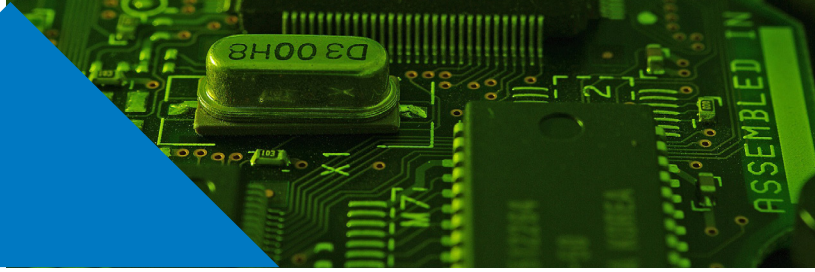
CNA
ANALYSIS & SOLUTIONS



INCORPORATING AUTONOMY INTO WARFIGHTING

A CRAWL-WALK-RUN APPROACH

The benefits, risks, and sensitivities surrounding autonomous weapon systems (AWS) demand an objective analytical approach to answer both whether and how the U.S. should explore the use of such systems. CNA analysis identifies that these technologies could bring important—potentially even critical—capabilities to the U.S. military, and singles out opportunities to explore AWS in lower-risk operational environments.

Autonomous weapon systems (AWS) are expected to revolutionize warfighting, with the potential to bring substantial new capabilities and capacity to militaries around the world. Indeed, the current U.S. National Security Strategy notes that "new advances in computing, autonomy, and manufacturing are already transforming the way we fight" [1]. Weapon systems are considered autonomous if they select and engage targets without human intervention.

Taking humans out of the loop when it comes to decisions to apply force presents risks, however. For example, will the systems act as intended? Can they adequately discriminate valid military targets from civilians, and adversary forces from friendly forces? As a result of broad practical, ethical, and legal concerns that some have about AWS, the UN is currently holding discussions on AWS. Many countries are open to the idea of some kind of restriction or code of conduct for such systems, and almost two dozen countries support implementing a preemptive ban on AWS [2]. Such risks and sensitivities challenge the U.S. and other countries to consider how to responsibly pursue the development of AWS—or whether to pursue it at all.

MITIGATE RISKS WHEN AWS MAY BE CRITICAL

Whenever manned or remotely operated systems cannot function effectively in warfighting, autonomous systems may be able to provide critical capabilities to the warfighter. CNA analysis identified important potential warfighting contexts in which this may be the case, due to real-time human control or oversight not being feasible. The use of AWS in such situations may be of critical importance.

One such context would be when U.S. forces must combat threats that are too numerous, fast, and/or dynamic for human control or oversight of countermeasures to be feasible. A large, autonomous aerial swarm could be one such threat. American AWS could adapt to the dynamic behavior of a swarm attack and prosecute it at machine speed, potentially by coordinating hundreds or thousands of individual weapons. CNA analysis suggests that U.S. forces should expect to encounter autonomous weapons such as aerial swarms on the battlefield, for even if the use of such systems is bound by an international agreement, it is likely that not all states would become parties to the agreement; non-state actors such as terrorist groups will also have access to AWS technologies [3].

Another context in which AWS may sometimes be the only feasible solution is in environments too dangerous for manned platforms and in which communications are denied, making the use of remotely operated systems such as remotely piloted aircraft impossible. It is not difficult to anticipate such an environment in war, when an adversary could employ communications jamming as well as other anti-access and area denial measures that are able to destroy approaching forces. In situations such as this, autonomous systems may be the U.S. military's only viable choice.

AWS may be critical in operational contexts like these, validating U.S. efforts to continue to explore AWS technologies. However, the risk that military personnel are unable to detect or intervene in real time if systems do not behave as intended may be especially acute when human oversight is infeasible. Therefore, we recommend that the U.S. military focus initial efforts on establishing measures designed to ensure that AWS will behave as intended—or that the risk of unintended effects can be mitigated—before any systems are employed.[1]

BEGIN AWS EXPLORATION IN LOWER-RISK CONTEXTS

Of the potential uses of AWS identified by CNA for the U.S. Navy that could provide important capabilities, we noted two categories in which the use of autonomy would involve limited risk:

1. Some suggestions for such measures are proposed in [4], see also [5].

- Maritime local defense
- The underwater domain

The risk of collateral damage is relatively low in both these contexts. Indeed, maritime local defense includes scenarios such as a ship at sea defending itself from missile and torpedo threats, and the underwater domain has limited traffic volume. Another reason these contexts involve more limited risk is that they already involve the employment of systems that share some characteristics with AWS. For example, the Aegis Combat System and the Phalanx Close-In Weapon System (CIWS) are capable of automatically defending naval ships against incoming missiles and aircraft while under operator supervision. In the underwater environment, because communications are very limited, manned submarines and unmanned underwater systems can operate for extended periods of time without any communications with theater commanders or other forces.

We recommend that the U.S. military employ a "crawl-walk-run" approach as it explores the use of AWS technologies. U.S. efforts at this time should focus on the use of AWS in lower risk contexts such as those described here, in addition to developing measures to mitigate risks associated with AWS as noted above. Both these risk mitigations and the lessons and best practices determined from exploring AWS in lower risk contexts should then be applied to subsequent explorations of AWS uses in other operational contexts, as the start of an iterative approach.

Declining to explore the potential use of AWS on the battlefield will present a risk to U.S. military dominance. The "crawl-walk-run" approach we describe here will allow the U.S. to explore the use of AWS while addressing the risks and sensitivities that they carry.

References

[1] White House. 2017. National Security Strategy of the United States of America. https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

[2] Campaign to Stop Killer Robots. "Country Views on Killer Robots: 16 November 2017." Campaign to Stop Killer Robots website. http://www.stopkillerrobots.org/wp-content/uploads/2013/03/KRC_CountryViews_16Nov2017.pdf.

[3] CNA. Arms Control and Lethal Autonomy: The Past Points Toward the Future.

[4] Lewis, Larry. Insights for the Third Offset: Addressing Challenges of Autonomy and Artificial Intelligence in Military Operations. CNA DRM-2017-U-016281-Final. Sep. 2017. https://www.cna.org/CNA_files/PDF/DRM-2017-U-016281-Final.pdf.

[5] CNA. Insights for the Third Offset: Addressing Challenges of Autonomy and Artificial Intelligence in Military Operations. https://www.cna.org/CNA_files/PDF/AI_10172017.pdf

CNA CENTER FOR AUTONOMY AND AI

CNA's Center for Autonomy and AI supports the U.S. goal of effectively incorporating autonomy, AI, and related technologies in military capabilities. Throughout history, the ability to adapt technological advances to warfighting has led to fundamental changes in how war is conducted and the tools used in its conduct. Autonomy and AI represent revolutionary technologies in warfare which offer opportunities to the U.S. for countering and deterring emerging threats, addressing security challenges and advancing U.S. national interests. But this opportunity is by no means certain, since autonomy also offers potential asymmetric advantages to near-peer competitors, some of which have been pursuing these capabilities aggressively. Likewise, rapid innovation in the private sector and a commercial research and development sector dwarfing that of the U.S. military create new challenges for the U.S., which will need to quickly identify and integrate cutting edge technological developments in this rapidly changing environment.

Because of the foundational impact autonomy and artificial intelligence will have on the character of warfare, CNA created the Center for Autonomy and Artificial Intelligence to focus on these emerging technologies and their contribution to national security. The Center capitalizes on the ability to leverage the scientists and analysts of CNA's staff of 600, with their experience base in military operations, test and evaluation, security and intelligence analyses, technology assessment, and autonomy and AI.

ABOUT CNA CORPORATION

CNA is a not-for-profit research and analysis organization with 75 years of experience providing government agencies with data-driven insights and real-world, actionable solutions grounded in our direct experience with the operational environments where these solutions are applied. CNA developed the foundational techniques for operational analysis to address complex challenges facing government programs. We have applied these techniques successfully in areas ranging from defense to aviation, education, justice, and homeland security.

For more information please contact:
Dr. Lawrence L. Lewis, Director, Center for Autonomy and AI
703-864-2020
Lewisl@cna.org

Dr. Diane M. Vavrichek, Research Scientist
703-824-2557
Vavrichekd@cna.org