VIEW

Penetrating Artificial Intelligence–enhanced Antiaccess/Area Denial

A Challenge for Tomorrow's Pacific Air Forces

Maj Richard Uber, PhD, USAF

Abstract

To ensure a free and open Indo-Pacific, the United States Air Force (USAF) must maintain its ability to freely operate in international airspace and project force forward to deter aggression. Future improvements to antiaccess/area-denial (A2/AD) systems will certainly include artificial intelligence (AI). AI is a strategic priority of our adversaries, as it can provide significant benefits for national defense. The USAF must be prepared to tackle these technical challenges to uphold our regional commitments and protect international interests in the Indo-Pacific. Three specific applications relevant to A2/AD are (1) target recognition from multiple fused data sources, (2) improved war gaming with agent-based models, and (3) blockchain-enabled autonomous systems. This article will introduce how these technologies might be integrated into future A2/AD systems and recommend some strategies for addressing and overcoming these challenges.

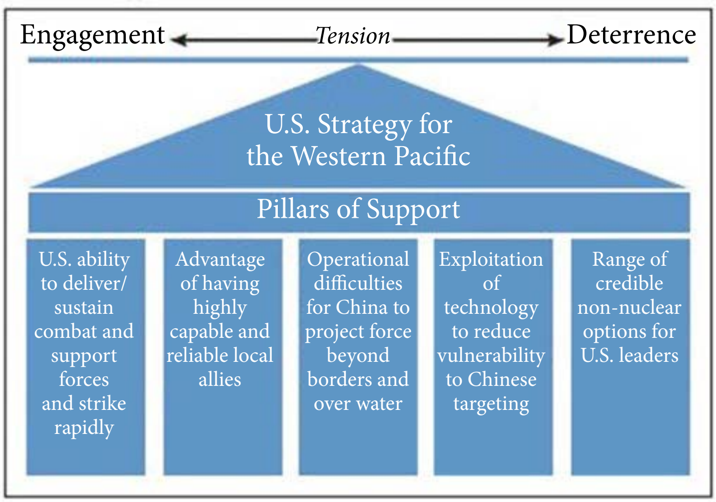
Strategic Setting

To ensure a free and open Indo-Pacific, the United States must maintain its ability to freely operate in international airspace and project force forward to deter aggression. The Department of the Air Force and Pacific Air Forces (PACAF) play a critical role in keeping the peace in this strategically important region. China, after a long period of hide-and-bide tactics has recently started taking more aggressive moves toward strategic strength, what Chinese Communist Party Chairman Xi Jinping refers to as a new long march.[1] While a force-on-force fight is unlikely, demonstrating both the will and ability to fight and win against a strong adversary is fundamental to preventing China from expanding territorial claims by force.

Bolstered by economic growth and investments in modernization, China's current stance in the South China Sea is already strong enough to dissuade neighboring countries from objecting too loudly or forcefully rebutting illegal harassment.[2] However, because China vigorously defends its sovereign interests, conflicts are generally localized where China stands to make strategic gains at very low risk. This strategy appears to rely on China's emphasis on creating a protective bubble of antiaccess/area denial (A2/AD), which has been a paramount priority since the mid-1990s.[3]

The United States has a duty to support Indo-Pacific allies and partners in contesting and deterring Chinese aggression. However, as the People's Liberation Army (PLA) strengthens its A2/AD posture through advanced weapons, improved data processing, and innovative strategies, China's self-confidence and determination grow as well. For the US Department of Defense (DOD) to assure regional partners of its commitment and resolve to confront Chinese belligerence, the US military must continue to develop new ways to defeat China's A2/AD systems.

A 2014 RAND report on US strategy in the Western Pacific proposed five main pillars of support ranging from deterrence to engagement (see fig. 1). This framework emphasizes the requirements for credible military options in the region. Given the PLA's ongoing modernization efforts, the pillar addressing exploitation of technology to reduce risk to forces will play an increasingly important role in US strategy. Underpinning nearly all strategic priorities in the Indo-Pacific is the need for strong relationships with allies and partners in the region.[4] The United States acts as a security guarantor for smaller nations who would not, independently, be able to stand firmly against aggressive coercion. Thus, as Michèle Flournoy, former Under Secretary of Defense for Policy, pointed out, "the United States must also prioritize the development, acquisition, and demonstration of those military capabilities essential to credibly deter Beijing's aggression, deny its ability to rapidly seize territory or create new facts on the ground, and be able to impose significant costs for any act of aggression."[5]



(Image from Terrence Kelly, et al., Developing a U.S. Strategy for Dealing with China — Now and into the Future [Santa Monica, CA: RAND Corporation, 2014], https://www.rand.org/pubs/research_briefs/RB9802.html.)

Figure 1. US strategy for the Western Pacific (RAND)

Chinese Artificial Intelligence Research and Development

Artificial intelligence (AI) has the potential to significantly accelerate the development cycle for new smart, autonomous and networked systems. China's recent emphasis on AI and modernization has attracted attention throughout the DOD and with policy makers and analysts at various levels. The 2017 *New Generation Artificial Intelligence Development Plan* established China's national goal of becoming the world leader in AI by 2030.[6] China not only sees AI as a key enabler for their future economy but also views it as a core national security technology. AI will play a role in future conflicts. Three specific applications relevant to A2/AD are target recognition from multiple fused data sources, improved war gaming with agent-based models, and autonomous systems.

Numerous state-guided research projects have been established to pursue AI and intelligent robotics (autonomy). Notably, the National Natural Science Foundation of China's (NSF-C) list of AI-related projects in 2017 includes topics such as "cross-domain collaborative multi-modal efficient sensing and enhanced intelligence, perception and behavior for machine understanding . . . in an open environment, . . . and man-machine cooperative hybrid intelligence."[7] A small sample of NSF-C funded projects undertaken the PLA Air Force researchers is shown in table 1. Overarching themes visible in the projects are improved signal processing, optimization, applied probability, and machine learning. Many of these applications are basic or applied research that could enable future A2/AD networks.

Additionally, in 2018, China's State Administration of Science, Technology and Industry for National Defence published guidance on cutting-edge technology projects. The first major theme was "intelligent detection and identification and autonomous control technology."[8] More broadly, detection and control technologies should be viewed as enabling technologies for a robust, integrated, networked, and increasingly automated A2/AD system.

Table 1. Selected papers from *Journal of Harbin Institute of Technology* 2018–2019. Affiliation includes "Air Force."

Result	Issue	Title	Affiliations	NSF-C Grant No.
1	2019 (05)	Precession feature extraction of ballistic target based on hybrid-scheme radar network	Air Force Engineering University, Unit 32147 of PLA, Unit 93786 of PLA	61372166, 61501495
2	2019 (05)	Tent chaos and simulated annealing improved moth-flame optimization algorithm	Air Force Engineering University, Northwestern Polytechnical University, Unit 95810 of PLA	61503409

Table 1 (continued)

Result	Issue	Title	Affiliations	NSF-C Grant No.
3	2019 (05)	Latent virus network spreading SEIQRS model and stability analysis	Air Force Engineering University, Unit 95507 of PLA	61573017, 61703420
4	2019 (05)	Modeling and characteristic analysis of clutter for airborne bistatic radar in fixed coordinate system	Air Force Early Warning Academy	51309232
5	2019 (04)	Characteristic functions and effectiveness-of-fit test for uncertain distributions	Air Force Engineering University	71601183, 71571190
6	2019 (04)	Situation assessment for unmanned aerial vehicle air combat based on anti-reasoning rules decision tree	Air Force Engineering University	61601505
7	2019 (04)	A target tracking algorithm for zigzag maneuver target tracking with non-gaussian noises and randomly delayed measurements	Air Force Engineering University, Unit 95910 of PLA	61472441
8	2018 (05)	Ant lion optimization algorithm based on self-adaptive Tent chaos search	Air Force Engineering University	71501184
9	2018 (05)	A low complexity SCL decoding algorithm for polar codes	Air Force Engineering University	61472442
10	2018 (04)	A novel softplus linear unit for deep CNN	Air Force Engineering University	61601499

Threat #1: Target Recognition from Multiple Fused Data Sources

A recent war game simulated an AI-enhanced ground fight where troops were outnumbered three to one by enemy forces. Adding autonomous air and ground sensors allowed troops to smartly detect, target, and engage adversaries (find, fix, finish), realizing an approximate "10–fold increase in combat power."[9] This exercise described a small area and simulated command-and-control (C2) AI that is not currently available to the field. However, it does demonstrate the potential benefits of a fully integrated smart sensor and C2 network.

Research emphasis in terms like "cross-domain collaborative multi-modal efficient sensing" and "intelligent detection and identification" imply that China continues efforts to build a connected network of persistent sensors for domain awareness and early warning. Advanced sensors connected to air defense systems supported by advanced fighter aircraft would make penetrating Chinese-controlled airspace a seriously difficult problem.

In addition to improved sensor fusion and detection algorithms, China has also been investing in hardware such as meter-wave radar technology to counter US low-observable aircraft.[10] Traditional stealth technology is less useful against a combination of sensors spanning both acoustic and electromagnetic (visible, infrared, microwave, etc.) spectra. These sensors may be found onshore and offshore, may be mobile or fixed, and will be networked together through an integrated communications network. The anticipated intent of these advanced sensors must be to connect them to air defense systems, "which will extend across coastal SAM [surface-to-air] sites on the Chinese mainland, missile batteries on artificial islands in the South China Sea, and better anti-aircraft weapons on Chinese warships."[11] Advanced routing algorithms to minimize risk of detection and engagement will be needed to plan strategic strikes.

Threat #2: Advanced War Games

Advances in game theory, agent-based modeling, and machine learning have led military leaders to imagine a future where computers might devise tactics, plans, and strategy. Spurred on by the success of AI systems in strategy-based games like Starcraft,[12] the PLA appears to be committed to investing research time and effort into building increasingly complex war games and models: "The PLA's objective is to use AI algorithms, machine learning, human-machine teaming, and autonomous systems collaboratively to paralyze its adversaries."[13]

Research teams at the PLA Army Command College in Nanjing appear to be leading efforts to incorporate advanced modeling techniques into training commanders and building plans. One author published at least eight papers related to combat modeling during 2010–2019 (see table 2). Many examples of recent research focus on multiple agent-based modeling and accelerating the OODA loop (Observe, Orient, Decide, Act) for combat decision making, while others focus on psychological and personality variables for training combat commanders.[14] Computational models can evaluate a wider range of possible combinations of conditions than human planners generally would have time to consider. What machines lack in imagination, they more than make up for with raw processing power. Through expanded models, Chinese strategists look to understand exactly which conditions lead to victory—then on the battlefield, take actions designed specifically to create those same conditions.

If combat models are trained on simulated sensor data to update conditions for agents, these same algorithms could be employed in live combat to suggest tactics and support command decisions in real time: "AI systems could enable military forces to operate faster, more cohesively, and with greater precision and coordination than humans alone can. The result could be to accelerate the pace of battle beyond human decision-making."[15] If one side is willing to hand over decision control to a machine and the other is not, the machines will gain the advantage of speed. Increased velocity comes at the expense of control. With humans out of the loop, small mistakes can quickly snowball—with catastrophic consequences.

When both sides, seeking only the advantage of speed, trust machines to make combat decisions, the loss of human control is referred to in Chinese circles as a "battlefield singularity."[16] Ethical principles will need to be followed at every stage in AI development to mitigate the risk posed by losing control of weapon systems.

Table 2. Research publications by Zhu Jiang at the PLA Army Command College in Nanjing

Result	Bibliographic Information
1	Jiang Zhu, Chuanhua Wen, Jun Chen, and Xiangyuan Huang, "A Personality-Based Combat Behavior Modeling Architecture and Methods," *Artificial Intelligence and Robotics Research* 8, no. 4 (2019), 248–54.
2	杜伟, 朱江, 闻传花, 王迎春, [Du Wei, Zhu Jiang, Wen Chuanhua, Wang Yingchun], 基于多Agent的作战体系仿真模型构建 [Multi-Agent-Based Combat System Simulation Model Construction.]. 舰船电子工程 [*Ship Electronic Engineering*] 36, no. 10 (2016).
3	朱江, 韶海玲, 杜正军, 汤磊 [Zhu Jiang, Shao Hailing, Du Zhengjun, Tang Lei], 新一代指挥控制过程模型设计 [A Next-Generation Command And Control Process Model Design]. 指挥与控制学报 [*Journal of Command and Control*] 1, no. 3 (2015).
4	朱江, 蔡蔚, 闻传花, 潘明聪,张钊 [Zhu Jiang, Cai Wei, Wen Chuanhua, Pan Mingcong, Zhang Zhao], 基于OODA指挥控制环的作战仿真实验 [Combat Simulation Experiment Based on OODA Command and Control Loop]. 指挥控制与仿真 [*Command Control and Simulation*] 37, no. 3 (2015).
5	朱江 [Zhu Jiang], 新一代战法实验平台的设计研究 [Design and Research of a New Generation of Tactical Experiment Platform]. 中国电子科学研究院学报 [*Journal of the Chinese Academy of Electronic Sciences*] 9, no. 5 (2014).
6	朱江, 许彬, 陈浩, 纵强 [Zhu Jiang, Xu Bin, Chen Hao, Zong Qiang], 心战Agent个性及传播建模 [Personality and Communication Modeling of Psychological Warfare Agent]. 计算机工程与科学 [*Computer Engineering and Science*] 35, no. 2 (2013).
7	朱江, 王三喜, 白海涛 [Zhu Jiang, Wang Sanxi, Bai Haitao], 基于多Agent 的弹药消耗计算模型和方法[Multi-Agent-Based Ammunition Consumption Calculation Model and Method]. 火力与指挥控制 [*Firepower and Command Control*] 38, no. 5 (2013).
8	张国宁, 沈寿林, 朱江, 赵姝淳 [Zhang Guoning, Shen Shoulin, Zhu Jiang, Zhao Shuchun], 联合战斗的复杂网络多Agent建模与仿真研究 [Research on Multi-Agent Modeling and Simulation of Complex Networks in Joint Combat]. 计算机仿真 [*Computer Simulation*] 3 (2010).

Threat #3: Blockchain-enabled Autonomous Swarms

Unmanned autonomous systems (UAS) have increasingly entered discussions about security and asymmetric tactics. Employment of networked small systems can give the user benefits of mass and agility compared to traditional large military equipment. As witnessed in coordinated attacks on Saudi Arabia's Abqaib Energy Facility on 14 September 2019,[17] these systems are capable of inflicting outsized damage with extremely low overhead. If integrated into an A2/AD package, UAS could serves as mobile platforms capable of carrying sensors, antennas, cameras, and even weapons.

While traditional UAS are generally quite fragile, easy to disable, confuse, destroy, or hack, integrating blockchain authentication protocols within the network can address many of these concerns. According to Feng Zebing and Lu Yue from the Security Research Center of China's Academy of Information and Communications Technology, blockchain for UAS swarms provides three key benefits (note: individual members of a swarm network are referred to as *nodes*):

1. Strong anonymity for identity management. Nodes that are not on the blockchain have no way to be certified by swarms, which effectively prevents network intrusion by malicious nodes.
2. Node consensus protects against false information. If the information cannot be verified by most nodes, it is considered illegal and will not be added to the chain.
3. Chained storage protects critical information. Tamper-proof features of blockchain effectively protect mission-critical data. Additionally, because each member records a backup of the blockchain's information, it is possible to recover all exploration data from the swarm as long as one system can successfully return to base. [18]

Thus, blockchain-enabled swarms pose a challenge to adversaries. The group is resilient against hacking, deception, and destruction of individual nodes, requiring actions to affect most or all components to be wholly effective.

The benefits of swarming and blockchain are not reserved for only small UAS. Larger aircraft can carry greater payloads and could easily be configured with similar command, control, and communication systems. Although more advanced unmanned combat aircraft will probably be remotely piloted for several years due to their increased speed, cost, and lethality, this may change as autonomy matures. Currently, China has several large, stealthy, unmanned aircraft in the works. Platforms called *Sharp Sword* and *Dark Sword* may be designed as AI-enabled next-generation air superiority fighters.[19]

PACAF Options for Countering Threats

International Team Building

First and foremost, the United States must maintain a strong network of allies and partners to counter Chinese belligerence. A coalition of like-minded nations committed to upholding international norms and maintaining a free and open Indo-Pacific is the best deterrent to Chinese expansionism. Additionally, multinational groups like the Association of Southeast Asian Nations (ASEAN) will play an increasingly important role.[20] July 2020 witnessed strong rhetoric in support of the rules-based order and opposing Chinese aggression. One example is Secretary of State Mike Pompeo's statement that "Beijing has a pattern of instigating territorial disputes. The world shouldn't allow this bullying to take place, nor should it permit it to continue."[21]

Current international research efforts on human-machine teaming like the Loyal Wingman program[22] showcase not only the strength of United States military technology but also the strength and resolve of American allies like Australia. Additionally, research partnerships sponsored through organizations like the Air Force Office of Scientific Research, Office of Naval Research, Army Research Office, and their associated international research arms are critical to ensuring a strong and technologically proficient network of allies and partners.

A strong deterrent effect relies on imposing unacceptable costs to aggression. As China seeks to build legitimacy and gain recognition as a regional leader, costs may be imposed across the wide range of political, economic, and information domains. Nevertheless, tough talk is just that, if not backed up with a trained, ready, and lethal military. As Gen David Goldfein, former Chief of Staff of the Air Force, poignantly pointed out, all A2/AD systems are imperfect, and the United States joint force will be ready to back up national policies:

> If [China or Russia] ever do see an F-35 . . . it will never be alone. It will be part of a penetrating joint team. And in the "we're here" message, the message is we're here in space, we've been here for a while, we've been watching you, we know what's going on, and we have already penetrated whatever defenses you think you have. You cannot put a block of wood over your country, you can put a block of Swiss cheese over your country, but like Swiss cheese there are holes there and we know where they are and we can exploit them and we can get in, we can hold targets at risk.[23]

To find those holes, planners and technicians will need to work together to learn as much as possible about adversarial capabilities and vulnerabilities.

Train against Machines

To better understand algorithmic warfare, it is useful to turn to an often-quoted phrase from Sun Tsu's *Art of War*, 知己知彼，百战不殆—Know yourself, know your enemy, and you will never be defeated. Because AI models depend on training data and programmers, decisions made by computers are predictable. Defeating algorithms is possible if you have access to the code. Understandably, however, military applications for AI are an issue of national security, and access is appropriately restricted. In the absence of a full model to analyze, the next best option is for the United States to build similar models using data that would be available to adversarial coders. This AI red team would be used to point out weaknesses in historical tactics and help planners devise new strategies to capitalize on machine inefficiencies.

Gen James Holmes, commander, Air Combat Command, further emphasized this point, stating that using autonomous systems as Red Air to train US pilots would be a near-term priority.[24] Training against AI-driven adversaries will teach pilots about relative strengths and weaknesses of unmanned systems. At the same time, these controlled tests will provide developers with valuable training data that adversarial programmers will not have, thus providing US coders and planners with an information advantage in the space of air-to-air combat between manned and unmanned systems. Furthermore, training in this manner provides valuable test data for proving battle readiness of US autonomous systems.

Fight Fire with Fire, Swarms with Swarms

The threats posed by advanced technologies are serious and will require serious preparation and training to address. Fortunately, the United States still has the most advanced technologies in the world. A recent study by RAND applied machine learning to mission planning and demonstrated some advantages and limitations of the technique. This experiment simulated a "group of [unmanned aerial vehicles (UAV)] with different sensor, weapon, decoy, and EW [electronic warfare] payloads . . . against an isolated air-defense system."[25] The underlying assumption that a variety of UAVs will be available to carry out combat tasks falls in line with current programs and research efforts. However, to present a real-world deterrent, the USAF needs to demonstrate its capability to avoid, strike, or decisively neutralize a much more complex air defense system.

One method to gain the offensive advantage against a strong A2/AD network is to mass large numbers of semiautonomous weapons to poke holes in the adversarial air defenses. The USAF is currently researching this topic through programs such as Golden Horde,[26] Gray Wolf,[27] and delivery platforms like Arsenal Planes.[28]

The fluidity of swarm warfare is akin to traditional tactics for maneuver and mass. Marine Corps Doctrinal Publication 1, *Warfare*, describes the following ebb and flow of combat operations:

> Military forces will mass to concentrate combat power against the enemy. However, this massing will also make them vulnerable to the effects of enemy fires, and they will find it necessary to disperse. Another competitive rhythm will develop—disperse, concentrate, disperse again—as each belligerent tries to concentrate combat power temporarily while limiting the vulnerability to enemy combat power.[29]

The repeating cycle of concentration and dispersion is likely to be automated in future systems. Human response time and speed would make manually controlling such coordinated effects nearly impossible. However, as planners and engineers work to build systems to carry out these battlefield effects, ethical considerations need to be integrated into every step of the design. Autonomy may be critical to maintaining the competitive edge, but machines are capable of spectacular miscalculations and unintentional escalations. Thus, extreme care must be taken to prevent autonomous routines from accelerating or amplifying misunderstandings in the Indo-Pacific.

Modernizing Joint Warfighting

Joint All-Domain Command and Control (JADC2) and Mosaic Warfare concepts promise to capitalize on the flexibility and advantages provided by emerging technology to "link any sensor to any shooter."[30] According to David Deptula and Heather Penny, "Mosaic is a force design that combines the attributes of highly capable systems with the volume and agility afforded by smaller force elements that can be rearranged into many different configurations or presentations."[31] Thus, Mosaic Warfare focuses more on the enabling systems hardware. On the other hand, JADC2 refers to the coordination of effects that the systems can bring to bear across all domains to create an overwhelming advantage for friendly forces. In concert, JADC2 and Mosaic will provide combat forces with the flexibility and adaptability to counter a wide range of future threats.

Looking to the Future

Many tasks futurists imagine assigning to autonomous systems can be performed by remote human operators. Human-controlled systems do not benefit from the same communication and coordination speeds that networked systems have and are prone to different types of mistakes. However, for the purpose of expanded sensing and patrolling capabilities for A2/AD, the net gain is similar. As militaries plan for possible future engagements, the time horizon is important. Near-term conflicts will likely rely more on manpower and be prone to mistakes based on human limitations. Far-term conflicts may integrate more automation and AI-driven decision making. Plans designed for one scenario will not work well against the other, as they will expect vulnerabilities where they are not present.

The United States leads the world in military technology, strategy, and capacity. However, the gap is narrowing, as competitors invest heavily in modernization and explore asymmetric tactics to level the playing field. As modern technologies make it possible to envision new ways to penetrate traditional defenses, they also enable weaker systems to defeat dominant military machines. The USAF must prepare for future fights where adversaries will attempt to strike directly at C2 networks or other perceived system vulnerabilities. Integrating JADC2 doctrine and exercising with compromised communications today will ensure air superiority amid the fog of future warfare. ✪

Major Richard Uber, PhD, USAF

Major Uber is a USAF operations research analyst and research fellow at the National Intelligence University's Ann Caracristi Institute for Intelligence Research. He earned his doctorate in applied mathematics from the Air Force Institute of Technology. He previously served as a military language instructor at the Defense Language Institute–Foreign Language Center and is a member of the Language Enabled Airman Program for Mandarin.

Notes

1. Roy Kamphausen, "The Chinese View of Strategic Competition with the United States," *U.S.-China Economic and Security Review Commission hearing*, opening remarks, 24 Jun 2020, https://www.uscc.gov/.

2. Gregory B. Poling, "The Conventional Wisdom on China's Island Bases is Dangerously Wrong," *War on the Rocks*, 10 January 2020, https://warontherocks.com/.

3. Terrence K. Kelly, David C. Gompert, and Duncan Long, *Smarter Power, Stronger Partners, Volume I: Exploiting U.S. Advantages to Prevent Aggression* (Santa Monica, CA: RAND Corporation, 2016), https://www.rand.org/.

4. Terrence K. Kelly et al., "Developing a U.S. Strategy for Dealing with China — Now and into the Future," RAND Corporation, 2014, www.rand.org/.

5. Michèle Flournoy, *Testimony before the U.S.-China Economic and Security Review Commission: The Chinese View of Strategic Competition with the United States*, 24 June 2020.

6. State Council of China, *State Council Notice on the Issuance of the New Generation AI Development Plan* [国务院关于印发新一代人工智能发展规划的通知], 20 July 2017, http://www.gov.cn/.

7. Elsa Kania, "AI Titan: China's Advances and Continued Challenges in Artificial Intelligence" (working paper, Harvard University, 2019), 31.

8. State Administration of Science, Technology and Industry for National Defence [国家国防科技工业局; SASTIND], *Project to Strengthen Development of the Defense Technology Industry at the Grassroots Level: Guidelines for Basic Research and Cutting-Edge Technology Projects (2018)* [国防科技工业强基工程基础研究与前沿技术项目指南 (2018年)], http://www.sastind.gov.cn, June 2018. CSET Translation, Ben Murphy (Ed.), Etcetera Language Group Inc., 30 September 2019.

9. Sydney J. Freedberg Jr., "AI & Robots Crush Foes In Army Wargame," *Breaking Defense*, 19 Dec 2019, https://breakingdefense.com/.

10. Liu Xuanzun, "China's meter wave anti-stealth radar capable of guiding missiles to destroy stealth aircraft: senior designer," *Fliegerfaust*, 26 May, 2019, https://www.fliegerfaust.com/.

11. Michael Peck, "Stealth Killer? China's Air Defenses Are Surpassing Russia's Anti-Aircraft Weapons," *National Interest,* 11 February 2020, https://nationalinterest.org/.

12. AlphaStar Team, "AlphaStar: Mastering the Real-Time Strategy Game Starcraft II," *DeepMind*, 24 January 2019, https://deepmind.com/.

13. Michael Dahm, "Chinese Debates on the Military Utility of Artificial Intelligence," *War on the Rocks*, 5 June 2020.

14. Jiang Zhu, et al., "A Personality-Based Combat Behavior Modeling Architecture and Methods," *Artificial Intelligence and Robotics Research 8*, no. 4, 2019, 248-254. Jiang Zhu is affiliated with the

Nanjing Army Command College. Additional publications by Jiang Zhu can be viewed online at http://czkj.ci.cqvip.com/ (accessed 14 July 2020).

15. Paul Scharre, "The Militarization of Artificial Intelligence," *Policy Roundtable: Artificial Intelligence and International Security*, 2 June 2020, https://tnsr.org/.

16. Chen Hanghui [陈航辉],"Artificial Intelligence: Disruptively Changing the Rules of the Game [人工智能 ：颠覆性改变"游戏规则],"*China Military Online*, 18 March 2016, http://www.81.cn/. Chen Hanghui is affiliated with the Nanjing Army Command College.

17. James Pothecary, "Abqaib: Lessons for Countering Drones," *Terrorism Monitor* 17, no. 19 (4 October 2019), https://jamestown.org/.

18. 冯泽冰 and 芦玥 [Feng Zebing and Lu Yu], 区块链增强无人机蜂群系统安全性分析, [Analysis on Blockchain strengthening UAV swarm system security], 信息通信技术与政策 [*Information and Communications Technology and Policy*], accessed 3 April 2020 from https://mp.weixin.qq.com/.

19. "China's Combat Drones Could Become Deadly Air Superiority Fighters with New AI," *Military Watch Magazine*, 15 August 2019, https://militarywatchmagazine.com/.

20. Paul Crespo, "ASEAN Countries Allying With U.S. Against China's Expansion," *American Action News*, 6 July 2020, https://americanactionnews.com/.

21. Michael R. Pompeo, *Secretary Michael R. Pompeo at a Press Availability*, 8 July 2020, https://www.state.gov/.

22. Gabriel Dominguez, "Boeing conducts end-to-end autonomous flight test in Australian outback," *Janes*, 16 July 2020, https://www.janes.com/.

23. Adam Twardowski, "General David Goldfein on building the Air Force of the future," *Order from Chaos* (blog), 22 February 2020, https://www.brookings.edu/.

24. James Holmes, "A conversation with Gen James "Mobile" Holmes," *Mitchell Institute Aerospace Nation*, 22 June 2020, https://www.mitchellaerospacepower.org/.

25. Li Ang Zhang, et al., "Air Dominance through Machine Learning," RAND Corporation, 2020, http://www.rand.org/.

26. Kyle Mizokami, "The Air Force Wants to Unleash a Robotic "Golden Horde" on Adversaries," *Popular Mechanics,* 30 November 2019, https://www.popularmechanics.com/.

27. Joseph Trevithick, "USAF Wants Swarms of Cheap 'Gray Wolf' Cruise Missiles That Can Overwhelm Enemy Defenses," *The Warzone*, 29 December 2017, https://www.thedrive.com/.

28. Courtney Albon, "SCO, Air Force shaping plans for Arsenal Plane experimentation," *Inside Defense*, 29 June 2020, https://insidedefense.com/.

29. Marine Corps Doctrinal Publication 1, *Warfighting* (Washington, DC: USMC, 20 June 1997), 10, https://web.archive.org/.

30. Mark Esper, "IISS Special Presentation with US Secretary of Defense Mark T. Esper," Institute for International Strategic Studies, *YouTube*, 21 July 2020, https://youtu.be/.

31. David Deptula and Heather Penny, *Restoring America's Military Competitiveness: Mosaic Warfare* (Arlington, VA: Mitchell Institute for Aerospace Studies, September 2019), 33, http://docs.wixstatic.com/.