United States Marine Corps
School of Advanced Warfighting
Marine Corps University
3070 Moreell Avenue
Marine Corps Combat Development Command
Quantico, VA 22134

FUTURE WAR PAPER

Artificial Intelligence and the First to Fight: The Implications of Artificial Intelligence for Forward-Deployed and Early-Deploying Forces in Contingency Operations

SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF OPERATIONAL STUDIES

Major Joshua E. Cavan, USMC

AY 2017-18

Mentor: Dr. Wray R. Johnson

Approved: 

Date: 

DISCLAIMER

THE OPINIONS AND CONCLUSIONS EXPRESSED HEREIN ARE THOSE OF THE INDIVIDUAL STUDENT AUTHOR AND DO NOT NECESSARILY REPRESENT THE VIEWS OF EITHER THE SCHOOL OF ADVANCED WARFIGHTING OR ANY OTHER GOVERNMENTAL AGENCY. REFERENCES TO THIS STUDY SHOULD INCLUDE THE FOREGOING STATEMENT

Introduction

Artificial intelligence has the potential to significantly affect the way civilian and military leaders make decisions in contingency situations. Artificial intelligence is machine intelligence, as opposed to natural, human intelligence. Machine learning drives artificial intelligence. Massive amounts of data enable machine learning. Computers sort through this data to solve problems and uncover trends and patterns. Artificial intelligence is already in use at the tactical level, in some automated weapons systems, in logistics systems, and for limited applications in targeting and intelligence.[1] Several nations, to include the United States, are working on expanding the use of artificial intelligence partnered with human analysts, planners, and decision makers as part of a decision support process at the operational level of war.[2] Artificial intelligence in support of operational decision making is the use of machine learning to expose key trends and patterns to guide decisions on when, where, and under what conditions to seek battle. The use of artificial intelligence as an operational-level decision support tool will change the way forward-deployed and early-deploying forces operate, shifting their focus to data collection while creating opportunities for surprise.

Artificial Intelligence to Support Decision Making

MCDP 6, *Command and Control*, defines command and control as "the means by which a commander recognizes what needs to be done and sees to it that appropriate actions are taken."[3] MCDP 6 uses John Boyd's Observe-Orient-Decide-Act loop to describe the command and control process and to describe the importance of generating tempo in command and control. In a competitive environment, such as warfare, whichever side's command and control and

decision-making processes enables them to cycle through the Observe-Orient-Decide-Act loop faster is likely to gain a temporal advantage.

Artificial intelligence integrated into decision support systems may be a way to gain a temporal advantage. The promise of artificial intelligence is that it can quickly process a large volume of data, convert that data to information, and point to courses of action based on an algorithm. Artificial intelligence can pull together disparate sources of information in ways and at a speed beyond the limits of human cognitive processing.

In this role, artificial intelligence is like a "Robot General Staff."[4] Much like the original Prussian General Staff, a Robot General Staff would use machine learning as its *Bildung*, or intellectual development to contribute to the collective genius of the staff.[5] This does not mean removing human staff members and decision makers from the process, rather it complements their efforts through automation and an expansion of the potential knowledge base.

The expanded knowledge base of an artificial intelligence enabled decision-making process expands the feedback loops and pushes the system more toward the vision of a "Cybernetic" system. The promise of Cybernetics has been to increase the efficiency of command and control processes in mechanical systems, manufacturing, and national security through efficient feedback loops that accurately sense the system and automatically adjust to keep the system at a desired state.[6] Artificial intelligence can speed feedback loops and increase the efficiency of Cybernetic control processes.

The limitation of artificial intelligence is that the machine learning behind the artificial intelligence needs vast amounts of data. This was true of early efforts to employ artificial intelligence in support of weapons systems as part of a Cybernetic control system. Norbert Wiener, of the Massachusetts Institute of Technology, a scientist and founder of the field of

Cybernetics, developed an early computer to guide anti-aircraft guns during World War II that promised to aim the rounds based on predictions of a pilot's evasive maneuvers. Weiner was never able to field the system because he could not collect enough data on actual evasive maneuvers to drive the system's machine learning. Moreover, the development of proximity fuses provided an effective alternative that did not require machine learning.[7] Today, however, a proliferation of sensors and vast improvements in processing power promises an abundance of useable data to support machine learning.

Data Drives Machine Learning

Collecting sufficient data to support the machine learning of military artificial intelligence systems is likely to become an important task for forward-deployed and early-deploying forces, including country teams, special operations forces, expeditionary forces, naval forces, air forces, and forward-deployed ground forces. These forces complement traditional technical means of gathering data on potential adversaries and the operating environment. These forces must recognize the importance of data collection and integrate it into their operations.

The importance of data collection may change how forward-deployed and early-deploying forces operate. Before the outbreak of conflict (during shaping and deterrence phases), these forces may need to fly, sail, or operate in contested areas or near the exercises of potential adversaries to collect data on adversary responses. They may also need to sense and track civilian patterns. They must have plans to retain, share, analyze, and use this data. Once a conflict has begun, forward-deployed and early-deploying forces must "fight to know," conducting operations such as reconnaissance in force and armed reconnaissance. The purpose

of these operations will be to collect data on adversary dispositions to aid machine learning, analysis, and subsequent understanding of adversary intentions.

There is, however, a risk that the data collected by forward-deployed and early-deploying forces will not actually represent what actions potential adversaries will take during a conflict. Adversaries are likely to change the way they operate after the outbreak of conflict. This may be because of a loosening of restraints and safety checks or because adversaries are deliberately hiding capabilities and intentions from observation during pre-conflict phases with the intent to deceive. An increase in tensions or the outbreak of conflict is also likely to change the patterns in the operating environment. These changes may be enough to invalidate pre-conflict machine learning.

Thus, there is risk and opportunity in pre-conflict machine learning to enable artificial intelligence in support of decision-making. Reliance on pre-conflict data can lead to bad decisions or unintended consequences. There is also the risk of falling prey to an adversary's deception operations. Artificial intelligence, based on data collected by forward-deployed and early-deploying forces may, however, be able to quickly spot significant deviations from pre-conflict patterns and drive tempo in decision making. Analysis of adversary use of artificial intelligence also provides opportunities to protect one's own operations through surprise.

Opportunities for Surprise- Deception, Ambiguity, and Stealth

MCDP 1, *Warfighting*, identifies surprise as "a genuine source of combat power in its own right because of its psychological effect."[8] Surprise can result from the use of artificial intelligence in the same way surprise can result from a purely human decision-making process. In any decision-making process, the decisions are only as good as the information collected to

support the decision, and the biases of those in the decision-making process. Algorithms rely only on data collected (unless programmers or machine learning systems explicitly recognize potential gaps) and are also prone to biases in analysis and decision making.[9] Gaps and biases will still exist, and can result in surprise. MCDP-1 lists three ways to achieve surprise: deception, ambiguity, and stealth.[10] Artificial Intelligence will have an impact on all three ways.

Deception is defined as "convinc[ing] the enemy we are going to do something other than what we are really going to do in order to induce him to act in a manner prejudicial to his own interests."[11] With deception, an adversary is surprised because all of the data he collected led him confidently to a conclusion that is not only wrong, but puts the adversary at a clear disadvantage. During the preparations for Operation Overlord, the invasion of Northwest Europe in World War II, the Allies successfully used deception. Through the creation of a fake Army Group and carefully leaked information, they convinced the Germans that the actual landings would take place at the Pas de Calais instead of Normandy. Even after the actual landings on 6 June had already occurred, the Germans withheld operational reserves as late as July because of a belief that the actual invasion was still coming at the Pas de Calais.[12]

Decision-making processes reliant upon artificial intelligence are prone to the same types of deception because data collected and analyzed by artificial intelligence can point to the wrong conclusion if an adversary has arranged the data to lead to a desired (and disadvantageous) conclusion. An adversary may present a deliberately misleading picture to forward-deployed and early-deploying forces to influence decision making. Soviet strategic planners developed the concept of "reflexive control" with this in mind. Reflexive control is "a means of conveying to a partner or an opponent specially prepared information to incline him to voluntarily make the predetermined decision desired by the initiator of the action."[13] The controlled release of false

and misleading information designed to play into an opponent's biases is designed to drive the opponent to make a decision on his own that is advantageous to the other side. An adversary may target forward-deployed and early-deploying forces with information that confirms the biases in their artificial intelligence enabled decision making systems and lead those forces to choose a less advantageous course of action.

Forward-deployed and early-deploying forces must counter deception efforts by collecting information that would indicate the adversary has chosen something other than his most likely course of action. They must consider deception as an explanation for patterns in the operating environment. They must recognize biases and act to consider information that does not confirm those biases.

Ambiguity is the second way to achieve surprise. Ambiguity is "to act in such a way that the enemy does not know what to expect."[14] Russian forces practiced ambiguity in their 2014 annexation of Crimea. Initial forces moved under the cover of routine resupply missions to a Russian naval base in Crimea. Other forces moved with strict signals discipline and wore no insignia. These "little green men" secured key infrastructure, contained Ukrainian forces within their bases, and disrupted the Ukrainian military response. The ambiguity of the forces invading Crimea helped to delay any coherent international response and contributed to Russia's success in annexing Crimea at relatively low cost.[15]

Ambiguity can challenge decision-making processes reliant upon artificial intelligence. Subtle shifts to conceal information can easily confuse algorithms programmed to look for certain information and reliant on automated data analysis.[16] MCDP 2, *Intelligence*, discusses the problem of signals and noise in analysis. Signals are valuable pieces of information, while noise is that which is not valuable – because it is wrong, misleading, or ambiguous.[17] Noise can

deliberately mask a signal and make that signal seem ambiguous. Intelligence collectors and analysts must often seek out sources of noise and apply filters and judgement to discern signals among the noise. Artificial intelligence driven analysis must do the same or risk falling prey to ambiguity.

Forward-deployed and early-deploying forces must act to resolve ambiguity. They must take every opportunity to identify units and unusual traffic moving in conflict areas. They must be suspicious of "routine" missions and observe closely to verify that these movements are not a bid to achieve surprise. They must use multiple means to verify information, to ensure that noise is not concealing an important signal.

Stealth is the last way to achieve surprise. Stealth is to "deny the enemy any knowledge of impending action" through ignorance.[18] In 1991, during Operation Desert Storm, Iraqi forces had a limited ability to observe the action of coalition forces massing in Saudi Arabia. The coalition took further action to degrade this capability through the destruction of the Iraqi Air Force and Iraq's forward sensor network. Coalition forces exploited Iraq's ignorance. Two armored corps used stealth to move more than 100 miles to the west through the Saudi desert and away from the expected direction of attack in the east along the Gulf Coast into Kuwait. The coalition forces attack through the desert exploited the Iraqi ignorance to achieve surprise, leading to a lopsided victory.[19]

Stealth is also a challenge to decision-making processes reliant upon Artificial Intelligence because the absence of data creates gaps for analysis and algorithmically-driven recommendations. Degraded or destroyed sensors can lead to information gaps. Sensors may have gaps in coverage or capability that an adversary can exploit. Signature management can lead to stealth. Weather, smoke, or other atmospheric conditions can enable stealth. Algorithms

must recognize the gaps in data collection and consider adversary action to exploit those gaps as a course of action.

Forward-deployed and early-deploying forces can help to combat stealth. Using multiple sensors and collection means can expose stealth designed to defeat one type of system. Patrolling to reconnoiter in unexpected areas can lead to chance encounters that disrupt adversary efforts at stealth. Systems masking their signatures may not be able to mask the signature of key support systems, such as fuel tankers, leaving them vulnerable to observation. Algorithms may be able to recognize patterns that lead to the discovery of hidden activities such as tunneling or preparations for infiltration.

Warfighting recognizes surprise as particularly useful in generating combat power (alongside boldness). Artificial intelligence supported decision-making processes can be vulnerable to surprise. Forward-deployed and early-deploying forces must work with artificial intelligence to guard against surprise.

Guarding Against Surprise

There are ways to guard against surprise. These include working with artificial intelligence on a regular basis to develop proficiency, red teaming the decision-making process, continuous learning by both humans and machines once conflict begins, and avoiding formulaic or predictable decision-making. These methods are all easier said than done, but the integration of artificial intelligence presents significant advantages in light of the risks.

The way to gain proficiency working with artificial intelligence as part of the decision-making process is through exercises and wargaming. Training forward-deployed and early-deploying forces to work as a human-machine team along with artificial intelligence develops

the ability of forward-deployed forces to provide relevant data for machine learning, generates data to drive machine learning, and develops the ability of staffs to work with artificial intelligence to solve operational problems. An increase in the number of repetitions for scenarios can help artificial intelligence gain an appreciation for areas where an adversary can achieve surprise and opportunities to surprise an adversary.

However, exercises and wargames have their limitations. Pre-conflict exercises may not replicate actual battlefield conditions sufficiently for data generated during these exercises to be relevant. A scarcity of reliable data to drive computer models of the operational environment in wargames. RAND Corporation researchers Paul K. Davis and Donald Blumenthal described this as the "base of sand" problem in 1991, and it is still relevant today.[20] Without realistic, verified data, combat models only serve as a tool for exploration rather than prediction. Since warfare is a complex adaptive system, it is highly sensitive to initial conditions. As Center for Naval Analyses researcher Dr. Andrew Illachinski demonstrated when attempting to model combat, very small changes in initial conditions to individual actors can have disproportionate effects on the outcome.[21] This makes it hard to accurately predict detailed results from a model. It also makes it difficult to certify that artificial intelligence taking part in a wargame is conducting machine learning that is relevant to real-world conditions. Worse, the artificial intelligence may learn the wrong lessons and have an inaccurate view of capabilities and intentions in the real world.

Red teaming can help mitigate some of the limitations of artificial intelligence and guard against surprise. Red teaming provides "an independent capability to fully explore alternatives in plans, operations, concepts, organizations and capabilities in the context of the operational environment and from the perspectives of partners, adversaries and others."[22] Red teams should

look at the algorithms used in decision-making processes to identify biases and gaps in analysis. Red teams should also test the alternative competing hypothesis that an adversary is trying to deceive.[23] Programmers should develop algorithms that incorporate artificial critical thinking functions using red teaming techniques, to include looking at deception as an alternative competing hypothesis.

Just like humans, machines shouldn't stop learning once a conflict begins. Even if pre-conflict data leads to some sort of surprise, forward-deployed and early-deploying forces should continue to collect as much data as possible to drive continuous learning for both humans and artificial intelligence. This data is arguably more valuable than pre-conflict data because it comes in the context of a consistent re-evaluation of the operational environment. Whichever side learns faster and enables better decision making has the potential to achieve an advantage in subsequent rounds of competition.

The most important way to guard against surprise is to avoid being formulaic or predictable in decision making. There is risk of becoming too mechanistic when there is too much dependence on artificial intelligence at the expense of human creativity. This may be one of the advantages the United States and our allies have over authoritarian societies if all sides have artificial intelligence of equal quality.

The Way Ahead

The pursuit of artificial intelligence to support operational decision making must continue because of the potential to enhance decision making and generate tempo. The United States must also continue to pursue artificial intelligence capabilities because of the real possibility that our adversaries will also develop and employ these capabilities.[24] The pursuit of artificial

intelligence in support of decision making comes with risks and opportunities and will impact the priorities for forward-deployed and early-deploying forces.

The United States must closely monitor potential adversary uses of artificial intelligence. Adversary algorithms must be a primary target for espionage. Conversely, our own algorithms become critical information to protect. Knowing an algorithm is like intimately knowing a decision maker and his staff. The algorithm gives insight into the biases of the decision-making process and illuminates ways to exploit the decision maker and achieve surprise through deception, ambiguity, or stealth.

The United States must look for opportunities to exploit adversary artificial intelligence to achieve surprise. This may be by exploiting overly formulaic decision making. Adversaries who favor centralized command and control are likely to use artificial intelligence to centralize control. Decentralized application of artificial intelligence, with loose synchronization, may help generate a faster tempo of decision making over a centralized adversary.

The United States may also be able to intentionally skew adversary data collection through false data, ambiguity, or stealth. Anticipating adversary use of artificial intelligence to gain insight into our operations leads us to the need to counter this through creativity – doing the unexpected to gain an advantage.

Forward-deployed and early-deploying forces must be aware of their role as a data collector. They must work to prevent surprise by operating to deny potential adversaries the ability to deceive, to be ambiguous, or to use stealth. They must prioritize the data they collect, giving greater weight to that which is most representative of probable conditions after the outbreak of conflict. Forward-deployed and early-deploying forces must develop effective filters to cut through adversary noise and focus on the right signals.

Forward-deployed and early-deploying forces also have a role in achieving surprise. They can present deceptive or ambiguous profiles to potential adversaries and must hide key capabilities to achieve stealth. Pre-conflict operations can test whether an adversary is likely to detect certain tactics or capabilities or can present false data to an adversary to aid in achieving an advantage through surprise.

Forward-deployed and early-deploying forces must develop their *Bildung* along with their artificial intelligence. Forces in contact with adversaries on a daily basis who study and observe the way that adversary operates and exercises can best judge the accuracy of analysis supported by artificial intelligence. Knowing an adversary well positions forward-deployed and early-deploying forces best to apply judgement and creativity to overcome surprise and turn the tables on an adversary to gain an advantage through tempo or surprise.

Conclusion

In conclusion, the use of artificial intelligence as part of the decision-making process increases the importance of data collection operations for forward-deployed and early-deploying forces and creates opportunities for surprise. Collecting valuable data while guarding against surprise will be critical parts of our decision-making process. With good data, the proper application of judgement, the avoidance of formulaic or predictable decision-making, and the use of data to deceive the adversary and protect our own information, we can use artificial intelligence to generate tempo in command and control and achieve surprise, which can translate into a decisive operational advantage.

---

[1] Bradley Peniston, "How Will The Pentagon Create Its AIs? The Algorithmic-Warfare Team Is Charting a Path," *Defense One*, July 13, 2017, http://www.defenseone.com/technology/2017/07/artificial-intelligence-pentagon/139402/?oref=search_cukor.

[2] Paul Mozur and John Markoff. "Is China Outsmarting America in A.I.?" *New York Times*, May 27, 2017, https://www.nytimes.com/2017/05/27/technology/china-us-ai-artificial-intelligence.html and The White House, *The National Security Strategy of the United States of America* (Washington, DC, December 2017), https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf, 20, 34.
[3] Headquarters US Marine Corps, *Command and Control*, MCDP 6 (Washington, DC: Headquarters US Marine Corps, October 4, 1996), 37.
[4] Anthony S. Cruz, "The Robot General: Implications of Watson on Military Operations," *Armed Forces Journal*, June 1, 2011, http://armedforcesjournal.com/the-robot-general/ and Benjamin Jensen and Ryan Kendall, "Waze for War: How the Army Can Integrate Artificial Intelligence," *War on The Rocks*, September 2, 2016, https://warontherocks.com/2016/09/waze-for-war-how-the-army-can-integrate-artificial-intelligence/.
[5] The concepts of *Bildung* and collective genius associated with the Prussian General Staff are from Charles Edward White, *The Enlightened Soldier: Scharnhorst and the* Militarische Gesellschaft *in Berlin 1801-1805* (New York, Prager, 1989).
[6] Thomas Rid, *Rise of the Machines: A Cybernetic History* (New York: W. W. Norton & Co., 2016), 2-4.
[7] Ibid., 29-36.
[8] Headquarters US Marine Corps, *Warfighting*, MCDP 1 (Washington, DC: Headquarters US Marine Corps, June 20, 1997), 42.
[9] Pedro Domingos, *The Master Algorithm: How the Quest for The Ultimate Learning Machine Will Remake Our World* (New York: Basic Books, 2015) discusses different types of algorithms used in machine learning and the gaps and biases inherent in each type of algorithm.
[10] Ibid., 43-44.
[11] Ibid., 43-44.
[12] Gordon A. Harrison, *Cross-Channel Attack* (Washington, DC: US Army Center of Military History, 1951), 350-351.
[13] Timothy L. Thomas, "Russia's Reflexive Control Theory and the Military," *Journal of Slavic Military Studies* 17, 2004, 237.
[14] *Warfighting*, 44.
[15] Mary Ellen Connell and Ryan Evans, Russia's "Ambiguous Warfare" and Implications for the U.S. Marine Corps (Arlington, VA: Center for Naval Analyses, May 2015), https://www.cna.org/CNA_files/PDF/DOP-2015-U-010447-Final.pdf, 9-10.
[16] A. Nguyen, J. Yosinski, and J. Clune, "Deep Neural Networks are Easily Fooled: High Confidence Predictions for Unrecognizable Images," Computer Vision and Pattern Recognition (CVPR '15) Conference Paper, IEEE, 2015, www.evolvingai.org/fooling.
[17] Headquarters US Marine Corps, *Intelligence*, MCDP 2 (Washington, DC: Headquarters US Marine Corps, June 7, 1997), 47-48.
[18] *Warfighting*, 44.
[19] Michael R. Gordon and Bernard E. Trainor, *The Generals' War: The Inside Story of The Conflict in The Gulf* (Boston: Little, Brown, and Company, 1995).
[20] Paul K. Davis and Donald Blumenthal, *The Base of Sand Problem: A White Paper on the State of Military Combat Modeling* (Santa Monica, CA: RAND, 1991), v-vii. https://www.rand.org/pubs/notes/N3148.html and Shawn Woodford, "Wargaming Multi-Domain Battle: The Base of Sand Problem," *Mystics & Statistics* (blog), The Dupuy Institute, April 10, 2017, www.dupuyinstitute.org/blog/2017/04/10/wargaming-multi-domain-battle-the-base-of-sand-problem/.
[21] Andrew Ilachinski, *Artificial War: Multiagent Based Simulation of Combat* (River Edge, NJ: World Scientific Publications, 2004).
[22] University of Foreign Military and Cultural Studies Center for Applied Critical Thinking, *Critical Thinking Handbook v8.1* (US Army Training and Doctrine Command G2, Fort Leavenworth, KS, September 2016), 1.
[23] *Critical Thinking Handbook v8.1*, 132-133.
[24] Elsa B. Kania, *Battlefield Singularity: Artificial Intelligence, Military Revolution, and China's Future Military Power*, Washington, DC: Center for a New American Security, November 2017. https://www.cnas.org/publications/reports/battlefield-singularity-artificial-intelligence-military-revolution-and-chinas-future-military-power discusses China's efforts to integrate artificial intelligence into its command and control process.

Bibliography

Chase, Michael S., Jeffrey Engstrom, Tai Ming Cheung, Kristen A. Gunness, Schott Warren Harold, Susan Puska, Samuel K. Berkowitz. *China's Incomplete Military Transformation: Assessing the Weaknesses of the People's Liberation Army (PLA)*. Santa Monica, CA: RAND, 2015. https://www.rand.org/content/dam/rand/pubs/research_reports/RR800/RR893/RAND_RR893.pdf.

Connell, Mary Ellen and Ryan Evans. *Russia's "Ambiguous Warfare" and Implications for the U.S. Marine Corps.* Arlington, VA: Center for Naval Analyses, May 2015. https://www.cna.org/CNA_files/PDF/DOP-2015-U-010447-Final.pdf.

Davis, Paul K. and Donald Blumenthal. *The Base of Sand Problem: A White Paper on the State of Military Combat Modeling.* Santa Monica, CA: RAND, 1991. https://www.rand.org/pubs/notes/N3148.html.

Domingos, Pedro. *The Master Algorithm: How the Quest for The Ultimate Learning Machine Will Remake Our World*. New York: Basic Books, 2015.

Erfurt, Waldemar. *Surprise.* FMFM 12-1. Translated by Daniel Vilfroy. Washington, DC: Headquarters US Marine Corps, 1988 (republication of the 1943 original). https://permanent.access.gpo.gov/lps83767/FMFRP%2012-1%20%20Surprise.pdf.

Ekelhof, Merel. "Human Control in the Targeting Process." *Autonomous Weapon Systems: Implications of Increasing Autonomy in the Critical Functions of Weapons (Expert Meeting).* Versoix, Switzerland: International Committee of the Red Cross, March 15-16 2016. https://www.icrc.org/en/publication/4283-autonomous-weapons-systems.

Headquarters, US Marine Corps. *Warfighting*. MCDP 1. Washington, DC: Headquarters US Marine Corps, June 20, 1997.

Headquarters, US Marine Corps. *Intelligence*. MCDP 2. Washington, DC: Headquarters US Marine Corps, June 7, 1997.

Headquarters, US Marine Corps. *Planning*. MCDP 5. Washington, DC: Headquarters US Marine Corps, July 21, 1997.

Headquarters, US Marine Corps. *Command and Control*. MCDP 6. Washington, DC: Headquarters US Marine Corps, October 4, 1996.

Ilachinski, Andrew. *Artificial War: Multiagent Based Simulation of Combat.* River Edge, NJ: World Scientific Publications, 2004.

Kania, Elsa B. *Battlefield Singularity: Artificial Intelligence, Military Revolution, and China's Future Military Power.* Washington, DC: Center for a New American Security,

November 2017. https://www.cnas.org/publications/reports/battlefield-singularity-artificial-intelligence-military-revolution-and-chinas-future-military-power.

Kowaleski, Annie. "Disinformation and Reflexive Control: The New Cold War." *Georgetown Security Studies Review*, February 1, 2017, http://georgetownsecuritystudiesreview.org/2017/02/01/disinformation-and-reflexive-control-the-new-cold-war/.

Mateski, Mark. "Russia, Reflexive Control, and the Subtle Art of Red Teaming." *Red Team Journal*, October 13, 2016, https://redteamjournal.com/2016/10/reflexive-control/#identifier_2_6791.

Mozur, Paul and John Markoff. "Is China Outsmarting America in A.I.?" *New York Times*, May, 27, 2017, https://www.nytimes.com/2017/05/27/technology/china-us-ai-artificial-intelligence.html.

Osinga, Frans P. B. *Science, Strategy, and War: The Strategic Theory of John Boyd*. New York, Routledge, 2007.

Peniston, Bradley. "How Will The Pentagon Create Its AIs? The Algorithmic-Warfare Team Is Charting a Path." *Defense One*, July 13, 2017, http://www.defenseone.com/technology/2017/07/artificial-intelligence-pentagon/139402/?oref=search_cukor.

Rid, Thomas. *Rise of the Machines: A Cybernetic History*. New York: W. W. Norton & Co., 2016.

Singer, P. W. *Wired for War: The Robotics Revolution and Conflict in the Twenty-First Century*. New York: Penguin Press, 2009.

Surdu, John R. and Kevin Kittka. "Deep Green: Commander's toll for COA's Concept." *Computing, Communications, and Control Technologies*: CCCT 2008. Orlando, FL, 29 June - 2 July 2008. http://www.bucksurdu.com/Professional/Documents/TheDeepGreenConcept.pdf.

Thomas, Timothy L. "Russia's Reflexive Control Theory and the Military." *Journal of Slavic Military Studies* 17, no. 2 (2004): 237-256.

Tucker, Patrick. "The Next Big War Will Turn on AI, Says US Secret-Weapons Czar." *Defense One*, March 28, 2017, http://www.defenseone.com/technology/2017/03/next-big-war-will-turn-ai-says-pentagons-secret-weapons-czar/136537/.

US Army Training and Doctrine Command G-2. "The Operational Environment and the Changing Character of Future Warfare." *US Army TRADOC Mad Scientist Laboratory*, posted November 29, 2017. https://community.apan.org/wg/tradoc-g2/mad-scientist/m/articles-of-interest/215990.

US Army Training and Doctrine Command G-2 Mad Scientist Initiative. Án Advanced Engagement Battlespace: Tactical, Operational and Strategic Implications for the Future Operational Environment." *Small Wars Journal*, October 23, 2017. http://smallwarsjournal.com/jrnl/art/an-advanced-engagement-battlespace-tactical-operational-and-strategic-implications-for-the-.

Watson, Ben. "3 Questions: Artificial Intelligence and the Military." *Defense One*, August 25, 2017, http://www.defenseone.com/technology/2017/08/3-questions-artificial-intelligence-and-military/140538/?oref=d-dontmiss.

Weisgerber, Marcus. "The Pentagon's New Algorithmic Warfare Cell Gets Its First Mission: Hunt ISIS." *Defense One*, May 14, 2017, http://www.defenseone.com/technology/2017/05/pentagons-new-algorithmic-warfare-cell-gets-its-first-mission-hunt-isis/137833/?oref=d-dontmiss.