Artificial Intelligence: A Threat to Strategic Stability'.

facilities and their attendant command, control and early-warning systems), and to exert 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 significantly increased the perceived operational value great military powers attach to the development of a range of AWS,[4] potentially making the delegation of lethal authority to AWS an increasingly irresistible but destabilising prospect.[5] That is, defending or capturing the technological upper-hand in cutting-edge warfighting assets of strategic rivals (traditionally conservative militaries) may eschew the potential risks of deploying unreliable, unverified and unsafe AWS. Today, therefore, the main risk for stability and escalation are the technical limitations of the current iteration of AI machine-learning software (brittleness, explainability, the unpredictability of machine learning, vulnerability to subversion or 'data poisoning', and the fallibility of AI systems to biases).[6] To be sure, immature deployments of these nascent systems in a nuclear context would have severe consequences.[7]

From what is known today about emerging technology,[8] new iterations of AI-augmented advanced conventional capabilities (e.g. cyber weapons, precision munitions, and hypersonic weapons) will compound the risk of military escalation,

---

[4] '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 analysing), planning, and decision-making. See, US Department of Defense, Directive 3000.09, Autonomy in Weapon Systems, 21 November 2012, <http://www.esd.whs.mil/Portals/54/Documents/DD/issuances/DODd/300009p.pdf>, accessed December 1 2019.
An autonomous weapon system (or lethal autonomous weapon system, LAWS) is a weapon system that, once activated, can select and engage targets without further intervention by a human operator. A distinction is often made by some between automatic, automated and autonomous systems, while others use these terms interchangeably. For this article, it is simply necessary to acknowledge that the debate exists.

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

[6] In this context, 'brittleness' refers to the inability of AI to contextualise in a fast-moving and complex environment. AI machine-learning systems rely on high-quality datasets to train their algorithms; thus, injecting so-called 'poisoned' data into those training sets could lead these systems to perform in undesired and potentially undetectable ways.

[7] 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.

[8] Military-use AI, and the advanced capabilities it enables, can be conceptualised as a natural manifestation (rather than the cause or origin) of an established trend in emerging technology towards co-mingling and increasing the speed of warfare, which could lead states to adopt destabilising launch postures. See 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/2017/03/how-us-nuclear-force-modernization-is-undermining-strategic-stability-the-burst-height-compensating-super-fuze/>, accessed 5 December 2019.

especially inadvertent and accidental escalation.[9] Co-mingling and entangling nuclear and non-nuclear capabilities[10] and the increasing speed of warfare may undermine strategic stability.[11] While the potential escalation risks posed by emerging technology have been widely discussed in the academic literature, the potential of military AI to compound these risks and spark inadvertent escalation has thus far only been lightly researched.[12] This article addresses how and why AI-enhanced drone swarming might affect strategic stability between nuclear-armed great powers.

[H1]AI Force-Multiplied Drone Swarms

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. Currently, only a few weapon systems select and engage their targets without human intervention.[13] Loitering attack munitions (LAMs) – also known as 'loitering munitions' or 'suicide drones' – pursue targets (such as enemy radar, ships or tanks) based on pre-programmed targeting criteria, and launch an attack when its sensors

[9] '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 escalation 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); Lawrence Freedman, *Evolution of Nuclear Strategy* Third Edition (London: Palgrave Macmillan, 2003), Chap. 14.

[10] 'Entanglement' in this context refers to dual-use delivery systems that can be armed with nuclear and non-nuclear warheads; the commingling of nuclear and non-nuclear forces and their support structures; and non-nuclear threats to nuclear weapons and their associated command, control, communication, and information (C3I) systems.

[11] 'Strategic stability' as a concept in political science has been defined in many ways. See, for example, Colby Elbridge and Michael Gerson (eds), *Strategic Stability: Contending Interpretations* (Carlisle, PA: Army War College, 2013).

[12] For notable exceptions, see Vincent Boulanin (ed.) *The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk: Vol. I Euro-Atlantic Perspectives* (Stockholm: SIPRI Publications, 2019); Edward Geist and Andrew J Lohn, *How Might Artificial Intelligence Affect the Risk of Nuclear War?* (Santa Monica, CA: RAND Corporation, 2018); Kareem Ayoub and Kenneth Payne, 'Strategy in the Age of Artificial Intelligence', *Journal of Strategic Studies* (Vol. 39, No. 5–6, 2016), pp. 799–819; Technology for Global Security and Center for Global Security Research, 'AI and the Military: Forever Altering Strategic Stability,' *Medium,* 13 February 2019; Jürgen Altmann and Frank Sauer, 'Autonomous Weapon Systems and Strategic Stability', *Survival* (Vol. 59, No. 5, 2017), pp. 117–42; James Johnson, 'Artificial Intelligence and Future Warfare: Implications for International Security', *Defense & Security Analysis* (Vol. 35, No. 2, 2019), pp. 147–69.

[13] To date, the only known operational loitering attack munition (LAM) is Israel's Harop (or Harpy II), a fully autonomous anti-radar loitering weapon that can remain in flight for up to six hours and dive-bomb radar signals without human direction with lethal effect on the battlefield. Also, several states are known to be developing fully autonomous weapons including China, Germany, India, Israel, South Korea, Russia, and the United Kingdom.

detect an enemy's air-defence radar.[14] Compared to cruise missiles (designed to fulfil a similar function), LAMs use AI technology to shoot down incoming projectiles faster than a human operator could and can remain in flight (or loiter) for far longer periods than human-operated munitions. In contrast to existing human-operated automated systems (for example, manned systems and remote-controlled drones),[15] AWS such as LAMs could complicate the ability of states to anticipate and attribute autonomous attacks reliably.[16]

A low-cost, lone-wolf UAV would be unlikely, for example, to 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 defence capabilities even in heavily defended regions such as China's east and coastal regions.[17] Moreover, stealth variants of these systems,[18] along with miniaturised electromagnetic jammers and cyber-weapons, may be used to interfere with or subvert an adversary's targeting sensors and communications systems, undermining its multi-layered air-defences in preparation for drone swarms and long-range stealth-bomber offensive attacks.[19] In 2011, for example,at Creech US Air Force Base, aircraft cockpit systems – operating MQ-1 and MQ-9 unmanned drones in the Middle East – were infected with malicious malware, exposing the vulnerability of US systems to cyber-attack.[20] This threat might, however, be countered by the integration of future iterations of AI technology into stealth fighters

[14] LAMs are hybrid offensive capabilities sitting between guided munitions and unmanned combat aerial systems. To date, the only known operational LAM is Israel's Harop (or Harpy II), combining a human-in-the-loop and fully autonomous mode. See, Tyler Rogoway, 'Meet Israel's 'Suicide Squad' of Self-Sacrificing Drones', *The Drive*, 8 August 2016, <https://www.thedrive.com/the-war-zone/4760/meet-israels-suicide-squad-of-self-sacrificing-drones.>, accessed 10 December 2019.
[15] For example, Daesh (also known as the Islamic State of Iraq and Syria, ISIS) used remote-controlled aerial drones in its military operations in Iraq and Syria. See Ben Watson, 'The Drones of ISIS,' *Defense One*, 12 January 2017.
[16] Rogoway, 'Meet Israel's 'Suicide Squad' of Self-Sacrificing Drones', *The Drive*.
[17] Paul Scharre, 'Highlighting Artificial Intelligence: An Interview with Paul Scharre', *Strategic Studies Quarterly* (Vol.11, No 4, November 2017), pp. 18-9.
[18] China, the US, the UK and France have developed and tested stealth UAV prototypes. See, Dan Gettinger, *The Drone Database* (New York, NY: Center for the Study of the Drone, Barnard College Press, 2019).
[19] The Russian military, for example, reportedly deployed jammers to disrupt GPS-guided UAVs in combat zones, including Syria and Eastern Ukraine. See, Madison Creery, 'The Russian Edge in Electronic Warfare', *Georgetown Security Studies Review*, 26 June 2019, <https://georgetownsecuritystudiesreview.org/2019/06/26/the-russian-edge-in-electronic-warfare/>, accessed 5 December 2019.
[20] Noah Shachtman, 'Computer Virus Hits US Drone Fleet', *Wired,* 10 July 2011.

such as the F-35.[21] Manned F-35 fighters developed by the United States 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.[22] In the future, the extended endurance of UAVs and unmanned support platforms could potentially increase the ability of drone swarms to survive these kinds of countermeasures.

[h1]Taking Humans out of the Loop

As military commanders are concerned with tightly controlling the rungs on the 'escalation ladder',[23] they should, in theory, be against delegating too much decision-making authority to machines – especially when nuclear weapons are involved. Competitive pressures between great military powers and the fear that others will gain the upper hand in the development and deployment of military AI (and the AWS that AI could empower) might overwhelm these concerns, however. It is worth highlighting a caveat. The hypothetical uses of drone swarming described below do not assume that militaries will *necessarily* be able to implement these AWS in the near term. Certainly, disagreements exist among AI researchers and analysts about the significant operational challenges faced by states in the deployment of AI-enabled AWS; in particular, issues relating to machine-to-machine communications, swarm coordination in complex and contested environments, and battery technology, to name a few.[24]

Several prominent researchers have opined that, notwithstanding the

[21] AI-infused algorithms able to integrate sensor information, consolidate targeting, automate maintenance and navigation and sensor information are currently being developed and tested to anticipate the kinds of high-intensity future threat to environments posed by drone swarming. Kris Osborn, 'The F-35 Stealth Fighter: The Safest Fighter Jet Ever Made?' *The National Interest*, September 27 2019, <https://nationalinterest.org/blog/buzz/f-35-stealth-fighter-safest-fighter-jet-ever-made-83921>, accessed 6 December 2019.

[22] A combination of restrictions contained within the DoD's 'Autonomy in Weapons Systems' guidance, as well as the cultural and bureaucratic norms and practices within the US armed services, will likely stymie efforts to incorporate AI-enabled systems. See Department of Defense Directive, 'Autonomy in Weapon Systems', 3000.09, Incorporating Change 1, 8 May 2017, <https://fas.org/irp/doddir/dod/d3000_09.pdf>, accessed 6 December 2019.

[23] 'Escalation ladder' in this context refers to the forty-four 'rungs' on a metaphorical ladder of escalating military conflict. For the seminal text that introduced the concepts of an 'escalation ladder' as it applies to the entire range of conflict from conventional conflict to all-out nuclear warfare see, Herman Kahn, *On Escalation: Metaphors and Scenarios* (New York: Praeger, 1965).

[24] For recent debate surrounding AWS, and the technical limitations faced by engineers in their production see, Zachary Kallenborn and Philipp C Bleek, 'Swarming Destruction: Drone Swarms and Chemical, Biological, Radiological, and Nuclear Weapons', *Nonproliferation Review*, pp. 523–43.

remaining technical challenges,[25] as well as the legal and ethical feasibility, it is likely that operational AWS could be seen within a matter of years. The moral and ethical considerations related to the use of autonomous control weapons and autonomous targeting is complex and highly contested; humans creating autonomous control technology to attack a human is inherently problematic.[26] According to former US Deputy Secretary of Defense Robert Work, the US, 'will not delegate lethal authority to a machine to make a decision' in the use of military force.[27] Work added, however, that such self-restraint could be tested by a strategic competitor (especially China or Russia) 'who 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'.[28] Removing human judgement from the crisis decision-making process, however, and pre-delegating authority to autonomous systems may severely challenge the safety, resilience and credibility of nuclear weapons in future warfare.[29]

History is replete with examples of near nuclear misses, demonstrating the importance of human judgement in mitigating the risk of miscalculation and misperception, of the intentions, redlines and willingness to use force between adversaries during crises.[30] But despite these precedents, the risks associated with unpredictable AI-augmented autonomous systems operating in dynamic and complex, and possibly *a priori* unknown environments, remain underappreciated by global defence communities.[31] Eschewing these risks, China and Russia plan to incorporate

---

[25] While recent breakthroughs in AI have made possible the automation of several tasks previously considered to be too complex (for example, dependable vehicle control and air-traffic control), there remain technical limits to what computers and robots can achieve autonomously. See, for example, Boulanin (ed.), *The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk Vol. I Euro-Atlantic Perspectives*, Chap. 3.

[26] For example, see Paul Scharre, *Autonomous Weapons and Operational Risk – Ethical Autonomy Project,* (Washington, DC: Center for a New American Security, 2016); Rob Sparrow, 'Ethics as a Source of Law: The Martens Clause and Autonomous Weapons', *ICRC Blog*, 14 November 2017, <https://blogs.icrc.org/law-and-policy/2017/11/14/ethics-source-law-martens-clause-autonomous-weapons/>; Heather Roff, *Autonomy, Robotics, and Collective Systems* (Geneva: Centre for Security Policy, 2016).

[27] Quote from an interview: *Washington Post,* 'David Ignatius and Pentagon's Robert Work Talk About New Technologies to Deter War', 30 March 2016, <https://www.washingtonpost.com/blogs/post-live/wp/2016/02/29/securing-tomorrow-with-david-ignatius-whats-at-stake-for-the-world-in-2016-and-beyond/>, accessed 5 December 2019.

[28] *Washington Post*, 'David Ignatius and Pentagon's Robert Work Talk About New Technologies to Deter War'.

[29] UAVs used in swarming operations do not necessarily need to be 'fully-autonomous'; humans could still decide to execute a lethal attack. See, Boulanin (ed.), *The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk Vol. I Euro-Atlantic Perspectives*, Chap. 3.

[30] Patricia Lewis et al., *Too Close for Comfort: Cases of Near Nuclear Use and Options for Policy* (London: Chatham House, 2014).

[31] Developing AWS that are able to interact and communicate with other agents (especially humans) in

AI into UAVs and unmanned underwater vehicles (UUVs) for swarming missions infused with AI machine-learning technology.[32] Chinese strategists have reportedly researched data-link technologies for 'bee-swarm' UAVs, emphasising network architecture, navigation and anti-jamming military operations, in particular, to target US aircraft carriers.[33]

[h1]Drone Swarming and New Strategic Challenges

Drones used in swarms are well-suited to conduct preemptive attacks and nuclear-ISR missions against an adversary's nuclear and non-nuclear mobile missile launchers and nuclear-powered ballistic missile submarines (SSBNs) and their attendant enabling facilities (for example, C3I and early-warning systems, antennas, sensors, and air intakes).[34] Some observers have posited that autonomous systems, such as the DoD's *Sea Hunter*, a prototype autonomous surface vehicle, may render the underwater domain transparent, thereby eroding the second-strike deterrence utility of stealth SSBNs. The technical feasibility of this hypothesis is highly contested, however.[35] Because of these technical challenges, the Cold War mutually assured destruction (MAD)-based nuclear deterrence is likely to remain unchallenged by AI-augmented counterforce capabilities for the foreseeable future.[36]

---

either a competitive or a collaborative context is inherently problematic because human behaviour is often unpredictable. See Andrew Ilachinski, *AI, Robots, and Swarms, Issues, Questions, and Recommended Studies* (Alexandria, VA: CNA, 2017), p. xv.

[32] The Pentagon refers to this unmanned underwater vehicles (UUV) as 'Kanyon'. The nuclear warhead carried by this drone is reportedly capable of destroying ports and cities. Matthew Griffin, 'Russia Tests its New Autonomous Nuclear Submarine off the US Coast', *Fanatical Futurist*, 11 December 2016, <http://www.fanaticalfuturist.com/2016/12/pentagon-detects-tests-of-russias-new-nuclear-capable-drone-submarine/>, accessed 7 December 2019.

[33] Elsa Kania, *Battlefield Singularity: Artificial Intelligence, Military Revolution, and China's Future Military Power* (Washington, DC: Center for a New American Security, November 2017), p. 23.

[34] In addition to drone swarms, an expanding range of advanced non-nuclear strategic weapons (such as cyber, anti-satellite weapons (ASAT) and hypersonic vehicles) are also well suited to conducting preemptive strikes – primarily used in cross-domain operations.

[35] While there are several technologies under development specifically designed to track SSBNs (for example the DoD's *Sea Hunter*), these programmes remain immature. Several technical challenges remain in the development of AWS that will limit their operational utility as weapons for offensive operations over extended geographical ranges and duration, and, above all, battery power. See Jonathan Gates, 'Is the SSBN Deterrent Vulnerable to Autonomous Drones?' *RUSI Journal* (Vol. 161, No. 6, 2016), pp. 28–35; Sebastian Brixey-Williams, 'Will the Atlantic Become Transparent?' Second Edition, *British Pugwash*, November 2016.

[36] A nuclear-armed state would need a very high degree of confidence that it could identify and preemptively destroy (or disable) all of an adversary's nuclear-weapon delivery systems capable of launching devastating retaliatory attacks. If a counterforce attack intends to disarm the adversary *before* it can respond with nuclear weapons, targeting certainty would need to be almost 100%. See Joseph Johnson, 'MAD in an AI Future?' Center for Global Security Research, Lawrence Livermore National Laboratory, 3 June 2019.

On the one hand, several experts argue that deployed in large swarms these platforms could transform anti-submarine warfare (ASW), rendering at-sea nuclear deterrence virtually redundant.[37] On the other hand, others consider such a hypothesis as technically premature because: it is unlikely that sensors onboard AWS would be able to detect deeply submerged submarines reliably; the range of these sensors (and the drones themselves) would be limited by battery power over extended ranges;[38] and, given the vast areas traversed by SSBNs on deterrence missions, the chance of detection is negligible, even if a large number of autonomous swarms were deployed on reconnaissance missions.[39]

Despite continued advances in sensor technology designed to overcome the challenge of submarine quieting in ASW (reduced cost, size and detection ranges), several technical challenges remain including: underwater communication between multiple systems; processing-power requirements; battery life and energy generation; and scaling the system.[40] Rather than making submarines redundant, therefore, modern ASW capabilities have reduced their effectiveness, slowing their deployment in patrol areas, inhibiting them from getting into firing position, and disrupting the coordination of attacks.[41]

Recent advances in sensor, communication and processing technologies (especially big-data analytics and machine learning) could become disruptive transformative technologies in future ASW and undersea support platforms (for example, UUVs, unmanned surface vehicles (USVs), and UAVs) to locate and attack submarines in real time, and enhance the stealth and endurance of submarines and their attendant weapon systems.[42] A combination of AI machine learning and big-data

---

[37] For example, see Owen R. Cote Jr., 'Invisible Nuclear-armed Submarines or Transparent Oceans? Are Ballistic Missile Submarines Still the Best Deterrent for the United States?' *Bulletin of the Atomic Scientists,* pp. 30-35.

[38] Unlike standard UUVs which are typically tethered and have a very short range, underwater gliders (for example, US Liquid Robotics' *Waverider* SV3), while slow, are able to roam over long distances for months at a time. See, Jonathan Gates, 'Is the SSBN Deterrent Vulnerable to Autonomous Drones?' *The RUSI Journal* (Vol.161, No.6, 2016), pp.28-35.

[39] Gates, 'Is the SSBN Deterrent Vulnerable to Autonomous Drones?'.

[40] Unmanned drone platforms are capable of carrying several types of sensors, and the swarming machine-learning systems to control them are either already available or in the advanced stages of development, including: active and passive sonar; magnetic anomaly detectors; wake detection LIDAR; thermal sensors, and laser-based optical sensors capable of piercing seawater.

[41] Even failed ASW operations have compelled a submarine to evade and lose the initiative, or made it more traceable, for a fresh ASW attack. See Bryan Clark, *The Emerging Era in Undersea Warfare* (Washington, DC: Center for Strategic and Budgetary Assessments, 2018), p. 3–4.

[42] See, Jürgen Altmann and Frank Sauer, 'Autonomous Weapon Systems and Strategic Stability', *Survival* (Vol. 59, No. 5, 2017), pp. 117–42; and James Johnson, 'Artificial Intelligence and Future

analytics could enhance Cold War-era sensitivity technology to detect radiation and chemical emissions from submarines, and in turn, enable new capabilities to detect and cue torpedo-seekers in long-range ASW (and potentially 'fire and forget') operations.[43] For now, however, the technical feasibility of this hypothesis remains highly contested.

Significant advances in power, sensor technology and communications would be needed before these autonomous systems have a game-changing strategic impact on submarine reconnaissance.[44] 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, in particular where strategic force asymmetries exist. Autonomous capabilities – like DARPA's *Sea Hunter* – demonstrate how autonomous weapons could accelerate the completion of the iterative targeting cycle to support joint operation; thereby, reducing the reliability and survivability of states' nuclear second-strike capability, and potentially, causing use-them-or-lose-them situations.

In the near-term, therefore, the most significant destabilising impact of AI on nuclear deterrence will likely be the synthesis of autonomy with a range of machine-learning-augmented sensors, potentially undermining states' confidence in the survival of their second-strike capabilities, which could trigger a retaliatory first strike.[45] Enhanced exponential growth in computing performance,[46] together with advances in the machine-learning techniques that can rapidly process data in real time, will empower drone swarms to perform increasingly complex missions, such as hunting hitherto hidden nuclear deterrence forces. In short, the ability of future iterations of AI that are able to make predictions based on the fusion of expanded and dispersed datasets, and then locate, track and target strategic missiles in underground

---

Warfare: Implications for International Security', *Defense & Security Analysis* (Vol. 35, No. 2, 2019), pp. 147–69.

[43] So-called 'fire-and-forget' (or 'semi-autonomous) missiles allow the onboard sensors and computer to guide a missile to its target without further operator communications following initial target selection and fire authorisation. See, Clark, *The Emerging Era in Undersea Warfare*, p. 10.

[44] Drones (including UAVs, UUVs and USVs) might nonetheless have a significant qualitative impact on ASW. For example, drone swarms deployed at chokepoints (or gateways), or an adversary's docking exit routes, could act as a layered physical barrier, deterring or denying an opponent's submarine the ability to operate within certain military zones (for instance, anti-access/area-denial (A2/AD) zones).

[45] See, James Johnson, 'The AI-cyber Nexus: Implications for Military Escalation, Deterrence and Strategic Stability', *Journal of Cyber Policy*, 9 December 2019, DOI:10.1080/23738871.2019.1701693.

[46] Tom Simonite, 'Moore's Law Is Dead. Now What?', *MIT Technology Review*, 13 May 2016.

silos (especially mobile intercontinental ballistic missile launchers), on board stealth aircraft, SSBNs and truck or rail-mounted transporter erectors-launchers (TELs), is set to grow.[47]

[H1]Tactical Possibilities of AI-Augmented Swarming

The following three scenarios illustrate the possible strategic operations AI-augmented drone swarms would execute.[48]

First, drone swarms could be deployed to conduct nuclear-ISR operations to locate and track dispersed (nuclear and non-nuclear) mobile missile launchers and their attendant enabling C3I systems.[49] Specifically, swarms incorporating AI-infused ISR, autonomous sensor platforms, automated targeting recognition (ATR) systems, and data-analysis systems may enhance the effectiveness and speed of sensor drones to locate mobile missiles and evade enemy defences.[50] Satellite imagery and signals intelligence from these swarms could then cue stealth fighters or armed drones to destroy these missiles. [51]

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 defences, clearing the path for swarms of hypersonic autonomous delivery systems armed with conventional or nuclear payloads.[52] The development and deployment of offensive-dominant weapons such as hypersonic boost-glide weapons (HGVs), which uses boost glide technology to propel warheads with conventional (and potentially

---

[47] Elias Groll, 'How AI Could Destabilize Nuclear Deterrence', *Foreign Policy*, 24 April 2018.
[48] The value of AWS in these scenarios does not mean that they are the *only* or necessarily most effective way to fulfil these missions. See Gates, 'Is the SSBN Deterrent Vulnerable to Autonomous Drones?'.
[49] In 2011, students at MIT 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 programmes. See Kallenborn and Bleek, 'Swarming Destruction', pp.1-2.
[50] See, Office of the Secretary of Defense, *2019 Missile Defense Review,* <https://media.defense.gov/2019/Jan/17/2002080666/-1/-1/1/2019-MISSILE-DEFENSE-REVIEW.PDF>, accessed 2 December 2019.
[51] Austin Long and Brendan Rittenhouse Green, 'Stalking the Secure Second Strike: Intelligence, Counterforce, and Nuclear Strategy', *Journal of Strategic Studies* (Vol. 38, Nos. 1–2, 2015), pp.21-24.
[52] Currently, ballistic missiles mounted with hypersonic boost-glide vehicles can only manoeuvre 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 close to its target. See, Boulanin, Vincent and Maaike Verbruggen. *Mapping the Development of Autonomy in Weapon Systems* (Stockholm, Sweden: Stockholm International Peace Research Institute, 2017), Chap. 3.

nuclear payloads),[53] may eventually exacerbate the problem of target ambiguity, increase the risks of inadvertent escalation, and in turn, lower the nuclear threshold.[54]

Because of the inherent difficulty in finding mobile missiles, even modest improvements towards enabling this capability (or even the perception of vulnerability) could be a strategic game-changer.[55] According to a RAND Corporation analysis, 'the hunt for conventionally armed missiles could result in the attrition of China's nuclear-capable missile force', undermining crisis stability and causing use-them-or-lose-them situations.[56] In this way, autonomy in advanced AI-augmented drone swarms will likely exacerbate the co-mingling problem-set, and in turn, increase strategic instability.

Second, drone swarming might enhance legacy – conventional and nuclear – weapon delivery systems (for example, intercontinental ballistic missiles and submarine-launched ballistic missiles), possibly incorporating hypersonic variants (discussed in detail below).[57] AI applications will likely enhance the delivery system targeting and tracking and improve the survivability of drone swarms against the current generation of missile defences. For example, technological advances in hypersonic boost-glide weapons – especially deployed in conjunction with cruise missiles, missile defence capabilities, and supported by drone swarms – could target an adversary's high-value assets such as radars, ASAT weapons, mobile missile launchers, C3I systems, and TELs used to undergird both nuclear and conventional

---

[53] Russia, China and the US have been the most active states in the development of hypersonic weapons. To date, however, no state has emerged as the dominant leader in this nascent technology. See James M Acton (ed.), 'Entanglement: Russian and Chinese Perspectives on Non-Nuclear Weapons and Nuclear Risks', Carnegie Endowment for International Peace, 2017, p. 54.

[54] Currently, the drag associated with HGVs 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.

[55] Analysts continue to emphasise the various technical challenges in locating mobile missiles for counterforce operations. UAVs would not only need to track in real time, but also communicate in real time in a manner that could not be detected, and cue a rapid surprise attack, before the mobile launchers could be relocated. See Austin Long and Brendan Rittenhouse Green, 'Stalking the Secure Second Strike: Intelligence, Counterforce, and Nuclear Strategy', *Journal of Strategic Studies* (Vol. 38, Nos. 1–2, 2015), pp. 21–24.

[56] Eric Heginbotham et al., *The U.S.-China Military Scorecard: Forces, Geography, and the Evolving Balance of Power 1996–2017* (Arlington, VA: RAND Corporation, 2015), p. 353.

[57] At least two nuclear-armed states are considering the possibility of using UAVs or UUVs for nuclear delivery. In 2015, Russia 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*, which could potentially be used to operate remotely while carrying nuclear payloads. Other unmanned combat aerial vehicle (UCAV) prototypes (for example, the Northrop Grumman X-47B, the Dassault nEUROn, and the BAE Systems' Taranis) could also feasibly be used in nuclear attacks. See Boulanin (ed.), *The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk*, pp. 56–57.

missiles.[58] However, the dependency of swarms on these systems (similar to cyber-defences, discussed below) could make them more vulnerable to attack, for example, from spoofing, manipulation, digital jamming, and electromagnetic pulses.[59]

To reduce these vulnerabilities, sensor drone swarm formations could apply AI-augmented ISR to bolster intelligence collection, intra-swarm communication and analysis, widening the geographical range of its operations and monitoring for potential threats to the swarm, thereby leaving the remainder of the swarm unfettered to perform its offensive activities.[60] For example, the US Defense Advanced Research Projects Agency (DARPA) recently tested how drone swarms might collaborate and coordinated tactical decisions in a high-threat environment with minimal (or denied) communications.[61]

Third, drone swarming tactics could equally bolster a states' ability to disable or suppress an adversary's defences (for example, air defences, missile defences, and ASW defences), clearing the path for a disarming attack.[62] Drone swarms might be armed with cyber or electronic warfare (EW) capabilities (in addition to anti-ship, anti-radiation, 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.[63] For instance, in classical defence, through denial tactics a state could attack an enemy's sensors and control systems with a drone swarm armed with EW or cyber weapons, degrading its integrated air-defence systems (for example, for spoofing and electromagnetic pulse attacks),[64] while simultaneously deploying a separate swarm to draw fire away from its weapon systems and protecting its

---

[58] See, James M. Acton, 'Silver Bullet? Asking the Right Questions About Conventional Prompt Global Strike' (Washington, DC: Carnegie Endowment for International Peace, 2013).
[59] While similar vulnerabilities exist in other technically advanced weapon systems discussed in this article, UAV swarms require a high degree of autonomy, which will likely make them more susceptible to these kinds of attacks.
[60] Drone swarms could be programmed to make regular changes to the route to counter an adversary using AI machine-learning-augmented intelligence to anticipate its trajectory and defeating detection. See Kallenborn and Bleek, 'Swarming Destruction', p.16.
[61] Pawlyk Oriana, 'Pentagon Still Questioning How Smart to make its Drone Swarms', *Military.com,* 7 February 2019.
[62] Mike Pietrucha, 'The Need for SEAD Part 1: The Nature of SEAD', *War on the Rocks*, 17 May 2016.
[63] Polat Cevik et al., 'The Small and Silent Force Multiplier: A Swarm UAV-Electronic Attack', *Journal of Intelligent and Robotic Systems* (Vol. 70, Nos. 1–4, April 2013), pp. 595–608.
[64] To date, all operable air-defence systems operate under human supervision, and fully automatic mode is generally used to defend against anti-ship cruise missiles. See, John K. Hawly, 'Patriot Wars: Automation and the Patriot Air and Missile Defense Systems', (Washington, DC: CNAS, January 2017).

sensors,[65] thus clearing the path for launching a sortie of conventionally (and possibly nuclear) armed drones and long-range stealth bombers.[66]

Conversely, drone swarms might enhance states' missile defences 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.[67]

[H1]Unravelling the Underwater Leg of Cold-War Nuclear Deterrence?

In the maritime domain, UUVs, USVs and UAVs, supported by AI-enabled intra-swarm communication and ISR systems, could be deployed simultaneously in both offensive and defensive ASW operations to saturate an enemy's defences and locate, disable and destroy its nuclear-armed or non-nuclear attack submarines.[68] Tracking a submarine from a ship (or even from another submarine) is a challenging operation even in relatively benign conditions[69] because of the stealth technology – especially minimal acoustic signatures – of modern diesel-electric submarines (SSKs) and SSBNs, along with the immense challenge of coordinating such an operation.[70]

While some experts do not expect a technically reliable and effective capability of this kind to be operational for at least a decade, others are more

---

[65] Swarms could be used as decoys to create false signatures (for example, time delays in tricking a defender), or to force an enemy to reveal (or 'light up') its weapons by switching on their radars to attack drone swarms.

[66] Drone swarms might also be used in swarm versus swarm combat scenarios, including drones armed with nuclear and conventional payloads and hypersonic boost-glide variants. Machine-to-machine collaboration is still at a very nascent stage, however.

[67] While the US Missile Defense Agency (MDA) is developing lasers for drones, the size of a drone needed to power a laser of meaningful power would be huge. The likelihood, therefore, that this will be seen 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 by the end of 2023. Jen Judon, 'MDA Awards Contracts for a Drone-Based Laser Design,' *Defense News*, December 11, 2017.

[68] The US Defense Advanced Research Projects Agency (DARPA) is currently developing the Anti-Submarine Warfare Continuous Trail Unmanned Vessel (ACTUV) programme to track quiet diesel-electric submarines with USVs from the surface. In 2017, China reportedly launched a new stealth unmanned oceanic combat vehicle (the D3000) capable of engaging in both ASW and surface warfare missions. See, P.W. Singer and Jeffrey Lin, 'With the D3000, China Enters the Robotic Warship Arms Race', *Popular Science*, 25 September 2017, <https://www.popsci.com/robotic-warship-arms-china-d3000/>, accessed 6 December 2019.

[69] Less benign environments, such as difficult to access Arctic Ice or contested A2/AD zones, would be far more complicated, and during crisis and conflict potentially escalatory and accident-prone.

[70] A submarine commander could reduce a submarine's vulnerability to ASW operations in the following ways: using the thermocline; changing speed; depth; heading; bathymetric features (i.e., the depth of water relative to sea level); and the hunting ship's acoustic profile, as well as using decoys and surface or environmental disturbance techniques. See David Blagden, 'What DARPA's Naval Drone Could Mean for the Balance of Power', *War on the Rocks*, 9 July 2016.

optimistic.[71] From a tactical perspective, drone swarms would not need ocean-wide coverage (or full ocean transparency) to detect and track submarines effectively.[72] According to British Rear Admiral John Gower, a relatively even spread of sensors might be sufficient for 'a *viable search and detection plan* [to] be conceived for the open ocean', requiring 'high tens of thousands or low hundreds of thousands of UUVs'.[73] Moreover, advances in mobile sensing platforms could enable drone swarms to locate submarines through chokepoints (or gateways) as they emerge from ports, and then to trail them autonomously.[74] In this way, new iterations of machine-learning-augmented UUVs and USVs might complement, and perhaps replace entirely, the traditional role of general-purpose SSBNs and manned surface vehicles in tracking and trailing submarines of adversaries at chokepoints, while simultaneously mounting sparsely distributed and mobile-distributed network system sensors on UUVs.[75]

[H1]Algorithm Warfare and *Force Majeure* Autonomous Weapons

If a state views the credibility of its survivable nuclear weapons (especially nuclear-armed submarines) to be at risk, conventional capabilities such as drone swarms will likely have a destabilising effect at a strategic level.[76] 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 destabilising. Moreover, the speed of AI could put the defender at a distinct disadvantage, creating additional incentives to strike first (or preemptively) at 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.

---

[71] Brixey-Williams, 'Will the Atlantic Become Transparent?'
[72] John Gower, 'Concerning SSBN Vulnerability – Recent Papers', *BASIC*, 10 June 2016.
[73] Ibid. Emphasis added by author.
[74] Patrick Tucker, 'How AI Will Transform Anti-Submarine Warfare', *Defense One*, 1 July 2019, <https://www.defenseone.com/technology/2019/07/how-ai-will-transform-anti-submarine-warfare/158121/>, accessed 5 December 2019.
[75] To date, the US Navy has deployed and tested digital network systems (DNS) in littoral waters. For example, PLUSNet (Persistent Littoral Undersea Surveillance Network) is a joint project between the US Navy's Office of Naval Research and DARPA that began in 2005. 'Persistent littoral surveillance: automated coast guards', Naval Technology, 30 April 2012, <https://www.naval-technology.com/features/featurenavy-persistent-littoral-surveillance-auvs-uuvs/,>, accessed 8 December 2019.
[76] See Jurgen Altmann and Frank Sauer, 'Autonomous Weapons and Strategic Stability', *Survival* (Vol. 59, No. 5, Oct-Nov 2017), pp. 121-127.

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.[77]

Combining speed, persistence, scope, coordination, and battlefield mass, AWS will offer states attractive asymmetric options to project military power within contested anti-access/area denial (A2/AD) zones.[78] Enhanced by sophisticated machine-learning neural networks,[79] China's manned and unmanned drone teaming operations could potentially impede future US freedom of navigation operations in the South China Seas.[80] 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 destabilising – at both a conventional and nuclear level.[81] China is reportedly developing and deploying UUVs to bolster its underwater monitoring and anti-submarine capabilities, as part of a broader goal to establish an 'underwater Great Wall' to challenge US undersea military primacy.[82] US AI-enhanced UUVs could, for example, potentially threaten both China's nuclear ballistic and non-nuclear attack

[77] 'Autonomy' is fundamentally a software endeavour. That is, software (for example, AI machine-learning techniques for sensing, modelling and decision-making) rather than hardware separates existing armed unmanned and remote-controlled weapon systems (for example, the US MQ-9 Reaper) from 'fully autonomous' iterations. Paul Scharre, 'Counter-Swarm: A Guide to Defeating Robotic Swarms', *War on the Rocks*, 3 March 2015, <http://warontherocks.com/2015/03/counter-swarm-a-guide-to-defeatingrobotic-swarms/>, accessed 1 December 2019.

[78] China's military has incorporated a range of advanced UAVs into all four services of its force structure. Elsa B. Kania, *Battlefield Singularity: Artificial Intelligence, Military Revolution, and China's Future Military Power*, (Washington DC: Center for a New American Security, 2017).

[79] The 'neural network' approach to AI represents only a small segment of the advances in AI techniques. AI also includes language-processing, knowledge representation and inferential reasoning, enabled by the rapid improvements in software, hardware, data-collection, and data storage.

[80] In early 2018, China began constructing the world's largest test site for 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. Elsa B. Kania, *Battlefield Singularity: Artificial Intelligence, Military Revolution, and China's Future Military Power*, p. 25.

[81] Reports indicate that China is engaged in the development of several potentially destabilising 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', 2019.

[82] Catherine Wong, '"Underwater Great Wall": Chinese Firm Proposes Building Network of Submarine Detectors to Boost Nation's Defence', *SCMP*, 19 May 2016, https://www.scmp.com/news/china/diplomacy-defence/article/1947212/underwater-great-wall-chinese-firm-proposes-building>, accessed 2 December 2019.

submarines.[83] Thus, even if US UUVs were programmed only to threaten China's non-nuclear (or non-strategic) attack submarine fleets, Chinese commanders might nonetheless fear that China's nascent, and relatively noisy and small (compared to U.S. and Russian SSBNs) sea-based nuclear deterrent could be neutralised more easily.[84]

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 non-nuclear attack fleets, Chinese commanders might nonetheless fear that its nascent and relatively small (compared to American and Russian SSBN fleets) sea-based nuclear deterrent could be neutralised more easily.[85] 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 US. To test the veracity of this scenario, a better understanding of Chinese thinking on the use of its nuclear and strategic non-nuclear capabilities and how they could inform China's attitude to escalation risk would be required.

[h1]Conclusion

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 tool to erode a militarily superior adversary's deterrence and resolve.[86] China's 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 to monitor and control the waters in the South China Sea, potentially impeding future US freedom of navigation operations. Were China to infuse its cruise missiles and hypersonic glide capabilities

[83] A range of autonomous ground vehicles and underwater vehicles are already in development globally, with varying degrees of success. See, Mary L. Cummings, *Artificial Intelligence and the Future of Warfare* (London, UK: Chatham House, 2017), pp. 8-9.

[84] For example, Chinese reports from the 2016 seizure of a US UUV suggest that this action was taken because of the perceived threat posed to Chinese nuclear-armed submarines by the US Navy in the region. Chris Buckley, 'Chinese Navy Returns Seized Underwater Drone to US', *New York Times*, 12 December 2016.

[85] James M Acton (ed.), 'Entanglement: Russian and Chinese Perspectives on Non-Nuclear Weapons and Nuclear Risks', *Carnegie Endowment for International Peace*, 2017, pp. 47-77.

[86] Paul Scharre, 'Autonomous Weapons and Operational Risk: Ethical Autonomy Project', Center for a New American Security, February 2016.

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 destabilising – at both a conventional and nuclear level.

In sum, notwithstanding the remaining technical challenges (especially the demand for power),[87] 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.

[author bio]

James Johnson is a Postdoctoral Research Fellow at the James Martin Center for Nonproliferation Studies (CNS) at the Middlebury Institute of International Studies, Monterey. James holds a Ph.D. in Politics & International Relations from the University of Leicester, where he is also an honorary visiting fellow with the School of History & International Relations. He is the author of *The US-China Military & Defense Relationship during the Obama Presidency* (New York: Palgrave, 2019).

[end author bio]

The author would like to thank William Potter and his colleagues at CNS for their support and guidance in the preparation of this paper.

[87] Supplying enough power for swarms of UAVs (or UUVs) for extended periods would require significant improvements in 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. See Gates, 'Is the SSBN Deterrent Vulnerable to Autonomous Drones?'