Autonomous Weapon Systems and International Crises

Nathan Leys

Abstract

The United States is investing heavily in autonomous weapon systems (AWS) as part of the Department of Defense’s “Third Offset” strategy. However, scholarship on AWS has largely failed to explore the ways in which these systems might themselves have strategic ramifications. This gap is especially apparent in relation to strategic interaction in crisis scenarios. This article seeks to highlight relevant dimensions of the ongoing debates over (1) how to define AWS, (2) the technology behind their development, and (3) their integration into the future force. The article then constructs five scenarios where introducing AWS may affect how an international crisis involving the United States and an adversary plays out.

In 2015, Secretary of Defense Chuck Hagel introduced the Defense Innovation Initiative, colloquially known as the “Third Offset.”1 The Third Offset’s objective is to maintain the United States’ qualitative military edge over potential peer or near-peer competitors by incorporating cutting-edge technologies into doctrine, structure, and operations. A central part of this initiative is leveraging advances in artificial intelligence (AI) to increase the role of autonomy in military robotics and battle networks. As former Deputy Defense Secretary Robert Work, one of the Third Offset’s key architects, recently stated, “The third offset is simple. At its core AI and autonomy will lead to a new era of human-machine collaboration.”2

The Third Offset has been criticized for being “a convenient handle for a menu of new defense capabilities” rather than a coherent strategy.3 At the same time, the strategic ramifications of AWS have gone relatively

---

Nathan Leys is a JD candidate at Yale Law School. He previously studied international security at George Mason University.
unexamined. This article attempts to fill that gap by examining how AWS might affect strategic competition between the United States and potential adversaries during a crisis.

Such an effort is warranted for at least three reasons. First, it is possible the United States could face crises involving peer or near-peer competitors in some future year. Avery Goldstein notes, “for the next decade . . . the gravest danger in Sino-American relations is the possibility the two countries will find themselves in a crisis that could escalate to open military conflict.” Graham Allison has further argued that such a crisis could be the spark for a US-China conflict fueled by a shift in the international balance of power. Recent tensions with Russia over Syria, Crimea, and the Baltic States also suggest that the United States could once again find itself embroiled in a crisis with its erstwhile Cold War adversary. A recent report from The Hague Center for Strategic Studies argues the past few years represent “a larger trend: the comeback of interstate crisis.” The United States and its rivals could soon find themselves stumbling into a crisis in which AWS will play a significant role.

Second, if AWS are successfully integrated at every level of command, the way the US military thinks about decision making will have to shift. The DOD conceptualizes AWS through the lens of human-robot interaction (HRI), framing autonomy as an ongoing collaboration between commanders, soldiers, and computers. Although political leaders will continue to make decisions at the strategic and grand strategic levels, those decision makers will receive their information and military options from the commanders at the operational level who will be the most immediately affected by HRI. The sharing of decisions with computers at all levels of command and control (C2) is a fundamental break with previous patterns of decision making and should be investigated as such.

Third, failing to consider the independent effect of autonomy on US behavior in crisis would represent a dangerously myopic approach to strategy. Because of the lack of historical data on the effects of AWS, there are legitimate concerns that any such forward-looking analysis runs the risk of mistaking projections for data. In fact, these criticisms ignore the longstanding role of evidence-based prediction in US defense planning. Additionally, to the extent that good strategy involves plans conditioned on an adversary’s likely responses, the United States should seek to understand how potential adversaries will view our use of AWS. In short, prediction in this area is a prerequisite for success of the Third Offset.
This inquiry does not seek to exhaust all possible mechanisms for autonomy’s influence on US behavior in crises, nor does it attempt to make iron-clad predictions about the future of conflict more broadly. Instead, it seeks to provide useful background on the debates surrounding AWS and illuminate some of the mechanisms by which the logic of AWS might interact with crisis dynamics.

Debates Informing the Development of AWS

Before entering a discussion of existing research on AWS, one obvious issue should be addressed: How does one research something that has not yet happened? The question is valid. There is no way to know for certain how autonomy will impact the battlefields of tomorrow, and for obvious reasons much of the cutting-edge research on existing AWS is classified. But it is possible to apply what we know about crises to what we know about AWS. Furthermore, the risks in making educated guesses about the future of AWS are far less than the risk of waiting until military autonomy is fully matured before attempting to reason through its implications.

Defining Autonomy in Weapons

Few scholars or policy makers agree on a precise definition of what constitutes an AWS. Definitional debates might sound pedantic, but they are actually crucial. One problem created by definitional ambiguity is that civilian policy makers and military commanders, or even commanders in different branches, might have different understandings of what AWS can and cannot do. Additionally, without agreement on what exactly constitutes an autonomous weapon, the default temptation may be to think of them in terms of science fiction tropes—indeed, almost every nontechnical article on the subject contains a reference to science fiction, a stock photo of a menacing robot assassin, or both. This definitional failure would lead to bad policy making and bad strategy.

Attempts to resolve the definition dilemma have resulted in two general ways of thinking about AWS. The first way of defining AWS differentiates them from other weapons in terms of degrees of control. Usually, these degrees are described relative to a loop roughly analogous to John Boyd’s OODA (observe-orient-decide-act) paradigm. Human Rights Watch laid out a three-part degree-of-control definition: “Human-in-
Autonomous Weapon Systems and International Crises

the-Loop” (humans select and engage targets), “Human-on-the-Loop” (robots select and engage targets, but a supervising human can override), and “Human-out-of-the-Loop Weapons” (full AWS). DOD’s 2012 directive on AWS encompasses the latter two categories.

This method of defining AWS runs headlong into the problem of reaction time, which threatens to turn humans in and on the loop into liabilities. An influential paper on the pragmatic regulation and development of AWS argues that as the speed of military conflict increases, necessary reaction times will shrink below human capabilities. Consider the Phalanx close-in weapons system (CIWS), mounted on US Navy ships as a last-ditch defense against antiaccess/area-denial (A2/AD) weapons like antiship cruise missiles. Because the time spent waiting for a crew member to approve a defensive action against an incoming threat could prove fatal to a ship, the Phalanx CIWS can be set to acquire and engage incoming missiles automatically. Having a human “on the loop” will become at best irrelevant and at worst dangerous once the loop moves too quickly for human reaction. In this way, autonomy becomes both a cause and effect of the increasing speed of warfare, and an intensifying first-mover advantage creates an incentive to develop AWS first and ask strategic questions later.

Although the degree-of-control paradigm helps illustrate the forces pushing the development of AWS forward, the US military has a different framework for defining autonomy. This approach has been spearheaded by the Defense Science Board (DSB), first in a 2012 report and then in a 2016 study appropriately titled “Autonomy.” The DSB argues degree-of-control definitions “are counter-productive because they focus too much attention on the computer rather than on the collaboration between the computer and its operator/supervisor” [italics in original]. The DSB views autonomy neither as a series of categories of human control over machines nor as a sliding scale of human control but rather as the “explicit allocation of cognitive functions and responsibilities between the human and computer to achieve specific capabilities.” Put differently, the operational-dynamic approach recognizes that an AWS may at any given point have differing levels of control over different aspects of a mission. Moreover, those levels may shift over the course of that mission and will almost certainly vary between missions conducted over the course of the system’s lifecycle.
This concept is more intuitive than the jargon makes it seem and is perhaps best illustrated by example. One Defense Advanced Research Projects Agency (DARPA)–sponsored study proposes a concept of operations (CONOPS) for conducting aerial warfare in which autonomous battle-management systems support human commanders’ decision making by recommending courses of action and helping direct human and robotic pilots against an adversary.¹⁷ Take Japan, which plans to build “high-performance robotic aircraft that would fly as helpers for manned fighters; a pilot would issue commands.”¹⁸ Such aircraft could plausibly be combined with the DARPA CONOPS to create a fighting force employing autonomy at multiple levels. Under the DSB’s paradigm, autonomy here is not simply about unmanned aerial vehicles (UAV) deciding to shoot down enemy aircraft on their own. Instead, HRI operates on (at least) two levels simultaneously: AI helping commanders decide how to deploy air assets, and autonomous UAV wingmen helping pilots conduct air operations.

Regardless of which definition is the most correct, the Department of Defense (DOD) subscribes to the latter paradigm. The DOD’s former Strategic Capabilities Office chief, William Roper, speaks of human soldiers acting as “quarterbacks” for teams of AWS.¹⁹ Robert Work has referenced the need for “human-machine collaboration” when “you’re operating against a cyber attack . . . or attack against your space architecture or missiles that are screaming in at you at Mach 6.”²⁰ Rather than a state of control, policy makers view autonomy as a multilevel process of human-computer teamwork.

**Technical Development**

Understanding the strategic ramifications of AWS does not require an engineer’s knowledge of how they work. That being said, the technologies behind AWS raise familiar questions regarding the prevention of friendly fire, miscalculation, and proliferation.

First, AWS must be able to identify legitimate targets. The tasks of getting a robot to distinguish a tank from a minivan or an enemy tank from a friendly tank are difficult and the consequences of a mistake enormous. Moreover, the job of differentiating a journalist with a camera from an enemy soldier with a weapon (or an enemy soldier attempting to surrender) is even more challenging.²¹ Although the technology involved has since advanced considerably, one facet of the Patriot missile
Autonomous Weapon Systems and International Crises

defense system’s friendly fire incidents during the Iraq War is instructive. Because “operators [are] trained to trust the system’s software” in scenarios where threats demand superhuman reaction times, the increasing tempo of combat can create a tradeoff between protecting troops and the accidental targeting of friendly forces (or noncombatants).22 The distinction problem will only become more important and difficult in hybrid scenarios where the lines between civilian and military are blurry at best. Human soldiers can make mistakes too, of course. But to the extent that AWS are developed and deployed because they enhance a military’s ability to deliver lethal force, it follows that a mistake by an autonomous system may have correspondingly greater consequences.

Second, because AWS rely on decision-making processes that differ from human cognitive processes, they may act in ways that are difficult or impossible for humans to comprehend or predict. The risk of side A’s AWS making a mistake that causes a miscalculation by side B’s commanders is obvious. Less obvious is how miscalculation might arise from the interaction of two sides’ AWS. The development of AI systems to play Go, an incredibly complex board game, is perhaps the paradigmatic example of the unpredictability of AI strategic interaction. AlphaGo, a program created by DeepMind, an AI research outfit under Google’s umbrella, defeated the world’s top human player in 2017. Subsequently, DeepMind released recordings of games AlphaGo had played against itself, developing strategies so foreign to conventional strategies that Go experts described them as “from an alternate dimension.”23 The risks of AI strategic interaction are illustrated by the trading algorithms used by Wall Street firms. These algorithms have been accused of causing so-called flash crashes by locking themselves into a tit-for-tat sell-off loop that moves so quickly humans cannot realize what is happening until it is over.24 Applied to AWS, the danger is that side A cannot predict with certainty under what conditions its own AWS might fire the first shot, either because of a glitch or because the AWS system adopts a strategy involving preemptive strikes that side A’s unsuspecting human commanders could never have foreseen.25

There is only so much a military can do to reduce the unpredictability of AWS. The Defense Science Board’s 2016 report, for instance, raises the possibility of installing a “black box,” an “audit trail that can explain why [AWS] did what they did.”26 The idea has some merit, but if the malfunction of an AWS leads to conflict with another military, an
ex post report only has so much utility. Ex ante, AWS will always be unpredictable to some degree, because to program an AWS to be perfectly predictable is to program it to be vulnerable to a more adaptable enemy AWS. And the uncertainty created by the interaction of rival AWS will not decline over time, since the pressure to drive the fight by deploying cutting-edge AWS means lessons learned from the interaction of two older systems may not apply to a future interaction between those systems’ successors.

Finally, the proliferation of cutting-edge weapons is not a new problem for strategists. However, compared to nuclear weapons or GPS-targeted precision munitions, the technologies enabling AWS are much more easily available in the commercial market. Many of the sensors used in AWS, for example, are increasingly vital to civilian autonomous technologies. Consider self-driving cars: Lidar (light radar), for instance, is favored by many developers of self-driving cars because of its ability to “pinpoint the location of objects up to 120 meters away with centimeter accuracy.” Other prototype vehicles use passive systems like high-resolution cameras and microphones to understand the world around them. Many of the challenges faced by military AWS, including operating in low-visibility conditions, differentiating human bodies from inanimate objects, and developing redundant systems to prevent the failure of one sensor rendering a robot blind or deaf, are the same problems that civilian engineers are attempting to solve. Indeed, the sensors that will allow a self-driving car to avoid hitting a pedestrian may soon be the same as those used by an AWS to kill an enemy combatant. The ubiquity of these technologies in the civilian world matters, because if AWS substantially increase the capabilities of an adopting military, the question of proliferation becomes inextricable from the question of how difficult and expensive it is to build AWS. Some analysts expect AWS will proliferate easily. A now-famous open letter signed by luminaries including Elon Musk, Stephen Hawking, and Steve Wozniak warns, “Autonomous weapons will become the Kalashnikovs of tomorrow.” But this comparison appears inaccurate. The Kalashnikov came to define modern low-level warfare because it is simple, cheap, easy to master, and practically unbreakable. It may soon be possible to rig a cheap drone to dive-bomb anything that moves, but the highly capable AWS likely to be deployed by the United States and its near-peer rivals are the opposite of simple, and as they develop, they will become more complex,
not less. Andrea Gilli and Mauro Gilli note that similar constraints may make the proliferation of military UAVs much more difficult than is commonly assumed. Given these technical limits, for the near- and medium-term, only the most technologically advanced militaries are likely to develop AWS effective enough to make a difference against the United States or similarly capable military.

Although the complexity of advanced AWS may make them less susceptible to proliferation than is commonly assumed, it could also make them vulnerable to cyberthreats. Michal Klincewicz argues any AWS capable of operating in chaotic battle conditions while accurately distinguishing appropriate targets will necessarily run software so complex it will contain vulnerabilities making it susceptible to hacking. Although some proposals for defensive autonomous cyberweapons have been floated, anything resembling such a system is either hypothetical, classified, or both. Commanders may attempt to mitigate the hacking problem by insulating AWS from wireless communication (the robotic analogue of a ship going radio silent), but as discussed below, this creates a new set of C2 problems.

AWS and the Future Force

Technology alone is not a strategy, however. AWS must be integrated into a human fighting force. Discussions of this human-machine teaming have illuminated three additional considerations that strategic thinkers should bear in mind: human proximity, disaggregated C2, and public opinion.

Proximity to Humans

AWS differ from human soldiers in their expendability—machines cannot die, so there is no such thing as autonomous self-sacrifice or suicide missions. This makes AWS qualitatively different from previous advances in military technology, because they raise the possibility of robot soldiers that can go where humans cannot. Proximity in this sense has two facets: an AWS’s location relative to its handler and to civilians/noncombatants.

The human-robot interaction envisioned by the DSB is not wholly dependent on the physical or temporal distance between the two. Consider, from closest to furthest in terms of space and time, the following
three examples. First, autonomous unmanned combat aerial vehicles (UCAV) acting as “bodyguards” could escort bombers into enemy airspace, using continuous real-time coordination with the human-piloted craft to fly closer to the bomber than a manned fighter jet ever could. Second, in terms of medium-range proximity, an integrated air- and missile-defense system could use a Phalanx CIWS to autonomously shoot down a passing missile targeting a friendly ship over the horizon. The most “distant” AWS are loitering munitions and stealthy autonomous unmanned underwater vehicles or encapsulated torpedoes like the US MK-60 CAPTOR system, which lurks underwater until it identifies the sonar signature of an enemy ship. In each example, a human gives an autonomous system a task (e.g., defend a bomber, protect friendly ships, patrol disputed territory), but HRI varies over space and time.

Proximity to humans also appears in discussions of AWS-civilian interaction. Indeed, many of the legal/ethical concerns previously discussed stem from the problem of differentiating combatants from noncombatants. These objections are commonly framed through the hypothetical use of AWS in law enforcement. Amnesty International, for example, has warned of the “further development of killer robots whose insidious creep into policing would put lives at risk and pose a serious threat to human rights.” Cristof Heyns says, “AWS may be used [in] hostage situations . . . crowd control; targeting specific classes of perpetrators such as prison escapees and big-game poachers; providing perimeter protection around buildings, such as high security prisons . . . or to protect pipelines. Such systems may also be used in ‘wars’ on drugs or other crime control or antiterrorism operations.”

On the other hand, there are those who doubt AWS will be used near civilians in the foreseeable future, if ever. For example, Robert Sparrow notes AWS will likely first be deployed in antisubmarine warfare, air-to-air combat, and other theaters where “there are few civilian targets.” In his study of the impact of AWS on the US Air Force, RAF Wing Commander Andrew Massie writes, “with clear delineation between friend and foe, clear fire corridors for autonomous kinetic, cyber, and electronic-warfare weapons might offer a decimating form of defense” in arenas where civilians are absent. AWS are more likely to be used in spatial contexts where civilians are not present, both because of the difficulty of differentiating combatants and noncombatants and because
the preponderance of situations in which the AWS currently under development will be useful will likely occur far from civilian areas.

**Disaggregated Command and Control**

One of the most significant transformations of military operations since the invention of the telegraph has been the use of long-distance communication to aggregate C2 to the upper echelons of command structures. While commanders’ ability to communicate with troops in the field is not—and has never been—perfect, new threats ranging from antisatellite weapons and cyberattacks to the cutting of undersea fiber-optic cables pose unprecedented dangers to the Pentagon’s ability to maintain robust C2 in contested environments. This is why near-peer and peer adversaries’ A2/AD operations are likely to target these C2 assets early in the event of armed conflict.

AWS are designed to operate in precisely such information-scarce scenarios. Even when C2 structures are operating at or near capacity, fleets of unmanned systems simultaneously communicating with their operators may overwhelm both technical and human bandwidth. A 2014 Rand Corporation study states, “[Unmanned vehicles] can potentially be equipped with different types of autonomous functions to reduce messaging loads on communications links to C2 and information analysis centers. For example, autonomous onboard planning algorithms can help reduce communications loads and lessen the need for frequent maneuver, heading, or flight commands.”

This problem would be compounded if C2 assets were to be destroyed in a conflict. In response to this challenge, DARPA is investing heavily in the Collaborative Operations in Denied Environments (CODE) project, “which would allow multiple drones to independently fly to their objective and then find, identify and kill their targets.” Under CODE, a swarm of AWS would have a single human operator in theater (or no direct human operator at all), as opposed to the status quo of positioning multiple operators for each system far from the battlespace for nonautonomous, remote-control weapons like Predator UAVs. In addition to reducing the load on centralized C2 structures, AWS could mitigate Klinczewicz’s fear of enemy cooption by “[decreasing] the likelihood of uplink communication hacking.” Ideally, autonomy will drastically improve the survivability of US unmanned systems should an enemy disrupt C2 capabilities.
Ironically, the qualities of AWS that improve their survivability in contested environments also challenge the Pentagon’s organizational culture. Massie notes, “There are grave limitations between that mode of operating and our current C2 structure. A generation of leaders has lived in an operational environment where . . . decision making for the use of lethal force has largely been held with higher echelons.”49 It is this paradox that Heather Roff terms the “strategic robot problem.”50 She argues the process of identifying and prioritizing targets “is inherently strategic, as it involves the matching of means to ends” and thus undermines C2 by allowing AWS to act as “individual commanders, as well as JAG officers, weaponizing officers and intelligence officers.”51

The extreme case of an autonomy-driven disaggregation of C2 would be a swarm of AWS designed to be unable to communicate with its commanders.52 Straub describes such a nonrecallable AWS as a deterrent similar to nuclear weapons during the Cold War and to the Zanryū Nipponhei, or Japanese holdouts, who continued fighting WWII long after the war had ended.53 Such a system is not the goal of programs like CODE. But if created and deployed, a Japanese holdout–capable AWS would represent not just the reluctant delegation of lethal decisions to lower echelons of command but also the foreclosing of an option to terminate hostilities.

**Public Opinion**

Public opinion on AWS is not well understood, because of a lack of popular understanding of AWS and because of a lack of research into what views the public does hold on autonomous weapons. A 2013 survey conducted by YouGov and University of Massachusetts–Amherst finds 55 percent of Americans oppose AWS, with only 26 percent in favor.54 However, a replication study finds that when the development of these systems is framed as potentially lifesaving for soldiers and inevitable by other countries, respondents’ approval of AWS increased, suggesting that public support or opposition to AWS is context dependent.55 While comparisons of data from different surveys should be treated cautiously, these results suggest the public is instinctively wary of AWS but may be amenable to persuasion.

A relationship between public sentiment, AWS, and policy making may operate differently in more authoritarian countries. Horowitz points out autocrats who fear revolt by their populations and a coup by their military may for that reason prefer to invest in AWS.56 Robert Work
made a similar argument at the Center for a New American Security in 2015: “Authoritarian regimes who believe people are weaknesses in the machine, that they are the weak link in the cog, that they cannot be trusted . . . they will naturally gravitate towards totally automated solutions. Why do I know this? Because that’s exactly the way the Soviets conceived of their reconnaissance strike complex.”57 If public opinion proves to be a constraint on US development, deployment, and use of AWS, the same may not be true of potential adversaries.

Some scholars approach the question of whether authoritarian states might be more likely to develop AWS than democracies from the other direction. They argue that by removing human soldiers from the battlefield in response to a democratic public’s preference for casualty avoidance, AWS may make democracies more war-prone by reducing the domestic political costs of conflict.58 On the other hand, one study found AWS “do not decrease the degree to which civilian and military leaders are identified as responsible for negative outcomes” such as instances of lethal malfunction.59 Policy makers may find themselves pulled between the potential benefits of avoiding a “Black Hawk Down” scenario and the risks of an AWS malfunction causing a robotic My Lai massacre. This is the closest the existing literature comes to examining how AWS might change the dynamics of competition between two powers. However, this subgenre of argument largely deals with which kinds of leaders might develop AWS, and when; it does not deal with how AWS may impact the behavior of states once that competition boils over into a crisis.

**AWS and Crisis Bargaining**

None of the foregoing is to suggest that previous research into AWS is misguided, irrelevant, or useless. But a sustained analysis of the writing on autonomy reveals a glaring lack of consideration of how AWS might affect the behavior of countries that adopt them. This gap is all the more striking because the entire point of the Third Offset, as set out by the Pentagon, is to help commanders make decisions and so keep the United States comfortably ahead of the competitors with which it could find itself embroiled in crisis.

To avoid being bogged down in theoretical debates about when, why, and how crises escalate, this article will proceed from this observation: in a crisis, perceptions—by decision makers and the public—matter a great deal.60 Using this axiom, the practical impact of the crisis-bargaining
gap will be illustrated through a series of scenarios, each drawn from real-world crises and involving systems substantially similar to AWS that have been deployed or prototyped.  

**Scenario One: Claims of Accident, Alliance Obligations, and Claiming Mistake as an Off-Ramp**

A Russian air-defense battery stationed near the Syrian-Turkish border shoots down a Turkish military jet carrying several prominent Turkish politicians in Turkey’s airspace. Amid the resulting uproar, the Russian military claims it does not know why the system fired but suspects that the autonomous targeting system may have malfunctioned. There is no way to evaluate the veracity of Russia’s claims. Alongside sanctions and public condemnations, Turkey demands unspecified US military action against Russia under the NATO Charter. American public opinion strongly supports Turkey. The United States has a range of choices, including striking Russian forces in Syria, refusing point-blank to meet a NATO ally’s demand for support after a Russian attack, or attempting to find an off-ramp for de-escalation.

In this case, the United States would prefer not to launch military action against Russia. Regardless of the veracity of Russia’s claim of an accidental firing, the United States could call for a diplomatic resolution short of kinetic force (e.g. international inspections of the system, a withdrawal of air defense batteries in the area, etc.). Autonomy could afford the United States an off-ramp by providing a plausible cover: the potentially accidental nature of the violation of an ally’s sovereignty means a military response is neither legally required nor morally warranted.

In short, AWS could provide a face-saving alternative for leaders trying to de-escalate a crisis. The technical complexities of AI-enabled weapons and the possibility of malfunction add a new layer of fog to war. It may not be possible in such situations to determine whether an AWS malfunctioned or a redline was crossed—more importantly, it may not matter. AWS operating in conditions of uncertainty make it possible for a first shot to be fired, even if no person fires it. In an interesting twist on the debate about whom to hold responsible in the event of an AWS’s malfunction, the most life-saving answer in a crisis may be no one: If there is no one to blame, there is no one to bomb. On the other hand, national leaders may well hold the owners of the AWS system respon-
sible regardless whether an attack was accidental. In this case, retaliation might seem desirable to maintain credibility.

Additionally, because nonautonomous weapons like stealth bombers and remote-control UAVs can already carry out retaliatory strikes without significant operational risk to US Soldiers, autonomy per se is not likely to be a unique reason why negligible operational risk means the United States might choose to escalate in such crises. Furthermore, these disparities in capabilities are already an incentive for adversaries to develop asymmetric responses, both in and out of the theater in question. It is not clear what kinds of asymmetric responses AWS will be able to neutralize; autonomous weapons therefore may not subtract much from the cost side of the United States’ cost/benefit analysis in deciding whether to strike.

**Scenario Two: Accidents Involving a Near-Peer Competitor**

After months of increasingly combative rhetoric, China announces the People’s Liberation Army will enforce an Air Defense Identification Zone (ADIZ) over contested islands in the South China Sea. The United States rejects the legitimacy of the ADIZ and begins air patrols in the area to reassure its allies and signal support for freedom of navigation rights. While a US F-35 and its four autonomous unmanned combat aerial vehicle wingmen are flying through the ADIZ, a Chinese drone begins harrying the patrol. The drone gets so close that an autonomous US UCAV’s threat-perception algorithm perceives an imminent danger to the F-35. Because the US UCAV and Chinese drone are too close to the F-35 for the UCAV to fire, the UCAV slams into the Chinese drone to protect the rest of the patrol.64 Each side accuses the other of reckless behavior, and both increase their unmanned and autonomous air patrols in the disputed zone.

In this case, both the United States and China would probably be less likely to escalate than if one of their human pilots had died. Compare the public outcry over Iran’s decision in January 2016 to detain 10 US Navy personnel in the Persian Gulf to the muted public reaction to China’s seizure in December 2016 of a US Navy submersible drone.65 A failure to respond to the death of a military member could prove politically disastrous for a US leader, but destroyed AWS do not have grieving families.

On the other hand, the diminished risk to US pilots and the resulting reduction in public demands for revenge may encourage leaders to deploy AWS when they would have otherwise chosen to not deploy piloted air
patrols. This could end up multiplying risk, because each side will to some degree be unaware of the other’s autonomous/unmanned capabilities, and neither side can know how adversarial military systems driven by AI will interact differently than those driven by human intelligence. Thus, AWS may make crises involving patrols over disputed territory more likely but less dangerous.

**Scenario Three: Public Pressure to Withdraw Forward-Deployed Forces**

Citing potential cost savings and reduced risk to American Soldiers, a Congressional report urges DOD to withdraw them from the Korean Demilitarized Zone (DMZ) and replace them with autonomous robotic sentries.\(^{66}\) Liberal doves and conservative hawks, persuaded by the report’s assertion that AWS will be at least as effective as the currently deployed US forces, unite in support of the proposal. The South Korean government supports the addition of the autonomous sentries but opposes the withdrawal of American troops.

This scenario draws on Thomas Schelling’s observation that although small forces of American troops stationed on allied soil cannot repel a mass invasion, “bluntly, they can die. They can die heroically, dramatically, and in a manner that guarantees that the action cannot stop there.”\(^{67}\) The notion, applying James Fearon’s formulation, is that if these tripwire troops are killed in an attack on an ally’s territory, the potential domestic political costs imposed on a US leader who chooses not to respond guarantee an overwhelming military response, making the US commitment to South Korea more credible. But AWS, by definition and design, cannot “die heroically.” If AWS physically displace human soldiers from an ally’s territory, the potential domestic political costs to leaders of not responding in the event of attack would be diminished. Hence, South Korean leaders might perceive the United States’ commitment as less credible.

One of the primary arguments for the development and deployment of AWS is that robots can remove humans from harm’s way. This assertion runs directly counter to the DOD’s insistence that AWS will fight alongside human soldiers, rather than displacing them.\(^{68}\) Whatever the Pentagon’s insistence today and regardless of whether AWS could replace humans without impacting military effectiveness, it is entirely plausible that placing soldiers in harm’s way will become politically untenable if
AWS are seen as a viable replacement for human soldiers. This is particularly true if the most visible permutations of AWS are autonomous unmanned underwater, surface, and air vehicles rather than AI-enabled computer systems designed to support military logistics and decision making. Congress and the public are more likely to demand the replacement of human soldiers with AWS if they can picture a robot armed with high-tech firearms storming onto the battlefield.

Designing AWS to support—rather than replace—human soldiers may make sense from a military perspective, but it raises political risks domestically and internationally. First, public misunderstandings of AI, steeped in science fiction archetypes of hyper-advanced robot warriors, may lead to the overestimation of AWS’ capabilities, even as they fuel pacifist opposition to AWS’ development. This overestimation, in turn, may convince supporters of AWS that new weapons can replace human soldiers without reducing military effectiveness.

The second danger to the international credibility of the United States and its commitments to its allies also flows from this potential for domestic overestimation of AWS’ capabilities. To the extent political pressure leads to AWS geographically displacing forward-deployed forces instead of supporting them, they may make US commitments to defend allies less credible. If South Korea is less certain of the US defense commitment, it might choose to self-help by building up its own military, possibly including the development of nuclear weapons or its own AWS.

This tension between the enhanced lethality of US forces and the diminished credibility of US commitments from forward-deployed AWS could be resolved in two ways. First, military leaders could convince civilian policy makers and the public that AWS would be ineffective unless they are directly supporting US Soldiers. Given the parochial incentives of commanders to emphasize the capabilities and downplay the limitations of new military systems during the appropriations process, this may be easier said than done. But if this framing is successful, and if AWS are deployed to augment tripwire forces, they may marginally increase the credibility of US commitments by signaling a prioritization of that ally’s defense and increasing the fighting effectiveness of deployed land forces.69

Alternatively, the United States could adopt a doomsday device approach to make US involvement in a conflict automatic. Such an effort would involve programming prepositioned AWS to strike North
Korean targets if a certain condition occurs (e.g., a critical mass of North Korean troops crosses the DMZ). To make this commitment credible, the United States would have to convince South Korea that it will not simply call off its AWS when the time comes. That would require pre-programming AWS to cut off all communication with US commanders at the moment the system decides to strike North Korea. This approach raises obvious concerns that a computer glitch or a large-scale military exercise could trip the system, not only dragging the United States into a war it does not want but also starting a conflict where a crisis might otherwise have been averted.

**Scenario Four: Public Demands for Humanitarian Intervention**

After peaceful protests, a Middle Eastern dictatorship begins a violent crackdown to suppress dissent. With thousands of refugees in immediate danger, public opinion strongly supports air strikes. The regime possesses advanced air defenses capable of shooting down US manned fighters and slower UAVs, but stealthy, autonomous UCAVs can avoid these batteries. Spurred by viral photos of regime abuses posted on social media, the president is considering declaring a “redline,” promising airstrikes and a no-fly zone if the regime attacks a refugee camp that the regime alleges provides cover to pro-democracy rebels.70

This scenario is similar to the second case in that it involves risk to manned and unmanned aircraft. However, the interest here is purely humanitarian, and the adversary is substantially less able to retaliate against the United States than a near-peer competitor. To the extent that AWS could act in place of manned aircraft, drones, or ground forces in a humanitarian intervention, autonomy may obviate US leaders’ fears of another Mogadishu and reduce the cost of enforcing a redline. Enforcing these redlines, in turn, may enhance the credibility of the United States’ other commitments, providing a benefit beyond any intrinsic good obtained by protecting human rights.

The public opinion aspect of this scenario should also be borne in mind. If public disapprobation of AWS hardens, using unpopular autonomous systems in a humanitarian operation demanded by the public may undermine support for the intervention. On the other hand, it is also possible that the use of AWS in such a scenario could improve the perception of such weapons in the public’s estimation. The public’s
approval or disapproval will likely hinge on the ability of AWS to discriminate between civilian and military targets, a task that is infinitely more complex in scenarios of insurgency, civil war, and hybrid conflict like this one.

Beyond the domestic audience, US policy makers should also consider international observers. If AWS prove devastatingly effective against a less-advanced military, other potential future adversaries may kick-start their efforts to develop their own indigenous AWS capabilities. A similar phenomenon occurred after US precision munitions decimated the Iraqi military in 1991–1992, a “wake-up call” for the People’s Liberation Army to begin modernizing its own forces.71 If AWS are so effective at obtaining US objectives that they change the humanitarian intervention calculus, their use may not only publicize valuable information about US autonomous capabilities but also carry ramifications for the military balance of future conflicts with peer or near-peer competitors.

A final crucial point is the role of AWS, and advanced technology in general, postintervention. No one seriously suggests AWS will be able to effectively carry out the counterinsurgency or police actions necessary to stabilize violent regions. Indeed, that is not the point of AWS. The Third Offset is an effort to shift the US military’s focus from Afghanistan- and Iraq-style operations to medium- and high-intensity warfare with technologically advanced adversaries. To put it bluntly, AWS are intended to fight militaries like China and Russia, not the Taliban.

Scenario Five: Command and Control and Assurances

A period of tension between the United States and China erupts into conflict in the South China Sea. The first shot is fired when an autonomous US UCAV identifies an autonomous Chinese air defense system’s radar as hostile and preemptively engages. Each side accuses the other of provoking the conflict, but because both the UCAV and Chinese system are destroyed in the clash, it is impossible to recover diagnostic logs that would shed light on why each AI acted as it did.

In the opening days of the resulting conflict, the United States and China each destroy much of the other’s space-based communication assets and C2 infrastructure in the Pacific. Before this occurs, however, the United States orders a handful of stealthy, autonomous attack submersibles to patrol the South China Sea and sink any PLA-Navy (PLAN) ship they encounter. Two weeks later, a ceasefire is brokered by the UN
to give the combatants time to negotiate an armistice. During negotiations, one of the US officials are autonomous submersibles, cut off from communication and unaware of the ceasefire, sinks a PLAN cruiser in the Straits of Malacca. US officials are forced to reveal they are unable to call off the submersibles until they can reestablish their military satellite constellation, and China breaks off negotiations.

This scenario combines concerns of AI-enabled preemption, non-recallable drones, and disaggregated C2. Rules of engagement can, to some degree, be programmed into an AWS. But just as nervous frontline soldiers can start a skirmish, AI-enabled weapons systems that make probabilistic decisions in milliseconds can miscalculate. As mentioned above in the discussion of adversarial trading algorithms, this is particularly true when each side deploys AWS that may misinterpret the actions of the other side’s systems and react in unpredictable and potentially dangerous ways. In that sense, this case is the inverse of Scenario Two; instead of providing a face-saving off-ramp for de-escalation, the uncertainty clouding the initial engagement presages further violence.

This scenario also illustrates Schelling’s observation that effective coercive bargaining requires credible threats and credible assurances. Because the Zanryū Nipponhei were essentially harmless, the Japanese empire at the end of WWII could credibly assure the United States that a peace agreement would actually hold. The AWS deployed in coming decades, however, will presumably be more capable of inflicting harm than an infantryman with a rifle trapped on an island in the middle of the Pacific. If and when AWS become so effective at operating in theaters where A2/AD has degraded C2 that they will continue to wreak havoc either until C2 is restored or they are destroyed, they could force crises to escalate by making it impossible to credibly de-escalate.

Conclusion

Policy makers and researchers should seek to better answer questions of how to use AWS, because these systems are likely to interact with many of the theoretical mechanisms that inform our understanding of international crises. If AWS on balance decrease America’s ability to send costly signals, this could reduce its ability to make credible threats and assurances in a crisis. This, in turn, could undermine the US alliance system. In such a situation, US allies may seek AWS themselves in much the same way that UAV technologies have proliferated.
It is an oversimplification, however, to say that because AWS cannot die, signals will not be credible. Much depends on the context in which AWS are used. For example, a lone autonomous UCAV or submersible may operate outside close physical or temporal proximity to US Soldiers, making de-escalation harder if conflict degrades C2. In contrast, an autonomous unmanned ground vehicle may operate in extremely close proximity to ground forces, multiplying lethality and improving survivability of US assets. The domestic political costs involving the loss of military assets may be lower in the former scenario but constant in the latter. If this is the case, US strategists should consider emphasizing the deployment of AWS only when it does not seriously compromise the United States’ ability to effectively bargain in crises.

Additionally, AWS may reduce the risk to American lives without necessarily reducing the US’s war-fighting capacity. This, in turn, may reduce US domestic political opposition to military interventions, especially in humanitarian contexts without an immediately apparent US national interest.

It is impossible to predict with total confidence how AWS will develop and influence policy making. Future research should focus on technologies that are emerging, not merely hypothetical, to mitigate this concern. Additionally, some may worry about the use of hypothetical scenarios to explore AWS. This critique is valid to some degree, but two factors caution against dismissal of this analysis. First, the United States cannot afford to wait for an *ex post* analysis of AWS. If research into military autonomy is to be useful, it must, to some degree, be hypothetical. Second, this article does not pretend to present ironclad findings on the relationship between AWS and crisis dynamics; instead it draws on existing research to suggest some mechanisms by which AWS might affect the dynamics of future foreign policy crises.

If the reader is left with more questions than answers, it is because this is a call for further inquiry. This future research should consider employing parallel simulations contrasting the involvement or absence of AWS in a crisis scenario. Additionally, although analysts have begun to speculate about the proliferation of AWS to states with different political systems and strategic cultures, there is no comparative research known to the author into how strategists in states like China, Russia, or Israel might conceptualize AWS differently than their counterparts in the
United States. Such insights would prove invaluable to security studies scholars and policy makers alike.

The Pentagon has repeatedly emphasized that the Third Offset is about much more than technology: it involves changing organizations, doctrines, and paradigms to accommodate and maximize the impact of technological advancements. However, merely recognizing the necessity of combining strategy and technology is different than considering how those innovations might change crisis dynamics and coercive diplomacy. Such an undertaking is indispensable if AWS are to help the United States maintain a strategic, and not just technological, edge over its adversaries.

Notes


4. Of course, the Third Offset involves more technologies than just AI and autonomous weapon systems. Other areas include biotechnology, nanotechnology, and 3D printing, among others. These technologies are important and deserve examination as well, but they are beyond the scope of this article. For a broader look at the relationship between technological dominance and military superiority, see Ben FitzGerald and Kelley Sayler, Creative Disruption: Technology, Strategy and the Future of the Global Defense Industry, Center for a New American Security, June 2014, https://s3.amazonaws.com/files.cnas.org/documents/CNAS_FutureDefenseIndustry_FitzGeraldSayler.pdf?mtime=20160906081304.


7. Tim Sweijs, Artur Usanov, and Rik Rutten, Back to the Brink: Escalation and Interstate Crisis, The Hague Centre for Strategic Studies (HCSS) StratMon2016 (The Hague: HCSS,
Autonomous Weapon Systems and International Crises


15. DOD, Role of Autonomy in DoD Systems, 4.

16. DOD, 4.


25. Of course, a human soldier may also choose to fire a first shot when his or her human commanders would never have allowed such an action. However, a human commander is better positioned to understand how his or her soldiers will interpret and apply rules of engagement than to predict how an AWS will do so.


43. See, for example, Evan Braden Montgomery, U.S.-China Competition in Defense Technological and Industrial Development: Implications for the Balance of Power over the Long Term, Study of Innovation and Technology in China research brief (University of California Institute on Global Conflict and Cooperation, 2017), 2, http://escholarship.org/uc/item/3nx3n18x.


51. Roff, 217, 222.


53. Straub, 45.


61. Some readers may take issue with the plausibility of some details in one or more of the following scenarios. These scenarios, however, are intended to be illustrative rather than predictive. The backgrounds laid out here are intended to be plausible enough to demonstrate how AWS might impact a crisis, not to predict that the details of these scenarios will actually come to pass.

62. This scenario is based not only on the Russian jet shot down by Turkey in 2015 but also on the Patriot and Harpoon systems’ friendly fire incidents, discussed above.


64. This scenario is loosely based on the Hainan Island incident of 2001 and more recent US freedom of navigation operations in the Pacific.


70. This is based on the Syrian chemical weapons redline breached in August 2013, US operations in the Balkans in the 1990s, and the no-fly zone over Kurdish regions of Iraq in the 1990s.


73. Schelling, Arms and Influence.


75. Horowitz, “Who’ll Want AI Weapons?”

76. For an excellent comparative discussion of how different strategic cultures viewed the technologies, weapons, and doctrines of the Second Offset, see Dima Adamsky, The Culture of Military Innovation: The Impact of Cultural Factors on the Revolution in Military Affairs in Russia, the U.S., and Israel (Stanford, CA: Stanford University Press, 2010).

Disclaimer

The views and opinions expressed or implied in SSQ are those of the authors and are not officially sanctioned by any agency or department of the US government. We encourage you to send comments to: strategicstudiesquarterly@us.af.mil