Artificial Intelligence & Future Warfare: Implications for International Security

Abstract:
Recent developments in artificial intelligence (AI) suggest that this emerging technology will have a deterministic and potentially transformative influence on military power, strategic competition, and world politics more broadly. After the initial surge of widespread speculation in the literature related to AI this article provides some much-needed specificity to the debate. It argues that left unchecked the uncertainties and vulnerabilities created by the rapid proliferation and diffusion of AI could become a significant potential source of instability and great power strategic rivalry. The article identifies several AI-related innovations and technological developments that will likely have substantial consequences for military applications from a tactical battlefield perspective to the strategic level.

Key words: Artificial Intelligence; International Security; US-China Relations; Future Warfare

Introduction:
In the past decade, researchers have achieved significant milestones in the development of artificial intelligence (AI) and related technologies (quantum computing, big data,[1] the 'internet of things', miniaturization, and robotics and autonomy),[2] and significantly faster than the projections of experts in the field.[3] For example, in 2014 the AI expert who designed the world's best Go-playing (or AlphaGo) program predicted that it would be another ten years before a computer could defeat a human Go champion.[4] Researchers at Google's DeepMind achieved this technological feat just one year later. The principal forces driving this evolution include: (1) the exponential growth in computing performance; (2) expanded datasets;[5] (3) advances in the implementation of machine learning techniques and algorithms (especially in the field of deep neural networks); and above all, (4) the rapid expansion of commercial interest and investment in AI.[6] Since at least the Second World War, partially autonomous systems have been used in military technology, but recent advances in machine learning and AI represent a fundamental turning point in the use of cognitive solutions and automation to enhance 'battlespace

awareness. [7] AI may bring fundamental changes to military power, with the implications of a re-ordering the balance of power.[8] In particular, the geopolitical competition between China and the United States will undoubtedly be affected by the race to develop AI capabilities.

World leaders have been quick to recognize the transformative potential of AI as a critical component of national security.[9] In large part driven by the perceived challenges posed by rising revisionist and revanchist powers (especially China and Russia),[10] the U.S. Defense Department (DoD) in 2016 released a 'National Artificial Intelligence Research and Development Strategic Plan' - one of a series of studies on AI machine learning - on the potential for AI to reinvigorate U.S. military dominance.[11] According to then-U.S. Deputy Secretary of Defense Robert Work, "we can't prove it, but we believe we are at an *inflection point in AI and autonomy*".[12] The DoD also established the Defense Innovation Unit Experimental (DIUx) to foster (albeit with mixed success) closer collaboration between the Pentagon and Silicon Valley.[13] AI may bring fundamental changes to military power, with the implication of reordering the balance of power (and to a lesser extent Russia) continues to develop a range of military-use AI technologies as part of a broader strategic effort to exploit perceived U.S. military vulnerabilities.[14] In a quest to become a 'science and technology superpower,' and catalyzed by AlphaGo's victory (or China's 'Sputnik moment'), Beijing launched a national-level AI-innovation agenda for 'civil-military fusion' - or U.S. Defense Advanced Research Projects Agency (DARPA) with Chinese characteristics.[15] Russia has targeted thirty percent of its entire military force structure to be robotic by 2025. In sum, national-level objectives and initiatives demonstrate recognition by the global security community of the transformative (or military-technical revolution) potential of AI for states national security and strategic calculus.[16]

This article argues that military-use AI is fast becoming a principal potential source of instability and great power strategic competition.[17] Towards this end, the paper makes three inter-related central arguments: (1) At its current development stage, AI in isolation has few genuinely strategic effects; rather it is a potential power force multiplier and enabler for several high-tech domains - including cyberspace, autonomy and robotics, and guided missiles; (2) the uncertainties and risks surrounding the proliferation and diffusion of dual-use AI technology could worsen

international security in several ways: exacerbate existing threats, transform the nature and characteristics of these threats, and introduce new (and potentially accidental prone and unsafe) threats to the security landscape; and (3) the concomitant pursuit of AI technology by great military powers (especially the U.S. and China) will create additional incentives for strategic competition and distrust, which has potentially profound implications for international security.

While much ink has been spilled on the impact of cyberspace on deterrence and strategic stability, the potential impact of the rapid diffusion and synthesis of AI capabilities on future warfare has been lightly researched.[18] In recent years, a growing number of International Relations (IR) studies have debated a range of issues relating to the 'AI question' - especially legal, ethical, normative, economic, and technical aspects of the discourse.[19] After the initial surge of widespread speculation in the literature related to AI this paper provides some much-needed specificity to the debate. Though the article's overarching goal is to elucidate some of the consequences of recent developments in military-use AI for international security, it does not eschew the technical aspects of the discourse.

At the core of the paper's thesis is deciphering from a broad range of technologies proven capabilities and applications, from mere speculation. What is AI, and how does it differ from other technologies? What are the possible development paths and linkages between these technologies and specific capabilities (both existing and under development)? In particular, it conceptualizes recent technological developments in AI with the broader spectrum of related technologies and then connects them to specific military capabilities and doctrines. It identifies several AI-related innovations and technological developments that will likely have substantial consequences for military applications (i.e., autonomous systems, robotics, and cyber capabilities) from a tactical battlefield perspective, and up to a strategic level.[20] In combination, the competitive pressures building in AI and the increasing sophistication of deep learning will likely have a profound impact on a tactical and operational level, which will have strategic consequences.[21]

This article proceeds as follows. First, it describes the current debate and widespread speculation surrounding AI technologies, as a potential enabler and force multiplier of a broad range of military applications. Next, it defines and categorizes the main security threats posed by AI-enhanced capabilities. Having described the

existing framework of analysis, it explains how and why specific innovations and military applications will likely have a significant impact on future conflict and escalation dynamics. Second, it conceptualizes the strategic implications of AI as a critical enabler of autonomous weapon systems, in particular, robotics and the swarming technology phenomena. Specifically, it considers how recent advances in machine learning, robotics, and big-data represent a critical inflection point in the automation of technology for military applications - comparisons have been made with nuclear, aerospace, cyberspace, and biotech technology to underscore the transformative potential of AI.[22] Despite the existence of several notable naysayers, a consensus has formed amongst industry and defense experts alike that AI will have an evolutionary, if not revolutionary, impact on autonomy and future warfare.[23] This section unpacks the strategic implications of several recent trends in the evolution of AI and autonomy, in particular, it conceptualizes autonomous systems as "asymmetric" tools to use against a superior adversary, and the strategic consequences of states' co-opting the commercial sector in the development of 'dual-use' technologies.[24]

Next, it describes AI as a potentially powerful force multiplier for (defensive and offensive) cyber capabilities including: the potential threats and vulnerabilities posed by the inexorable linkages forming between digital and physical domains, and in what ways the unexplainable features of AI (or 'black box') might affect the future strategic landscape.[25] This section critically unpacks claims that AI will advantage offensive cyber operations through the development of customized payloads, and also reflects on the alternative view that AI might equally benefit defensive cyber operations, through improved network monitoring and threat identification at speed - or the nascent concept of 'counter-AI.'

Finally, the article mines a wide-range of Chinese open-sources to elucidate early Chinese thinking on military-use of AI in future warfare.[26] It describes how disruptive technologies and the shifting geopolitical landscape are fundamentally reshaping the security environment, and postulates the likely implications of these uncertain and unpredictable dynamics for U.S.-China strategic competition. This section also considers the potentially destabilizing effect of diverging U.S.-China approaches to AI innovation, which could exacerbate underlying mistrust suspicion and misperceptions. It closes with a brief discussion on the risks and trade-offs

associated with "autonomy" on the battlefield and human-machine collaboration (or 'keeping humans in the loop'),[27] and the potential ramifications of diverging approaches to these concepts on the brittle Sino-American relationship.

Defining the AI challenge for international security:

As an enabler and force multiplier of a broad range of military capabilities, AI is more akin to electricity, radios, radar, and C4ISR systems, than a "weapon" per se.[28] As a new and potentially more powerful class of technology, AI could redefine and transform the status-quo in military-use technology with unpredictable, and likely highly destabilizing, strategic implications. Even if AI-augmented weapons and systems are unable to produce better decisions than humans,[29] militaries that use AI will doubtless gain significant advantages on the battlefield (e.g., remote-sensing, situational-awareness, battlefield-maneuver, and a compressed decision-making loop), compared to those who depend on human judgment alone; in particular, in operating environments that demands endurance and rapid decision-making across multiple combat zones.

At the strategic level of decision-making, AI-enabled command and control systems will likely be able to avoid many shortcomings inherent to human strategic decision during the "fog of war" such as: the susceptibility to invest in sunk costs, skewed risk judgment, cognitive heuristics, and group-think.[30] The U.S. intelligence community, for example, is actively pursuing several publicly documented AI research projects to reduce the "human-factors burden", increase actionable military intelligence, and enhance military decision-making, and ultimately, to predict future attacks and national security threats.[31] The literature on the diffusion on military technology demonstrates: how states react to and assimilate innovations (and to other countries that choose not to adopt them) has profound implications for the global order, strategic stability, and the likelihood of war.[32]

The potential security threats posed by AI-enhanced capabilities can be grouped under three broad categories:[33] (1) digital security (e.g., spear-phishing, speech synthesis, impersonation, automated hacking, and data poisoning);[34] (2) physical security (e.g., micro-drones in swarm attacks); and (3) political security (e.g., surveillance, deception, and coercion) especially in the context of authoritarian states. While it is too early to predict precisely which AI programs will enable which

capabilities (or how these dynamics might influence the offensive or defensive balance), the general trajectory of this disruptive technology is, however, clear.[35] Just as low-cost of 'cyber weapons' has given the offense the upper hand in the cyberspace,[36] so the proliferation of cheap weaponized AI-augmented autonomous systems could lower the threshold for future drone attacks (e.g. targeted assassinations), and make attacks more difficult to attribute.[37]

Robotics and swarming technology:

Future progress in AI technology will affect robotics and autonomous capabilities in ways that could be potentially transformative for future warfare and the military balance.[38] Autonomous weapons and robotics are frequently described, alongside gunpowder and nuclear weapons, as the 'third revolution in warfare', or the "fourth-industrial revolution.[39] Several prominent researchers posit that AI has reached an inflection point where we can expect the deployment - notwithstanding the legal and ethical feasibility - of autonomous armed-unmanned aerial vehicles (UAVs) within a matter of years.[40] Former U.S. DARPA Program Manager Gill Pratt argued technological and economic trends are converging to deliver a "Cambrian Explosion" of new robotic systems.[41] That is, the unique attributes of unmanned and autonomous systems may force defense planners to recalibrate their existing approaches to deterrence, reassurance, dissuasion, and compellence to take account of the potentially revolutionary impact of AI. Underscoring the strategic significance of this trend, Director of U.S. National Intelligence Daniel Coats stated that advances in AI would "enable new military capabilities for our adversaries," especially China and Russia.[42]

These autonomous systems would, in theory, incorporate AI technologies such as visual perception, speech, and facial recognition, and decision-making tools to execute a range of (air, ground, and maritime) operations; independent of human intervention and supervision.[43] Currently, only a few weapon systems ~~that~~ choose and engage their targets without human intervention. For example, loitering attack munitions (LAMs) loiter for targets (e.g., enemy radars, ships, or tanks) based on pre-programmed targeting criteria, to destroy its target when their sensors detect an enemy's air-defence radar. Compared to cruise missiles, (designed to fulfil 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 more extended periods.[44] Currently, the only operational 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. In addition, several states are known to be developing fully autonomous weapons including China, Germany, India, Israel, Republic of Korea, Russia, and the United Kingdom. In robotics, for example, Russia has deployed several remotely piloted tanks, such as the Uran-9 and Vehar, and in 2016, China for the first time tested a guided missile from a drone via satellite link.[45]

It is expected that sophisticated AI augmented unmanned weapon systems will soon be deployed for a range of reconnaissance and strike missions. Furthermore, stealth variants of these systems will likely be used to penetrate sophisticated multi-layered air defenses, thereby endangering their deterrent effect. Autonomous weapons will also offer states additional asymmetric (especially maritime) options to project military power within the sanctuary of anti-access/area-denial contested zones.[46] Larger unmanned underwater vehicles (UUVs) could become low-cost missile platforms in their own right. Specific operations which might incorporate AI augmented unmanned weapon systems include:[47] mine clearance and mine-laying; distribution and collection of data from undersea anti-submarine sensor networks; active sonar patrolling; intelligence, surveillance, and reconnaissance; electronic warfare; resupplying missiles to manned submarines; non-combat operations (such as counterterrorism and border defense); and guidance support for missiles for over-the-horizon targeting.[48]

China's air and sea-based drones linked to sophisticated neural networks could, for example, support China's (manned and unmanned) teaming operations to monitor and control the waters in South China Seas, which could be used to impede future U.S. freedom of navigation operations. 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.[49] AI technology will, in theory, enable swarms of autonomous UAVs to accomplish a much larger variety of missions than individual human pilots; increasing their survivability in contested airspaces, and affording nations that deploy them a decisive edge over those without these capabilities. As a result, an in-depth attack by swarms of low-cost, agile, and

autonomous adversaries can *only* be defended with systems that operate with the equivalent speed, autonomy, and intelligence.[50]

The application of AI technology in electronic warfare in an increasingly complex threat environment might help thwart attempts an adversary interfering with military GPS or communications satellite signals. Miniaturized electromagnetic jammers could, for example, be used to interfere with an adversary's targeting sensors and communications, which in conjunction with cyber-attacks, might then be used to exploit, confuse, and overwhelm an adversary's defenses.[51] To be sure, the Russian military has reportedly deployed jammers to disrupt GPS-guided unmanned air vehicles in combat zones including Syria and Eastern Ukraine. The recent hardening of the U.S. Air Force's small diameter bomb (SDB) system reflects the perceived emerging threats posed to U.S. satellite-based communications systems, operating in GPS-denied environments.[52]

The integration of AI applications into early-warning (especially nuclear) systems could compress the decision-making timeframe, and accelerate the various stage of the escalate ladder to launch a missile, which would adversely affect crisis stability at a conventional and nuclear level of warfare.[53] Conceptually, at least, a state could deploy long-range conventional missile salvos supported by big data analytics, cyber capabilities, and AI-augmented autonomous weapons, and then use its missile defenses to mop-up an adversary's remaining retaliatory capabilities.[54] China's Joint Staff Department, for example, recently called for the application of big data, cyber, cloud computing, AI, to support military planning, operational decision-making, and the establishment of joint operations command system to augment and integrate these capabilities.[55] A range of autonomous ground vehicles and underwater vehicles are already in development globally, with varying degrees of success.[56] In the majority of cases, however, these technologies have yet to make the transition to operational implementation. According to one observer, many agencies developing AI-enhanced autonomous ground and underwater vehicles, "are struggling to make the leap from development to operational implementation."[57] The key risk for international security is, therefore, that geopolitical pressures compel states to use AI-enabled autonomous weapon systems before the technology underlining them is sufficiently mature - which would make these systems more susceptible to subversion. In extremis, an enemy may believe that AI is more effective than it is,

leading to erroneous and potentially escalatory decision-making.[58] To avoid situations such as this political leaders will need to proactively co-ordinate (at a military, diplomatic, industry, and academic level) as AI technology matures.

Before leaving, the Pentagon Robert Work established an algorithmic-warfare team (also known as 'Project Maven') to examine how AI might support U.S. counter-terrorism operations in Syria, and more accurately locate hidden North Korean and Russian mobile missile launchers.[59] Recent reports indicate that the DoD has also developed an early proto-type AI-driven 'missile-hunting system', designed to detect and respond to signs of preparations for a missile launch. To support these efforts the Trump administration has reportedly proposed to more than triple the funding for an AI-driven missile program.[60] Critics have highlighted the potentially high risks this program carries. Not least, that it could provoke an AI arms race with China and Russia, upset the fragile global nuclear balance, and absent adequate safeguards, commanders could risk losing control of (and possibly accelerate) the escalation ladder.[61] In the case of AI applications to target mobile missile launchers, for example, the use of AI may be strategically destabilizing "not because it works too well but *because it works just well enough to feed uncertainty.*"[62]

The uncertainty created by AI threats to strategic stability could be either the result of an adversary's exaggerated faith in its effectiveness or (and perhaps more concerning) the false belief that a particular AI capability is operationally effective when it is not. A state may, for example, becomes convinced of its ability to counter or subvert (through input manipulation, hacking, or data poisoning) an AI application and avoid retaliation, which could lead an adversary to pursue escalatory pathways - including a pre-emptive first strike.[63] In spite of U.S. reassurances, both China and Russia fear that the U.S. intends to leverage AI, in conjunction with mobile and autonomous sensor platforms, to threaten their retaliatory nuclear capacity - especially mobile ICBMs that China and Russia rely on for deterrence.[64] For example, AI software fused with big data analytics and quantum-enabled sensors could make an adversary's submarines (including those on nuclear deterrence patrols) potentially easier to locate,[65] which may lead to 'use it or lose it' situations that worsen strategic stability.[66]

Unlike nuclear weapons, autonomous weapons do not require expensive, heavily regulated, or hard to acquire raw materials. Moreover, the ubiquity and

rapidly declining unit costs of drones mean that these capabilities will become increasingly capable, autonomous, and easy to mass-produce.[67] In contrast to human-operated automation systems, ~~the recent proliferation of~~ autonomous systems will inevitably complicate the ability of states to anticipate, and attribute drone attacks.[68] These challenges will likely increase the propensity for state (and non-state) actors to deploy drones in "grey-zone" operations - to test an adversary's deterrence posture and resolve, but without tipping the threshold into warfare with a more powerful opponent.[69] Under crisis and conflict condition, these asymmetric tactics could exacerbate strategic ambiguity, erode deterrence, and increase escalation risks.[70] In 2016, for example, North Korea employed small drones to spy on South Korea's defenses that resulted in a potentially escalatory military encounter in the demilitarised zone.[71] Perceived as relatively low-risk capability with ambiguous rules of engagement, and absent robust normative and legal frameworks, autonomous weapons will become increasingly attractive as a means to erode a superior adversary's deterrence posture and resolve.[72]

According to analyst Paul Scharre: "ultra-cheap 3D-printed mini-drones could allow the United States to field billions of tiny, insect-like drones" on the future networked battlefield.[73] Autonomous systems, unlike human operators, are unable to function beyond the limits baked into their algorithmic codes; and thus, apply common sense and contextualization to the situation at hand.[74] A lone wolf low-cost drone in isolation would unlikely pose a significant threat to a U.S. F-35 stealth fighter, but hundreds of AI augmented autonomous drones in a swarming sortie might overwhelm these weapon systems; possibly rendering them redundant altogether.[75] Chinese strategists have reportedly conducted research on data-link technologies for "bee swarm" UAVs, which emphasize network architecture, navigation, and anti-jamming operations. The Russian military also plans to incorporate AI into unmanned aerial and undersea vehicles for "swarming" missions.[76] Kalashnikov, a Russian defence 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.[77] Swarms of robotic systems fused with AI machine learning could presage a powerful interplay of enhanced range, mass, coordination, intelligence, and speed in future warfare.[78]

A report by the Boston Consulting Group noted that the global spending on "military robotics" (defined as "unmanned" vehicles) increased three-fold between 2000 and 2015.[79] Several analysts have argued that due to the blurring of commercial and military-use (or dual-use) autonomous systems, this rapid growth might understate the actual impact of these increased adoption rates.[80] The historical record demonstrates, technologies that have *only* military utility and have high production costs (e.g., stealth technology), tend to diffuse at a slower pace than where economic forces are driving the process.[81] Moreover, much of the research into critical AI applications, and the degree of human-control over them are inherently dual-use in nature. To be sure, the specifications of a commercial autonomous drone used to deliver packages and explosives (e.g. improvised explosive devices), are very similar. Image recognition software designed to recognize cats on YouTube could, therefore, equally be used by remotely piloted aircraft to capture terrorist activity in Syria and Afghanistan. Of imminent concern is the ability of global militaries to field safe and reliable semi-autonomous, and later, fully autonomous versions - that for now generally do not exist.[82] In sum, the inexorable expansion in the market for low-cost autonomy and robotics, and advancements in the use and diffusion of machine learning will significantly increase the potential risks these systems pose to international security.[83]

The Cyber-AI nexus:

Several U.S. national security officials have posited that AI and machine learning will have a transformative influence on cyber domain, as force multipliers for both defensive and offensive cyber weapons.[84] The line between AI-augmented cyber-offense and cyber-defense will likely remain an obscure one, however. As a result, effective defense against attacks by sophisticated autonomous AI systems (such as a bot) will require increasingly innovative (and self-learning) solutions.[85] Director of U.S. National Intelligence Daniel Coats recently warned that AI could *increase* the vulnerability of the U.S. to cyber-attacks, weaken its ability to attribute such attacks, improve the effectiveness and capabilities of a foreign weapon and intelligence systems, and create new accident and related liability issues.[86] In other words, the development of customized payloads AI will advantage offensive cyber, but juxtaposed, through improved network monitoring and threat identification at speed;

AI will likely benefit defensive cyber operations.

On the one hand, AI could potentially reduce a military's vulnerability to cyber-attacks. While research in the field of 'counter-AI' is still at a very nascent stage, analysts have made some progress in detecting anomalies in network behavior; as a means to isolate possible exploitable vulnerabilities within machine-learning AI software. Whereas conventional cyber-defense tools search for historical matches to previous malicious code; so would be hackers only need to modify small portions of that code to circumvent this defense.[87] In contrast, early AI cyber-defense tools have been designed to recognize changes to patterns of behavior in a network and detect anomalies, thus offering a potentially higher barrier to previously unobserved attack methods.[88] On the other hand, autonomy itself may increase a military's vulnerability to a cyber-attack. An adversary could use malware to take control or manipulate the behavior of an autonomous system, which would be very difficult to detect or counter.[89] U.S. Cyber Fleet Command Commander Michael Gilday, recently told the Senate Armed Services Committee that the Navy must "improve an ability to *detect new and unknown malware* proactively…so we [the U.S.] can act quickly using advanced analytics enabled by AI and machine learning," which may give the U.S. a "tactical advantage" to identify malicious activity early on.[90] Moreover, even if analysts can obtain high-quality and reliable intelligence, they may not want to reveal it, because doing so could compromise a source, capability, or tactic.[91]

While automation allows scale, AI machine learning can facilitate the development, profiling, and accurate delivery of customized cyber-attacks (e.g., large-scale spear-phishing campaigns), for example; to shape and amplify an adversary's political narrative, cause political disruption, manipulate public opinion, and overwhelm states' cyber-defenses. [92] Recent advances in AI suggest that state and non-state cyber-attacks will soon be able to leverage machine learning for offensive operations, such as email phishing and botnet attacks.[93] Compounding these risks further, recent assessments by cyber-security experts indicate an alarmingly low-level of confidence - in contrast to cyber-offense - in the probable success of cyber-defense technologies to counter or mitigate vulnerabilities in cyber-space.[94] Given the risk of being outmatched by an adversary in cyberspace, operating at machine-speed, both AI cyber attackers and defenders will, therefore, have little option but to delegate increasingly high levels of autonomy to execute operations, or risk losing the upper-

hand in future cyber-attacks - especially attacks that cross the rubric from the virtual to the physical world.

As the linkages between digital and physical systems (or the 'Internet of Things') inevitably expand,[95] the potential to an adversary to use cyber-attacks in *both* kinetic and non-kinetic attacks will increase.[96] For example, an AI-powered self-driving car could be hacked and made to crash on a public highway. Moreover, a hacker could also target autonomous robotic systems themselves, which would cause unpredictable and potentially unmanageable errors, malfunctions, or behavioral manipulations - or 'data-poisoning.[97] Future cyber-attacks will likely target robotic control and operating systems with so-called 'weaponized software.' A significant risk variable in the operation of autonomous systems is the time that passes between a system failure (i.e., performing in a manner other than how the human operator intended), and the time it takes for a human operator to take corrective action. If the system failure is a deliberate act (i.e., hacking, spoofing or tricking), however; this timeframe will be compressed.[98] Recent explorative research into the use of non-recallable unmanned vehicles (for deterrent and coercive operations) opens the proverbial 'Pandora's Box' that relates to the efficacy of weaponized software for warfighting, not to mention the ethical and societal implications of taking humans further out of the decision-making loop.[99] Until which time researchers unravel some of the unexplainable features of AI, human error, and machine error will likely compound one-another, with unpredictable results. Simply put, we are at a critical crossroad in the parallel (and symbiotic) evolution of the AI and cyberspace that national security communities globally will need to prepare for proactively.[100]

Early research on the effects of AI on the future battlefield has tended to focus on what is *currently* known and explainable.[101] However, many aspects of the AI phenomena remain a 'black box' (i.e., beyond the comprehension of human operators). That is AI applications that use complex neural networks often generate unexpected outputs and behavior, which even their creators may misunderstand or misinterpret.[102] Though many AI programs have already surpassed human cognitive capabilities, the risk is that mistakes made by these systems - that humans would unlikely make - caused by deliberate attempts to trick or bypass machine learning applications, will prove especially difficult to anticipate or counter.[103] The question of whether AI programs will be able to accurately and objectively replicate, mimic, and

predict human behavior lies at the heart of AI research.[104] Assuming the future feasibility of general AI (or 'superintelligence'), the concerns raised by alarmists focus on issues related to AI military-use applications that may surpass human intelligence. In addition, and closely related, the possible unintended consequences and threat posed to humans as AI applications begin to define their objectives.[105] For now, defense planners must recognize that the ability of human decision-makers to mitigate extreme uncertainty during crisis and conflict conditions will be amongst the most challenging and urgent expertise to recreate in AI systems and programs.

Strategic competition & arms racing in AI:

Parallel trends in the shifting geopolitical landscape and disruptive technologies are fundamentally reshaping the security environment, which in turn, will have significant implications for how a future U.S.-China crisis or conflict might unfold.[106] At this early stage, it is difficult to predict precisely how AI might affect military force structure, organization, and defense planning. Recent evidence suggests that neither Beijing nor Washington have fully assimilated these overlapping trends into their respective military organizations, doctrines, or strategic cultures. To be sure, critics claim that a vast gulf exists within the Pentagon, between the design of AI applications and the development of operational concepts to integrate them into military doctrine.[107] The historical record has shown that in previous military revolutions the ability of militaries to assimilate and adopt new operational concepts and doctrine is a vital determinant of the ability of states' to leverage, and successfully synthesize, technologies for warfighting.[108]

Beijing's assessment of U.S. military-technological programs and initiatives heavily influenced China's initial approach to AI, in particular, those associated with the DoD's Third Offset Strategy, and more recently, 'Project Maven;' described as China's 'offsetting the offset' strategy, and involving developing technologies and related concepts such as: quantum computing; command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR); hypersonic weapons; AI machine-learning systems; human-machine collaboration; convolutional neural networks; big-data analytics; human-assisted operations; combat-teaming; and autonomous weapons.[109] As China's approach to AI matures, however, it will more likely align closer with the People's Liberation Army's (PLA's) unique organizational,

command and control, and strategic cultural traditions.[110] Beijing, like the U.S., has yet to formally articulate a coherent strategic framework, operational concepts, or the established institutions and mechanisms to support the use of AI for warfighting.[111] That said, the intensity of discussion and research within the PLA surrounding military-use AI is indicative of the high-level importance attached to this ubiquitous dual-use technology.[112]

As China and the U.S. internalize these emerging technological trends, it is likely that each side will conceptualize them very differently. Scholarship on military innovation has demonstrated that - with the possible exception of nuclear weapons - technological innovation alone rarely causes the military balance to shift; instead, *how* militaries employ a technology usually proves critical.[113] A significant cause for concern is that if the many national, cultural, and normative differences that separate Sino-American approaches to military innovation are reflected in the software used to teach AI programs, the resultant prejudices and preferences might become baked into the weapon systems they support.[114] As a result, even if AI systems are designed to produce bias-free analysis, human bias inherent in data sampling, sensor types, and other uncontrollable factors might nonetheless result in subjective decision-making.[115] Under crisis and conflict conditions, these kinds of cognitive biases might exacerbate underlying U.S.-China mutual mistrust, suspicion, and misperceptions.

In the race to innovate in AI, uncertainties surrounding U.S and China progress (and setbacks) will have profound and potentially destabilizing implications for the strategic balance.[116] For now, at least, the U.S. retains the upper-hand in AI innovation,[117] In this emerging innovation arms-race, however, China is no longer the minor party. Instead, China is fast becoming a true peer-competitor in AI and is expected to overtake the U.S. in this emerging strategic domain soon.[118] By its estimates, Beijing has set 2020 as a target to achieve ‘breakthroughs in a series of landmark AI products,' and to establish an ‘international competitive advantage' in the development of dual-use technologies and applications - especially those which target the United States.[119] To be sure, China’s innovation ambitions could be expedited by a fundamental mismatch (even dissonance) analysts have identified between the rapid pace of commercial innovation and academic research into AI and the lagging timescales and assumptions that underpin the Pentagon’s existing procurement processes and practices.[120]

Chinese centralized planning, socialist market economy, and in particular, a vast pool of data-sets, could offer Beijing significant scope to leverage China's market forces and human capital to realize its 'civil-military fusion' objective in AI.[121] While large data is an advantage, however, it remains an open question whether China's national strategic planning and socialist market economy will prove advantageous in the development of AI. According to a recent report, China is on track to possess twenty percent of the world's entire data by 2020 - and thirty percent by 2030.[122] The head of the U.S. DoD's Strategic Capabilities Office, William Roper, highlighted the pivotal role the accumulation of, and competition for, information for machine learning will play in future warfare. Roper stated: "It's *wealth and fuel*. Your data keeps working for you. You stockpile the most data that you can and *train that to teach and train autonomous systems*".[123] In contrast to the nuclear arms race that defined the Cold War-era, states competing in the AI arms race will be less concerned with sustaining the qualitative and quantitative lead in warheads, but instead more concerned with maintaining information superiority - to feed machine-learning algorithms.[124] Chinese President Xi Jinping recently stated that AI, 'big data,' cloud storage, cyberspace, and quantum communications were amongst the "liveliest and most promising areas for civil-military fusion," and towards this end, he pledged additional state support and resources.[125] In contrast, the increasingly strained relationship between the Trump administration and Silicon Valley will likely pose additional challenges to this critical partnership in the development of AI technologies for the U.S. military.[126] Following a recent high-profile backlash from employees at Google, the company recently announced that it would discontinue its work with the Pentagon on Project Maven.[127]

As a first mover AI-power, therefore, China will likely chart a course at the vanguard in the development of technical standards, mechanisms, and governance of AI that will likely strengthen the competitiveness and quality of China's military capabilities.[128] China's early approach to AI suggests a wide-reaching conceptualization that the PLA will synthesize into entire force structure; to support future 'intelligentized' operations, and seize the 'commanding heights' of future strategic competition.[129] Specifically, Chinese researchers have focused on AI applications for war-gaming, training, command, and control, intelligence analysis, and augmenting autonomous weapons systems.[130] President Xi's 'One Belt One

Road,' and the virtual dimension the 'digital Silk Road,' are high-level efforts designed to ensure that the mechanisms, coordination, and support for this agenda will become increasingly normalized.[131] Moreover, in 2017 Xi explicitly called for the acceleration of the military 'intelligentization' agenda, to better prepare China for future warfare against a near-peer adversary like the United States.[132]

China's pursuit of AI (especially dual-use capabilities) will fuel the perception (accurate or otherwise) in Washington that Beijing is intent on exploiting this strategically critical technology to fulfill its broader revisionist goals. Despite a brief pause in the development of the U.S.'s AI strategic roadmap, the White House recently announced the creation of a new committee of AI experts to advise it on policy choices.[133] In 2017, following the recommendation of the Committee on Foreign Investment in the U.S., President Trump blocked a Chinese firm from acquiring Lattice Semiconductor; a company that manufactures chips critical in the operation of AI applications.[134] This action typifies a broader concern that synergies created by China's civil-military fusion strategy could allow the technology, expertise, and intellectual property shared between American and Chinese commercial entities to be transferred to the PLA.[135]

Though Chinese strategic writings have emphasized the importance of human-machine collaboration and teaming (or keeping humans 'in the loop'),[136]The PLA's historical resistance to command and control decentralization and general mistrust of human personnel could prompt military leaders to gravitate more quickly towards full-battlefield autonomy.[137] The opposite conclusion could also be drawn, however: if Chinese commanders were unwilling to give up centralized control to junior officers, why would they give such authority to machines? Recent reports indicate China's navy is contemplating fitting its nuclear-powered submarines (and possibly nuclear-armed ones) with a so-called 'AI-augmented brainpower.[138] This capacity could, in theory, synthesize and interpret large quantities of data generated by sonar signals and sound pulses, to detect submerged objects, and support a broad range of maritime operations. To be sure, the kinds of activities and the level of autonomy afforded to AI-augmented systems to support China's strategic underwater forces will have profound implications for future crisis and conflict in the increasingly contested undersea domain. In extremis, if military command and control systems came under attack (possibly from AI-augmented cyber-weapons), military commanders may

decide to pre-delegate decision-making to machine-learning systems. Russia, for example, operates a so-called ‘dead hand' designed to launch its nuclear missiles at hyper-speed automatically, if its pressure sensors were to detect an imminent nuclear attack.[139]

The evidence suggests that China (and Russia) has relatively few moral, legal or ethical qualms in deploying lethal autonomous weapons.[140] Moreover, and in contrast to the U.S., discussion on the potential limitations and risks associated with AI, autonomy, and cyber-warfare appears mostly absent from Chinese open-sources.[141] Reports suggest that China has already begun to incorporate AI into its next-generation conventional missiles and missile-defense intelligence gathering systems, to enhance their precision and lethality.[142] By contrast, the U.S. will likely be much more constrained in the development of these technologies. Resistance within the U.S. military to incorporate AI stems in large part from the prevailing liberal-democratic norms governing the use of military force, and the growing concerns surrounding the many ‘black box’ aspects of AI-machine learning, and in particular, to avoid the so-called ‘Terminator Conundrum’ - the implications of weapons that could operate independently and beyond the control of their developers.[143]

Chinese analysts, by overlooking the potential shortcomings, uncertainties, and vulnerabilities associated with AI, and overstating (even overdramatizing) the utility of AI and autonomy (or taking humans ‘out of the loop’), could under crisis and conflict conditions complicate escalation management,[144] and worsen strategic stability in future warfare.[145] That said, given the aggressive pursuit of military-use AI by its strategic rivals, America’s current commitment to having humans in charge might waver.[146] Moreover, international law remains unclear and indeterminate on lethal autonomy, and in its absence, militaries (including the U.S.) will continue to develop weapon systems with varying degrees of autonomy.[147] Ultimately, militaries will need to consider the trade-off between the risks associated with autonomous weapons, with the possibility of affording an adversary using fully autonomous weapons the asymmetric upper hand. At this early stage, it is impossible to know for sure when, whether, and under what circumstances greater degrees of autonomy in human-machine collaboration will provide a distinct strategic battlefield advantage.

Conclusion:

The seemingly unstoppable momentum from several parallel and mutually reinforcing trends has meant that disruptive AI technologies will likely prove every bit as fraught with risk as previous transformative military innovations, perhaps even more so. The rapid proliferation, diffusion, and synthesis of AI, together with the opacity and dual-use features associated with this nascent technology, could generate a destabilizing and potentially intractable AI arms race. In sum, absent robust defenses, policies (e.g., red-teaming exercises) and norms to counter or mitigate these risks, disruptive AI technologies could negatively affect international security in three interconnected ways:[148] (1) Amplify the uncertainties and risks posed by *existing* threats (in the physical and virtual domains); (2) transform the nature and characteristics of these threats; and (3) introduce *new risks* to the security landscape.

This article makes the following core arguments. First, advanced AI-augmented unmanned (ground-based, sea-based, and stealth variants) weapon systems will soon be deployed for a range of defensive and offensive missions, which could undermine the deterrent utility of existing multi-layered defense systems. Moreover, the prospect of fusing AI (especially 'big data' analytics and quantum computing) with early-warning systems and sensors; by compressing the decision-making timeframe, and making concealed high-value military assets (e.g. submarines and nuclear launch sites) easier to find, and therefore target, could adversely impact the international security and potentially, crisis stability at a nuclear level of warfare.[149]

Second, the ubiquity and declining costs of drones will mean that these asymmetric tools will continue to proliferate at an inexorable pace; increasing the power of *both* state and non-state actors to erode (especially in swarming attacks) a superior adversary's deterrence and resolve. The rapid diffusion and dual-use features of augmented autonomous weapons, much like in cyber-space, will complicate the ability of states to anticipate, attribute, and effectively counter future autonomous attacks. As a result, the nascent development of 'counter-AI' will assume an increasingly central role in states' national security and strategic calculations. Furthermore, the relatively slow pace - and in some cases inertia - of the global defense industry's AI development vis-à-vis the commercial sector could affect the balance of power and the structure of international competition; in ways which worsen the outlook for international security.

Third, as the linkages between the digital and physical (especially the 'Internet of Things') domains increase, so the threats posed from cyber-attacks - in both the kinetic and non-kinetic domains - will grow. Moreover, machine learning will likely expand the scope and scale future cyber-attacks (e.g., large-scale spear-phishing campaigns), which may overwhelm states incipient cyber-defenses - let alone 'counter-AI' capabilities. The many unexplainable (or 'black box') features of AI will compound these risks, and further complicate defense planning for an uncertain and complex strategic landscape. For now, it remains unclear what capabilities AI will augment and enhance, whether entirely new weapons could emerge, and how these dynamics might affect the future military and strategic balance between states - and potentially between states and non-state entities.

Finally, the fast emerging U.S.-China race to innovate in AI will have profound and potentially highly destabilizing implications for future strategic stability. As both sides internalize these nascent technological trends within their respective military organizations, it is likely each side will conceptualize them very differently. In particular, Sino-American prejudices, preferences, and other cognitive biases will become hardcoded and entrenched into AI-powered weapons. Under crisis and conflict the conditions, biases of this kind might exacerbate underlying U.S.-China mutual mistrust, suspicion, and misperceptions. These technical challenges will likely heighten the perception (accurate or otherwise) within Washington that Beijing is intent on exploiting AI to fulfill its revisionist geopolitical ambitions. Chinese and Russian aggressive pursuit of military-use AI and a relatively low moral, legal, and ethical threshold in the use of lethal autonomous weapons, may prompt the U.S. to shift from its current pledge to keep 'humans in the loop,' which would intensify the emerging arms-race in AI and adversely affect international security.

Future scholarship would be beneficial on the following issues: What norms from other dual-use domains apply to, and have potential implications for, AI? What unique challenges and risks (if any) does AI pose as a dual-use technology? In a world of rapidly evolving and defenses, how should the trade-offs between resource demands, accuracy, and robustness, be prioritized and managed attacks? Is there an equivalent of 'patching' for AI systems? How effective would exit ramps and firebreaks are in managing the escalation and disruptive technologies? Finally,

China's progress in multiple military applications of AI merits continued scholarly attention and scrutiny.

Notes:

[1] I. Emmanuel, and C. Stanier, (2016). "Defining Big Data," in *Proceedings of the International Conference on Big Data and Advanced Wireless Technologies* (New York, NY: ACM, 2016).
[2] Artificial intelligence (AI) refers to computer systems capable of performing tasks requiring human intelligence, such as: visual perception, speech recognition, and decision-making. These systems have the potential to solve tasks requiring human-like perception, cognition, planning, learning, communication or physical action
[3] Recent progress in AI falls within two distinct fields: (1) 'narrow' AI, and specifically, machine learning; (2) 'general' AI, which refers to AI with the scale and fluidity akin to the human brain. 'Narrow' AI is already in wide use for civilian tasks. Most AI researchers anticipate that 'general' AI to be at least several decades away.
[4] 'Go' is a board game, popular in Asia, with an exponentially greater mathematical and strategic depth than chess.
[5] 'Machine learning' is a concept that encompasses a wide variety of techniques designed to identify patterns in, and learn and make predictions from data sets.
[6] Greg Allen and Taniel Chan, *Artificial Intelligence and National security*. (Cambridge, MA: Belfer Centre for Science and International Affairs, 2017).
[7] The U.S. DoD defines 'battlespace awareness' as a capability area where unmanned systems in all domains can contribute significantly into the future to conduct intelligence, surveillance, and reconnaissance (ISR) and environment collection related tasks.
[8] For a history of AI and the military see, Kareem Ayoub and Kenneth Payne, 'Strategy in the Age of Artificial Intelligence,' *Journal of Strategic Studies* 39, no. 5-6 (2016), pp.799-805.
[9] Robert O. Work, *Remarks by Defense Deputy Secretary Robert Work at the CNAS Inaugural National Security Forum, Speech, CNAS Inaugural National Security Forum*, (Washington, D.C.: CNAS, July 2015).
[10] Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China, 2017* (U.S. Department of Defense, Washington, D.C., 2017), https://www.defense.gov/Portals/1/Documents/pubs/2017_DoD_China_Report.pdf
[11] National Science and Technology Council, *The National Artificial Intelligence Research and Development Strategic Plan,* (Executive Office of the President of the United States, Washington, D.C., October 2016), https://www.nitrd.gov/PUBS/national_ai_rd_strategic_plan.pdf
[12] Recent defence initiatives that have applied deep-learning techniques to autonomous systems include: the U.S. Air Force Research Laboratory's (AFRL's) Autonomous Defensive Cyber Operations (ADCO); National Geospatial Agency's (NGA's) Coherence Out of Chaos program (deep-learning-based queuing of satellite data for human analysts); and Israel's Iron Dome air defence system. Reagan *Defense Forum: The Third Offset Strategy*, (Washington, D.C., U.S. Department of Defense. November 7, 2015), https://dod.defense.gov/News/Speeches/Speech-View/Article/628246/reagan-defense-forum-the-third-offset-strategy/
[13] Fred Kaplan, "The Pentagon's Innovation Experiment," *MIT Technology Review,* 16 December 2016, https://www.technologyreview.com/s/603084/the-pentagons-innovation-experiment/
[14] In addition to AI, China, and Russia have also developed other technologically advanced (and potentially disruptive) weapons such as: cyber warfare tools; stealth and counter-stealth technologies; counter-space; missile defense; and guided precision munitions.
[15] The State Council Information Office of the People's Republic of China, "State Council Notice on the Issuance of the New Generation AI Development Plan," July 20, 2017, http://www.gov.cn/zhengce/content/2017-07/20/content_5211996.htm.
[16] A military-technical revolution (MTR) has is associated with periods of sharp, discontinuous change

make redundant or subordinate existing military regimes; or the most common means for conducting war.

[17] 'Strategic Stability' as a concept in IR has been defined in many ways. At the heart of strategic stability is limiting the incentives for states to launch a first nuclear strike, and thus, reducing the conditions under which countries face pressures to escalate a conflict. Non-nuclear technologies with strategic effects (such as AI) have the potential to disrupt these risks adversely. For a history and analysis on "strategic stability," see Colby Elbridge and Michael Gerson. Eds., *Strategic Stability: Contending Interpretations* (Carlisle, PA: Army War College, 2013).

[18] Notable exceptions include: Patrica Lewis and Unal Beyza, "Cybersecurity of nuclear weapons systems: Threats, vulnerabilities and consequences," (London: Chatham House, 2018); Mary L. Cummings, "Artificial intelligence and the future of warfare," (London, UK: Chatham House, 2017); Lawrence Freedman, *The future of war* (London: Penguin Random House, 2017); Lucas Kello, *The virtual weapon and international order* (New Haven: Yale University Press, 2017); Pavel Sharikov, "Artificial intelligence, cyberattack, and nuclear weapons - A dangerous combination," *Bulletin of the Atomic Scientists*, 74 no. 6, (2018), pp.368–373; Ayoub and Payne, "Strategy in the Age of Artificial Intelligence," pp.793-819.

[19] See, Greg Allen and Taniel Chan, *Artificial intelligence and national security* (Cambridge, MA: Belfer Center for Science and International Affairs, 2017), Max Tegmark, *Life 3.0*. (London: Penguin Random House*,* 2017); Adam Segal*, Conquest in cyberspace: National security & information warfare* (New York: Cambridge University Press, 2015). For a recent technical study on autonomous weapons systems see, Jeremy Straub, "Consideration of the use of autonomous, non-recallable unmanned vehicles and programs as a deterrent or threat by state actors and others," *Technology in Society,* Vol. 44, (February 2016), pp.1-112.

[20] Ayoub and Payne, "Strategy in the Age of Artificial Intelligence," pp.793-819.

[21] For example, in 1988 the targeting system of a U.S. Aegis-equipped destroyer - set to semi-automatic mode - mistakenly targeted and destroyed an Iranian civilian airliner, having identified it as an incoming F-14 fighter. Peter Singer, *Wired for War: The Robotics Revolution and Conflict in the Twenty-first Century* (London: Penguin, 2009), pp.124-5.

[22] Greg Allen and Taniel Chan, *Artificial intelligence and national security* (Cambridge, MA: Belfer Center for Science and International Affairs, 2017) https://www.belfercenter.org/sites/default/files/files/publication/AI%20NatSec%20-%20final.pdf

[23] Daniel S. Hadley and Lucas J. Nathan, *Artificial intelligence and national security*, (Congressional Research Service, Washington, D.C., 2017) https://fas.org/sgp/crs/natsec/R45178.pdf

[24] 'Dual use' refers to the military or commercial use of technologies. In case of AI and autonomous systems, defense and commercial enterprises compete for virtually the same talent pool and use similar infrastructure and hardware to support these efforts. 'Asymmetry' in this context refers to the relatively low-cost and ubiquity of autonomous weapon systems, and the utility of these weapons against a more powerful adversary.

[25] 'Black box' in this context refers to the idea that we can understand the inputs and outputs of AI-driven applications, but that many aspects of how the technology works and makes decisions are not clearly understood - even by their designers.

[26] The article engages with the following (authorized and semi-authorized) Chinese-language sources: (1) publications by China's leading military research institutions (e.g. China Electronics Technology Group Corporation); (2) authorized military-doctrinal publications (e.g. the *Academy of Military Studies, Military Science Press*); (3) official Chinese-military press (e.g. PLA Daily); and (4) other journals and media outlets that report on national security issues (e.g. *Strategic Air Force, Xinhua,* and *Caixin*). The author is responsible for all translations that result from the mining of Chinese-language sources documents for this paper.

[27] 'Autonomy' in this context refers to a system that reasons probabilistically are given a set of inputs, meaning that it makes predictions and assumptions about best possible courses of action given sensor data input.

[28] For analysis on the idea of 'technology' as a force multiplier and enabler of a broad class of advanced weapons see, James S. Johnson, *The US-China Military and Defense Relationship during the Obama Presidency,* (New York, NY: Palgrave Macmillan, 2018), chap. 4.

[29] In contrast to human decision-makers cognitive stressors, time pressures, and other physical effects of combat (such as lack of glucose and fatigue), do not adversely affect AI systems. Ayoub and Payne, "Strategy in the Age of Artificial Intelligence," pp.793-819.
p.798.

[30] Ben Connable, *Embracing the Fog of War: Assessment and Metrics in Counterinsurgency*, (Santa

Monica, CA: RAND Corporation, 2012).
[31] Patrick Tucker, "What the CIA's Tech Director Wants from AI," *Defense One*, September 6, 2017, https://cdn.defenseone.com/b/defenseone/interstitial.html?v=8.20.0&rf=https%3A%2F%2Fwww.defenseone.com%2Ftechnology%2F2017%2F09%2Fcia-technology-director-artificial-intelligence%2F140801%2F
[32] See, Michael C. Horowitz, *The Diffusion of Military Power: Causes and Consequences for International Politics,* (NJ: Princeton University Press, 2010); Gregory D. Koblentz, *Council special report-strategic stability in the second nuclear age*, (NY: Council on Foreign Relations Press, 2014).
[33] Center for a New American Security, University of Oxford, University of Cambridge, Future of Humanity Institute, OpenAI & Future of Humanity Institute, *The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation*, (Oxford, UK: Oxford University, February 2018 https://arxiv.org/pdf/1802.07228.pdf
[34] These AI vulnerabilities are, however, distinct from traditional software vulnerabilities (e.g., buffer overflows), and demonstrate that while AI systems may exceed human performance, they often fail in unpredictable ways that a human never would.
[35] 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).
[36] 'Cyber weapons' can best be defined as a computer program designed to compromise the integrity (or availability) of data in an adversary's IT network for military purposes. Joseph J. Nye, "Deterrence and Dissuasion in Cyberspace", *International Security,* 41, no. 3 (2017), pp.44-71.
[37] The ability of states to attribute a drone attack will depend in part on how homogeneous drone technology becomes, and in particular, the use of these weapons by non-state actors.
[38] State Council pp.12-13.
[39]" To date, only the United States, United Kingdom, and Israel have reportedly used armed drones operationally; other states, however, have expressed an interest in developing this capacity - notably, China, Germany, Italy, and France. However, no nation has formally stated an intention to build entirely autonomous weapon systems.
[40] The moral and ethical considerations related to the use of autonomous control weapons and autonomous targeting is complex and highly contested; humans creating technology to an attack humans is inherently problematic. See, Heather Roff, *Autonomy, Robotics, and Collective Systems*, (Geneva: Centre for Security Policy, 2016) https://globalsecurity.asu.edu/robotics-autonomy/
[41] Robotic 'Cambrian Explosion' is an analogy to the history of life on Earth in which the pace of evolutionary change, for both diversity and complexity of life forms, increased significantly. Gill Pratt, "Is a Cambrian Explosion Coming for Robotics?**"** *Journal of Economic Perspectives* 29, no. 3 (2015), pp.51-60.
[42] Daniel R. Coats, Director of national intelligence, U.S. Office of the Director of National Security, "Statement for the Record Worldwide Threat Assessment of the US intelligence Community Senate select committee on intelligence," 11 May 2017, https://www.dni.gov/files/documents/Newsroom/Testimonies/SSCI%20Unclassified%20SFR%20-%20Final.pdf
[43] The U.S. 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.
[44] Edward Geist and Andrew Lohn, *How might artificial intelligence affect the risk of nuclear war?* (Santa Monica, CA: RAND Corporation, 2018).
[45] Samuel Bendett,"Get Ready, NATO: Russia's New Killer Robots are Nearly Ready for War." *The National Interest.* March 7, 2017, https://nationalinterest.org/blog/the-buzz/russias-new-killer-robots-are-nearly-ready-war-19698; Tair Eshel, "China Tested an Upgraded CH-4 "Rainbow" Weaponized Drone," *Defense Update*, June 5, 2016, https://defense-update.com/20160605_improved_ch-4_rainbow.html
[46] The PLA has incorporated a range of advanced UAVs into all four services of its force structure.
[47] James S. Johnson, "Washington's perceptions and misperceptions of Beijing's anti-access area-denial (A2-AD) 'strategy': Implications for military escalation control and strategic stability," *The Pacific Review*, 30 no. 3, (2017), pp.271-288. Russia's expanding A2/AD capability has received less attention than China's, but these capabilities pose similar strategic challenges to America and its allies. See, Richard Fontaine and James N. Miller, *A new era in U.S.-Russian strategic stability* (Washington, D.C.: Centre for a New American Security, 2017).

[48] Given the comparative lack of complex human interaction and society, the maritime and air power domains are considered more susceptible to AI - relative to ground force dominant urban warfare. Ayoub and Payne, "Strategy in the Age of Artificial Intelligence," p.806.
[49] Kristin Huang, "China starts work on world's biggest test site for drone ships at gateway to South China Sea," *South China Morning Post,* 12 February 2018 https://www.scmp.com/news/china/diplomacy-defence/article/2133076/china-starts-work-worlds-biggest-test-site-drone-ships
[50] Ayoub and Payne, "Strategy in the Age of Artificial Intelligence," pp.806-807.
[51] As Russia discovered in Syria, a combination of traditional short-range defenses and electronic warfare systems, even a modestly sized swarm, is not sufficient to guarantee the destruction of all of the drones used in an attack.
[52] The small diameter bomb (SDB) system is the U.S. Air force's next generation of low-cost and low collateral-damage precision strike weapons for internal and external carriage. Sandra I. Erwin, "Army turns to artificial intelligence to counter electronic attacks," Spacenews.com, 29 August 2018 https://spacenews.com/army-turns-to-artificial-intelligence-to-counter-electronic-attacks/
[53] 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).
[54] Paul Scharre, *Autonomous weapons, and operational risk - Ethical autonomy project* (Washington, D.C.: Centre for a New American Security, 2016), p.33.
[55] Elsa Kania, *Battlefield singularity: Artificial intelligence, military revolution, and China's future military power,* (Washington, D.C.: Centre for a New American Security, 2017).
[56] Mary L. Cummings, *Artificial intelligence and the future of warfare*, (London, UK: Chatham House, 2017), pp.8-9.
[57] Ibid.
[58] Edward Geist and Andrew Lohn, *How might artificial intelligence affect the risk of nuclear war?* (Santa Monica, CA: RAND Corporation, 2018), p.21.
[59] Marcus Weisgurber, "The Pentagon's New Algorithmic Warfare Cell Gets Its First Mission: Hunt ISIS", *Defense One,* May 14, 2017, https://www.defenseone.com/technology/2017/05/pentagons-new-algorithmic-warfare-cell-gets-its-first-mission-hunt-isis/137833/
[60] Phil Stewart, "Deep in the Pentagon, a secret AI program to find hidden nuclear missiles", *Reuters,* 5 June 2018 https://www.reuters.com/article/us-usa-pentagon-missiles-ai-insight/deep-in-the-pentagon-a-secret-ai-program-to-find-hidden-nuclear-missiles-idUSKCN1J114J
[61] Pavel Sharikov, "Artificial intelligence, cyberattack, and nuclear weapons - A dangerous combination," *Bulletin of the Atomic Scientists*, 74 no. 6, (2018), pp.368–373.
[62] Advances in AI ISR and analysis systems could mitigate some of the uncertainties associated with tracking and targeting mobile nuclear missile launchers and make them more vulnerable to pre-emptive attacks. Edward Geist and Andrew Lohn J, *How might artificial intelligence affect the risk of nuclear war?* (Santa Monica, CA: RAND Corporation, 2018), p.15.
[63] Ibid. pp.19-20.
[64] Ibid. p.9.
[65] China is a latecomer to quantum computing. In the past few years, however, Chinese researchers have become serious contenders in this field; a sector long dominated by the U.S. For example, China's 'New Generation AI Development Plan' incorporates quantum-accelerated machine learning.
[66] Edward Geist and Andrew Lohn J, *How might artificial intelligence affect the risk of nuclear war?* (Santa Monica, CA: RAND Corporation, 2018).
[67] 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*, January 12, 2017, https://www.defenseone.com/technology/2017/01/drones-isis/134542/
[68] For national security reasons states usually employ drones with tell-tale signatures. In the case of non-state drone attacks, these signatures are not available.
[69] 'Grey-zone' (or hybrid) warfare refers to a metaphorical state between war and peace, where an aggressor aims to reap either political or territorial gains associated with overt military aggression without crossing the threshold of open conflict with a powerful adversary.
[70] In conflict and crises arms racing, escalation pressures, temptations to strike first, deterrence failure, and so forth, are invariably interrelated.
[71] "Seoul Fires Warning Shots at 'North Korea Drone,'" *Sky News*, January 13, 2016, http://news.sky.com/story/seoul-fires-warning-shots-at-north-korea-drone-10128538
[72] Paul Scharre, *Autonomous weapons, and operational risk - Ethical autonomy project,* (Washington, D.C.: Center for a New American Security, 2016).

[73] Paul Scharre, *Robotics on the Battlefield Part II: The Coming Swarm*, (Washington, D.C.: Center for a New American Security, 2014).
[74] Future 'general' AI systems could consider the broader context and adapt to novel situations. Though theoretical at this stage, the introduction of these 'superintelligent' systems would create potentially greater risks and operational challenges for militaries. For analysis of the possible risks associated with 'general' AI see, Nick Bostrom, *Superintelligence: Paths, Dangers, Strategies* (Oxford: Oxford University Press, 2014).
[75] "Highlighting Artificial Intelligence: An Interview with Paul Scharre," *Strategic Studies Quarterly*, Vol. 11, Issue 4, (November 2017), pp.18-19.
[76] 'Swarming' in this context can be defined as: engaging an adversary either with fire or in force in simultaneous multi-directional strikes that do not rely on central control, but instead respond to cues from their environment.
[77] Tristan Greene, "Russia is Developing AI Missiles to Dominate the New Arms Race," *The Next Web*, July 27, 2017, https://thenextweb.com/artificial-intelligence/2017/07/27/russia-is-developing-ai-missiles-to-dominate-the-new-arms-race/
[78] For example, commanders could attack an enemy's sensors and control systems to degrade their integrated air-defense systems, as a precursor for deploying swarms of UAVs and long-range stealth bombers.
[79] Alison Sander and Mel Wolfgang, "BCG Perspectives: The Rise of Robotics," *The Boston Consulting Group*, August 27, 2014, http://image-src.bcg.com/Images/The_Rise_of_Robotics_Aug_2014_tcm9-82495.pdf
[80] See, Robert O. Work, Shawn W. Brimley. 2014 *20YY Preparing for War in the Robotic Age*, Center for a New American Security, Washington, pp.5-10.
[81] See, Michael C. Horowitz, *The Diffusion of Military Power: Causes and Consequences for International Politics,* (NJ: Princeton University Press, 2010).
[82] Mary L. Cummings, *Artificial intelligence and the future of warfare*, (London, UK: Chatham House, 2017).
[83] The pace of military-use AI diffusion to other states and non-state entities will likely be constrained, however, by three major aspects related to this phenomena: (1) Hardware constraints (i.e. physical processors); (2) the algorithmic complexity inherent to Deep learning; and (3) the resources and know-how to effectively deploy AI code. Ayoub and Payne, "Strategy in the Age of Artificial Intelligence," p.809.
[84] Most defense analysts agree that cyber-warfare is 'offensive-dominant' in nature. See, David Gompert, Martin Libicki, and Lawrence Cavaiola, "Cyber House Rules: On War, Retaliation and Escalation," *Survival,* 57 no. 1, (2015), pp.81-104. For an opposing view see, Thomas Rid, "Think Again: Cyberwar," *Foreign Policy,* March/April 2012 https://foreignpolicy.com/2012/02/27/think-again-cyberwar/
[85] Pavel Sharikov, "Artificial intelligence, cyberattack, and nuclear weapons - A dangerous combination," *Bulletin of the Atomic Scientists*, 74 no. 6, (2018), pp.368–373.
[86] Carolyn Bartholomew and Dennis Shea, *U.S.-China Economic and Security Review Commission - 2017 Annual Report*, (Washington, D.C.: The U.S.-China Economic and Security Review Commission, 2017), p.534.
[87] Scott Rosenberg, "Firewalls Don't Stop Hackers, AI Might," *Wired*, August 27, 2017, https://www.wired.com/story/firewalls-dont-stop-hackers-ai-might/
[88] Deep learning boosts the ability of machines to extract salient features from a landscape or image, which may be used for classification and pattern recognition. Ayoub and Payne, "Strategy in the Age of Artificial Intelligence," p.804.
[89] For example, the difficulty analysts faced in detecting malware that infected a UAV's control system at the Creech U.S. Air Force Base in Nevada. Noah Shachtman, "Exclusive: Computer virus hits U.S. drone fleet," *Wired*, 7 Oct 2011, https://www.wired.com/2011/10/virus-hits-drone-fleet/
[90] Kevin Osborn, "Navy Cyber War Breakthrough - AI Finds Malware in Encrypted Traffic," *Warrior Maven,* 15 May 2018 https://defensemaven.io/warriormaven/cyber/navy-cyber-war-breakthrough-ai-finds-malware-in-encrypted-traffic-HpglPohphEaP01z5u0-7jA/
[91] Martin Libicki, *Cyberspace in Peace and War*, (Annapolis: Naval Institute Press, 2016).
[92] For instance, Russia used bot-based strategies during the 2016 U.S. presidential election and the Syrian civil war. Several Chinese technology companies (e.g., iFlyTek) also have capabilities for spoofing and broader psychological cyber operations.
[93] Sixty-two percent of respondents at a recent 'Black Hat' conference believed that within a year AI would be deployed in cyber-attacks. The Cylance Team, "Black Hat Attendees See AI As Double-

Edged Sword," *The Threat Vector*, August 1, 2017, https://threatvector.cylance.com/en_us/home/black-hat-attendees-see-ai-as-double-edged-sword.html

[94] Michael Viscuso, *Carbon Black*, "Beyond the Hype: Security Experts Weigh in on Artificial Intelligence, Machine Learning, and Non- Malware Attacks," March 28, 2017, https://www.carbonblack.com/2017/03/28/beyond-hype-security-experts-weigh-artificial-intelligence-machine-learning-non-malware-attacks/

[95] 'The Internet of Things' is the interconnectivity between physical objects, such as a smartphone or electronic appliance, via the Internet that allows these objects to collect and share data.

[96] A recent survey reported that seventy percent of IoT devices lack even basic security safeguards. The 2016 DoS attack on Dyn that brought down high-profile websites such as Twitter and Netflix was thought to be caused by the. Michael Chui, Markus Löffler, and Roger Roberts, "The Internet of Things," *McKinsey Quarterly,* March 2010 https://www.mckinsey.com/industries/high-tech/our-insights/the-internet-of-things

[97] Andy Greenberg, "Hackers Remotely Kill a Jeep on the Highway-With Me in It." *Wired*, July 21, 2015 https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

[98] During the 2003 invasion of Iraq, for example, a Patriot missile that shot down a British jet - and killing both crewmen - was caused by the failure of humans in the loop to override an erroneous automated decision to fire.

[99] Jeremy Straub, "Consideration of the use of autonomous, non-recallable unmanned vehicles and programs as a deterrent or threat by state actors and others," *Technology in Society,* Vol. 44, (February 2016), pp.1-112.

[100] George Dvorsky, "Hackers Have Already Started to Weaponize Artificial Intelligence," *Gizmodo*, November 9, 2017, https://gizmodo.com/hackers-have-already-started-to-weaponize-artificial-in-1797688425

[101] David Gunning, "Explainable Artificial Intelligence (XAI)," *Defense Advanced Research Projects Agency*, August 11, 2016, http://www.darpa.mil/program/explainable-artificial-intelligence

[102] The challenge of complexity is even more difficult for cutting-edge AI systems that use neural networks - in addition to rule-based systems. Paul Scharre, *Autonomous weapons, and operational risk - Ethical autonomy project*, (Washington, D.C.: Centre for a New American Security, 2016), p.17.

[103] James Vincent, "Magic AI: These are the Optical Illusions that Trick, Fool, and Flummox Computers," *The Verge*, April 12, 2017, https://www.theverge.com/2017/4/12/15271874/ai-adversarial-images-fooling-attacks-artificial-intelligence

[104] Mary L. Cummings, *Artificial intelligence and the future of warfare*, (London, UK: Chatham House, 2017).

[105] Without knowing with certainty the utility of general AI applications, it is therefore impossible to anticipate what might satisfy these systems in terms of its pre-set goals. See, Nick Bostrom, "Ethical Issues in Advanced Artificial Intelligence," in *Science Fiction and Philosophy: From Time Travel to Superintelligence,* ed. Susan Schneider (Oxford: John Wiley & Sons, 2009), pp.277-286.

[106] For a recent study on U.S.-China strategic relations see James S. Johnson, *The US-China Military and Defense Relationship during the Obama Presidency,* (New York, NY: Palgrave Macmillan, 2018).

[107] Andrew Ilachinski, *AI, Robots, and Swarms - Issues, Questions, and Recommended Studies,* (Washington, D.C.: CNA Analysis and Solutions, 2017), xvi.

[108] Michael C. Horowitz, *The Diffusion of Military Power: Causes and Consequences for International Politics,* (NJ: Princeton University Press, 2010).

[109] China's long-standing approach to military innovation has been based on a 'leap-frogging' strategy; designed to encourage civil-military collaboration in the development of asymmetric dual-use capabilities.

[110] James S. Johnson, *The US-China Military and Defense Relationship during the Obama Presidency,* (New York, NY: Palgrave Macmillan, 2018), chap. 4.

[111] For a recent study on Chinese approaches to weapon system-related operational concepts see, Jeffrey Engstrom, *Systems confrontation and system destruction warfare*, (Santa Monica, CA: RAND Corporation, 2018).

[112] "National People's Congress Representative Liu Guozhi: Artificial Intelligence Will Accelerate the Process of Military Transformation," *PLA Daily*, March 7, 2017 http://jz.chinamil.com.cn/zhuanti/content/2017-03/07/content_7517615.htm/

[113] See, Barry R. Posen, *The sources of military doctrine: France, Britain, and Germany between the world wars,* (Ithaca, NY: Cornell Studies in Security Affairs, 1986).

[114] For example, Microsoft's racist 'Chatbot Tay' is the most infamous example of this kind of prejudice displayed based on the data and parameters used by developers.

[115] However, if future AI can collect and categorize its data via sensors, then the susceptibility of machines to human biases will likely decrease. For a history of AI and the military see, Ayoub, and Payne, "Strategy in the Age of Artificial Intelligence," pp.793-819.
[116] China and the United have developed the capability to leverage AI to achieve asymmetric combat advantages, but its use will also introduce new vulnerabilities. Moreover, there will likely be continued obstacles to the effective sharing, acquisition, and fielding of AI systems for military applications.
[117] The U.S. leads China in the number of AI patent applications, the number of AI-related organizations, the amount of funding provided, but China is rapidly closing this gap.
[118] International Institute for Strategic Studies (IISS), *The military balance, 2018*, (London, UK: IISS, 2018), pp.10-13.
[119] From 2014, China has surpassed the United States in the output of published research papers on deep learning - by circa 20 percent in 2016 alone. While increases in the quantity of AI-related publications do not necessarily correspond to advances in quality, this trajectory nonetheless, clearly demonstrates that China is firmly committed to its AI development agenda.
[120] Andrew Ilachinski, *AI, Robots, and Swarms - Issues, Questions, and Recommended Studies*, (Washington, D.C.: CNA Analysis and Solutions, 2017), xiv.
[121] Beijing's approach to AI is, however, far from perfect. Chinese state-led resource management characterized as inefficient and intrinsically corrupt (with government-favored research institutions receiving a disproportionate share of state-funding) might cause the government to misallocate resources, over-invest in non-productive and poorly conceptualized AI projects.
[122] In contrast, between 2012-2017 U.S. DoD expenditure on AI-related contracts was relatively flat. Govini, "Department of Defense Artificial Intelligence, Big Data, and Cloud Taxonomy," December 3, 2017, 9, available at http://www.govini/home/insights/
[123] Patrick Tucker, "The Next Big War Will Turn on AI, Says US Secret-Weapons Czar," *Defense One*, 28, March 2017 https://www.defenseone.com/technology/2017/03/next-big-war-will-turn-ai-says-pentagons-secret-weapons-czar/136537/
[124] Pavel Sharikov, "Artificial intelligence, cyberattack, and nuclear weapons - A dangerous combination," *Bulletin of the Atomic Scientists*, 74 no. 6, (2018), p.370.
[125] For example, in collaboration with Baidu, Beijing established a 'National Engineering Laboratory of Deep Learning Technology' initiative. Robin Li, "China brain project seeks military funding as Baidu makes artificial intelligence plans," *South China Morning Post,* 3 March 2015 https://www.scmp.com/lifestyle/article/1728422/china-brain-project-seeks-military-funding-baidu-makes-artificial
[126] For example, when Google acquired DeepMind, it specifically prohibited the use of its research for military purposes. Loren DeJonge Schulman, Alexandra Sander, and Madeline Christian, "The Rocky Relationship Between Washington & Silicon Valley: Clearing the Path to Improved Collaboration," (Washington, D.C.: CNAS, July 2015).
[127] Jeremy White, "Google Pledges not to work on weapons after Project Maven backlash," *The Independent,* 7 June 2018 https://www.independent.co.uk/life-style/gadgets-and-tech/news/google-ai-weapons-military-project-maven-sundar-pichai-blog-post-a8388731.html
[128] Given the lack of empirical open-sources that relates to the Chinese view on military applications of AI, this paper highlights some of the critical observable trends and proffers areas for future research that relates to these issues.
[129] "National People's Congress Representative Liu Guozhi: Artificial Intelligence Will Accelerate the Process of Military Transformation, *PLA Daily*, March http://jz.chinamil.com.cn/zhuanti/content/2017-03/07/content_7517615.htm/
[130] Shou Xiaosong, ed., *The Science of Military Strategy*, 3rd ed., (Beijing: Military Science Press, 2013).
[131] China's recent five-year plan reportedly committed over USD$100 billion to AI. Moreover, as China moves forward with its One Belt One Road related projects that extend to potentially more than eighty countries AI would become an integral part of these international infrastructure projects. Wenyuan Wu, "China's Digital Silk Road: Pitfalls Among High Hopes," *The Diplomat,* 3 November 2017 https://thediplomat.com/2017/11/chinas-digital-silk-road-pitfalls-among-high-hopes/
[132] "Xi Jinping's Report at the 19th Chinese Communist Party National Congress", *Xinhua*, October 27, 2017, http://www.china.com.cn/19da/2017-10/27/content_41805113_3.htm
[133] Aaron Boyd, "White House Announces Select Committee of Federal AI Experts," *Nextgov,* May 10, 2018, https://www.nextgov.com/emerging-tech/2018/05/white-house-announces-select-committee-federal-ai-experts/148123/

[134] Ana Swanson, "Trump Blocks China-Backed Bid to Buy U.S. Chip Maker," *The New York Times*, September 13, 2017, https://www.nytimes.com/2017/09/13/business/trump-lattice-semiconductor-china.html
[135] Carolyn Bartholomew and Dennis Shea, *U.S.-China Economic and Security Review Commission - 2017 Annual Report,* (Washington, D.C.: The U.S.-China Economic and Security Review Commission, 2017), p.507.
[136] 'Keeping humans in the loop' refers to maintaining human control of autonomous weapons; both in the design of the rules that govern these systems, and the execution of those rules when firing. That said, human decision-making and automation are not necessarily mutually exclusive. For example, the human-machine teaming cognitive design envisaged by the Pentagon, in theory at least, could leverage the predictability, reliability, and speed of full-automation while retaining the robustness and flexibility of human intelligence.
[137] For a recent comprehensive examination of the PLA's shortcomings see, Michael S. Chase, Jeffrey Engstrom, Tai Ming Cheung, Kirsten A. Gunness, Scott W. Harold, Susan Puska, and Samuel K. Berkowitz, *China's incomplete military transformation- assessing the weaknesses of the people's liberation army (PLA),* (Santa Monica, CA: RAND Corporation, 2015).
[138] Stephen Chen, "China's plan to use artificial intelligence to boost the thinking skills of nuclear submarine commanders," *South China Morning Post,* 4 February 2018 https://www.scmp.com/news/china/society/article/2131127/chinas-plan-use-artificial-intelligence-boost-thinking-skills
[139] Richard Fontaine and James N. Miller, *A new era in U.S.-Russian strategic stability* (Washington, D.C.: Centre for a New American Security, 2017), p.26.
[140] To date, there have been few publications on the legal and ethical implications for military-use AI, which have dominated the discourse in the West. Samuel Bendett, "Get Ready, NATO: Russia's New Killer Robots Are Nearly Ready for War," *The National Interest*, November 8, 2017, https://nationalinterest.org/blog/the-buzz/russias-new-killer-robots-are-nearly-ready-war-19698
[141] For example, James S. Johnson, *The US-China Military and Defense Relationship during the Obama Presidency,* (New York, NY: Palgrave Macmillan, 2018), chap. 4.
[142] Elsa Kania. *Battlefield singularity: Artificial intelligence, military revolution, and China's future military power,* (Washington, D.C.: Centre for a New American Security, 2017).
[143] Colin Clark, "'The Terminator Conundrum:' VCJCS Selva On Thinking Weapons," *Breaking Defense*, January 21, 2016, https://breakingdefense.com/2016/01/the-terminator-conundrum-vcjcs-selva-on-thinking-weapons/
[144] For example, whilst much has been written by Chinese analysts on the Pentagon's Third Offset Strategy programs (including AI) there has been very little discussion on the potential limitations of these advanced systems - including those associated with reducing human control.
[145] Edward Geist and Andrew Lohn J, *How might artificial intelligence affect the risk of nuclear war?* (Santa Monica, CA: RAND Corporation, 2018), p.5.
[146] It remains unclear, however, what operational contexts and applications, and to what degree China and Russian might pursue fully autonomous weapon systems.
[147] Kelsey Atherton, "3 big takeaways from the Navy's new robot road map", *C4ISRnet,* 30 May 2018 https://www.c4isrnet.com/unmanned/2018/05/30/three-big-takeaways-from-the-navys-new-robot-roadmap/
[148] DARPA's Cyber Grand Challenge demonstrated the potential power of AI cyber-defense tools. "Mayhem Declared Preliminary Winner of Historic Cyber Grand Challenge," *Defense Advanced Research Projects Agency*, August 4, 2016, https://www.darpa.mil/news-events/2016-08-04
[149] Defense analysts and AI industry experts disagree about the implications of AI-enabled capabilities for nuclear security. See, Edward Geist and Andrew Lohn J, *How might artificial intelligence affect the risk of nuclear war?* (Santa Monica, CA: RAND Corporation, 2018).