
Advanced Battle Management System (ABMS)

先进战斗管理系统

空军面临的需求、进展、挑战与机遇

Ellen Y. Chou, Editor

(C) 2022, COMMITTEE ON AIR FORCE ADVANCED BATTLE MANAGEMENT SYSTEM

前言

美国国防部 (DoD) 正在通过联合全域指挥与控制 (JADC2) 框架，提升更加紧密整合和联合行动的能力，以应对灵活的对手。该框架将无缝整合传感器、网络、平台、指挥官、操作员和武器系统，实现快速信息收集、决策和联合多国部队的投射。空军部 (DAF) 对 JADC2 的贡献是先进战斗管理系统 (ABMS)。

然而，对于 ABMS 的性质及其结构是否合理存在疑问，因为它缺乏一组明确定义的离散分配的最低性能目标、单一的固定要求集、拟议能力交付的时间表以及用于执行这些目标的预算和资源的系统分配。尽管敏捷性、灵活性和适应性是值得追求的目标，但如果不能提供足够详细、具体和指标的计划来同步如此庞大且复杂的系统体系结构，成功的大规模能力交付将面临挑战，甚至不太可能实现。

为了解决这些问题，委员会受命审查以下内容：

1. 评估计划中的 ABMS 数据和通信架构，并比较其预期性能特征与支持实时火控、全域传感器到射手的数据流、指挥与控制 (C2) 活动、基于人工智能 (AI) 的生活模式训练、战损评估及其他相关数据活动所需的性能特征；
2. 确定 ABMS 技术和计划中的系统集成架构中存在的任何技术差距和不足；
3. 审查 ABMS 的治理，并建议如何改进计划中的组织和执行计划与流程，以更好地实现 DAF 和整个 DoD 的 JADC2 作战快速实现。

在研究进行过程中，前空军部采办、技术与后勤助理部长 (SAF/AQ) 将先进战斗管理系统 (ABMS) 的主要责任办公室 (OPR) 从空军部首席架构师办公室 (DAF CAO) 转移至空军部快速能力办公室 (RCO)。这一变化产生了两个主要结果。首先，委员会最初被要求审查的任务与 RCO 的 ABMS 优先事项和职责并不完全一致。因此，委员会请求的一些信息无法提供，而委员会收到的一些信息后来被更新信息取代。其次，由于系统的技术设计和治理在空军部内部正在发生重大变化，委员会对 ABMS 的了解基本上是一个过渡性的画面。

作为一个处于定义早期阶段的不断发展的系统，ABMS 架构及其支持元素仍然处于动态变化中。委员会从 2020 年 10 月至 2021 年 3 月看到的 ABMS 技术架构主要反映了在空军部首席架构师办公室管理的大规模 “上坡 (on-ramp) ” 演习中涌现出来的 ABMS 现状。早期的架构和方法正在由空军部快速能力办公室进行评估和修订，以在能力发布中创建一系列

采办计划。因此，委员会的分析反映了这一早期架构的方法、优势、挑战和机遇，并为首席架构师办公室、快速能力办公室、空军部和更广泛的国防部元素提供了见解和建议，以供他们在追求更新的 ABMS 架构、其内部的个别采办计划和更大的 JADC2 框架时考虑。空军部快速能力办公室在新任空军部长的指导下，已经在其不断发展的 ABMS 计划和设计中解决了其中的一些问题，但其他问题（尤其是非技术因素）需要进一步考虑。

报告组织及主要观察

本报告按主题分为四章：视角、架构与数据、治理、以及挑战与机遇。第一章描述了为什么需要 ABMS 以及它如何从联合监视和雷达系统的替代项目演变为一个包罗万象的指挥与控制（C2）系统家族。第二章审视了当前和计划中的架构，包括数据标准、软件、安全性、测试和建模。第三章概述了过去和现在的 ABMS 治理，强调了人机系统集成、培训、文化和其他考虑因素。第四章详细讨论了互操作性和情报，并总结了委员会的建议。

从总体上看，委员会认为，作为一个非传统采办项目，ABMS 进展顺利，但仍在持续发展。其技术设计和架构尚处于初期阶段且不断演变，因此委员会难以对其数据和通信架构进行全面评估，尤其是与正在开发和定义的 JADC2 框架相关的部分。此外，委员会发现其性能特征在规模和范围上受到限制，因为这些特征主要与上坡演示有关，而不是实际的操作活动，其中现实世界的物理约束可能会限制实际性能。

委员会认为将空军部快速能力办公室指定为 ABMS 的主导组织是一个积极的步骤，有助于将 ABMS 从演示和实验转向重点能力发布。委员会还支持空军部长呼吁建立绩效指标，以评估改进和衡量操作结果。

作为一个系统家族，ABMS 难以量化。委员会无法详细评估 ABMS 的确切成本，因为它涉及多个项目组合，其中一些项目未被指定为 ABMS 的组成部分，但仍被纳入更广泛的 ABMS 生态系统。国会决定将 ABMS 的总体预算减少近一半，显然限制了 ABMS 在近期到中期内的成就。然而，这一预算限制也可能迫使空军部领导做出重要决策和优先考虑 ABMS 的投资和能力，这是委员会所支持的。

委员会发现，目前的 ABMS 和更广泛的 JADC2 治理结构不充分，缺乏在所有领域执行 C2 的适当权威。缺少一个国防部级别的执行代理来解决和处理所有 JADC2 框架参与者的技术、操作和指挥决策问题，导致各军种和国防部机构各自开发自己的 C2 系统，这些系统具有独特的需求、标准和技术规范，给实现互操作性带来了挑战。

委员会认识到，在本次分析过程中，ABMS 在其技术方法和治理结构上都有所发展。因此，值得注意的是，下面总结并在本报告其余部分详细阐述的一些建议是针对早期的 ABMS 方法的，而另一些可能对更新、更集中的计划仍然适用。

各部门的建议

空军部首席架构师办公室（CAO）和快速能力办公室（RCO）建议：

- 在联合全域指挥与控制（JADC2）级别定义先进战斗管理系统（ABMS）架构，以确保与其他类似 ABMS 系统的互操作性（建议 1）。
- 设计 ABMS 架构时，应具有模块化设计，并包含开放标准和接口，以便能够与其他军种变体进行配置（建议 3）。
- 设计 ABMS 架构时，应具有特定的技术要求和解决方案，以确保在受限或被拒绝访问的环境中，通信、数据和计算能够继续运行（建议 4）。

- 尽可能全面地设计和执行一个包含所有要素的人工智能战略，包括学说、指挥链、政策、联合环境中武器释放的授权、与 JADC2 的接口，而不仅仅是 ABMS 的某些选定能力（建议 6）。
- 与空军部首席软件官协调，扩大容器化和 Kubernetes 的使用，以实现 ABMS 的持续开发，并检测和缓解安全漏洞（建议 8）。
- 采用开发、安全和运维（DevSecOps）作为 ABMS 的通用开发环境，通过容器化和持续集成/持续交付实现这一目标（建议 9）。
- 在 ABMS 架构中设计弹性，并指定所需性能的动态标准（建议 11）。
- 与空军部数字工程企业办公室合作，在 ABMS 的工程和维护活动中应用基于模型的系统工程（MBSE）方法，并使 MBSE 成为操作员需求和开发团队之间的桥梁（建议 17）。

空军部（DAF）快速能力办公室（RCO）建议：

- 采用一系列数据交换技术，以支持从战术到战略的全方位能力（建议 5）。
- 对于具有强大接口规范的模块化开放系统设计，获取性能和接口要求，而不是所有知识产权（建议 10）。
- 随着技术成熟分阶段应用零信任（ZT），并集成 ZT 服务，包括在整个先进战斗管理系统中使用多因素认证（建议 13）。
- 除了采用零信任外，还应利用最成熟的可用网络安全实践和能力，包括多因素认证、身份、凭证和访问管理、加密、渗透测试、托管检测服务、行为监控应用程序等（建议 14）。
- 使用空军的任务防御团队（Mission Defense Teams）对先进战斗管理系统的网络防御进行红队测试，以应对恶意行为者的攻击。根据这些红队演习的结果，空军部快速能力办公室应加强和提升网络防御，以解决漏洞（建议 15）。
- 与美国网络司令部（U.S. Cyber Command）合作，解决物联网防御及其他在《美国网络司令部技术挑战问题集》（United States Cyber Command Technical Challenge Problem Set）文件中突出的网络漏洞和利用（建议 16）。
- 基于现有的数字工程和建模与仿真活动，扩大数字双胞胎在先进战斗管理系统开发中的使用，特别是在引入新能力和技术时（建议 18）。
- 考虑扩大通用任务控制中心（Common Mission Control Center），并将其指定为先进战斗管理系统的零阶段（建议 19）。
- 将人机系统集成方法纳入先进战斗管理系统，以确保所有人类用户与当前和未来的系统元素完全有效地整合（建议 22）。

联合参谋部、各军种和美国国防部领导的建议：

- 为所有参与联合全域指挥与控制（JADC2）的成员建立互操作性要求和性能指标，以便最终整合所有能力（建议 2）。
- 就共同的数据结构和数据的安全级别达成立即协议，并在联合层面定义数据标准和工具。没有一套共同商定的开放标准及已知的接口交换要求，军种将面临开发不兼容和孤立解决方案的风险（建议 7）。
- 为 JADC2 和先进战斗管理系统（ABMS）建立并实施一个强大的企业级进攻性和防御性网络安全战略。安全性是一个基本要求，必须从一开始就设计并完全集成到所有支持 JADC2 的系统架构中（建议 12）。
- 建立一个权威的联合级别机构，负责解决和处理所有 JADC2 框架参与者的技术、操作和指挥决策（建议 20）。

- 如果要实现联合战斗概念 (JWC) 所设想的真正联合和多国一体化作战，需要解决实现真正 JWC 横向整合的文化、社会和情感障碍（建议 21）。
- 确保在设计、运行、人员配置和培训 ABMS（以及其他支持更广泛的 JADC2 框架的系统）时，审查和解决人工智能的伦理使用问题，符合政策和战争法的要求（建议 24）。

空军部采办、技术与后勤助理部长 (SAF/AQ) 和副参谋长战略、整合与需求部门的建议：

- 在设计和实施更广泛的先进战斗管理系统 (ABMS) 生态系统计划时，考虑并将人员、文化、培训及其他非物质的教义、组织、培训、物资、领导、教育、人员、设施和政策问题融入其中（建议 23）。

空军教育训练司令部的建议：

- 建立一个课程，培训或招聘在人工智能/机器学习、基于模型的系统工程、网络安全、情报评估以及信息技术、软件和硬件的测试与评估方面的高度合格专家，这些专家能够与军事操作和文化方面的专家合作（建议 25）。

这些建议在完整报告中有详细探讨。

1 观点

“我们的空军必须加速变革，以控制和利用空域，达到国家对我们的期望和要求。如果我们不改变——如果我们未能适应——我们将面临失去几十年来捍卫国家利益的确定性的风险。我们将面临在高端战斗中失败的风险。我们将面临失去优秀空军人员、信誉以及保障未来能力的风险。我们必须带着目标前进——我们必须加速变革，否则就会失败。”

—美国空军参谋长，查尔斯·Q·布朗将军¹

为了加速变革以控制和利用空域，先进战斗管理系统 (ABMS)²是空军部 (DAF) 对联合全域指挥与控制 (JADC2)³概念的贡献。JADC2 概念旨在实现无缝的联合和多国信息共享及作战指挥与控制 (C2)。这些努力旨在使当前和未来的传感器、指挥部、操作员和武器系统能够以克服预期对手决策和行动所需的速度共享适当且准确的信息。⁴ABMS 旨在在美国国防部 (DoD) 企业中，在高端对抗和低强度战斗环境中共享关键作战数据。情报、监视和侦察 (ISR) 等信息、武器系统的可用性以及军事行动状态和行动构成了 ABMS 架构

¹C.Q. Brown, Jr., 2020, Accelerate Change or Lose, https://www.af.mil/Portals/1/documents/2020SAF/ACOL_booklet_FINAL_13_Nov_1006_WEB.pdf, August.

²P. Dunlap, 2020, "ABMS Overview," Presentation to the Air Force ABMS Committee, October 30. See also J. Eddins, 2021, "Valenzia: ABMS Will Deliver the 'Decision Advantage,'" Airman Magazine, <https://www.airmanmagazine.af.mil/Features/Display/Article/2634972/valenzia-abms-will-deliver-the-decision-advantage/>, May 26. D. Mayer. 2021, "ABMS Aims to Revolutionize Data Flow, Speed Decisions," Air Force News, April 1, <https://www.af.mil/News/Article-Display/Article/2559022/abmsaims-to-revolutionize-data-flow-speed-decisions/>. CRS (Congressional Research Service), 2021, Advanced Battle Management System (ABMS), <https://sgp.fas.org/crs/weapons/IF11866.pdf>, June 29.

³See J. Garamone, 2020, "Joint All-Domain Command, Control Framework Belongs to Warfighters," DoD News, November 30, <https://www.defense.gov/Explore/News/Article/Article/2427998/jointall-domain-command-control-framework-belongs-to-warfighters/>. CRS, 2021, Joint All-Domain Command and Control: Background and Issues for Congress, <https://crsreports.congress.gov/product/pdf/R/R46725/2>, March 18. CRS, 2021, Joint All-Domain Command and Control (JADC2), <https://sgp.fas.org/crs/natsec/IF11493.pdf>, July 1.

⁴Office of the Under Secretary of Defense (Comptroller/Chief Financial Officer), Defense Budget Overview, United States Department of Defense Fiscal Year 2022 Budget Request, 2021

的基础，使联合和盟军指挥官能够实时准确地了解环境，并比任何潜在对手的观察-定位-决策-行动（OODA）循环更快地采取行动。⁵

由于 ABMS 的不断演变，目前对于它的实际定义和未来承诺存在一些混淆。⁶ ABMS 起源于其他概念，如多域或全域指挥与控制（C2）以及空军取消的联合监视和目标攻击雷达系统（JSTARS）重资本项目，⁷ ABMS 既是一个概念，也是一个部署广泛能力的倡议。ABMS 已成为 JADC2 的同义词，但这误导性地忽视了陆军和海军的其他 JADC2 努力。⁸此外，ABMS（和 JADC2）不仅需要在物资方面进行调整，还需要在整个被称为 DOTMLPF-P 的范围内进行调整——即国防部必须解决教义、组织、培训、物资、领导、教育、人员、设施和政策（DOTMLPF-P）方面的问题，才能成功实施 ABMS。⁹因此，虽然 ABMS 将显著部署能力和系统，但其预期影响是全面的军事行动。这也是为什么各组织难以理解 ABMS 的现状及其未来发展的原因。从概念到执行，ABMS 不仅关注 C2、网络以及特定的武器系统和平台，还寻求提供一个企业级解决方案来连接和整合所有部队能力。图 1.1 展示了空军部对 ABMS 的愿景。

提供 ABMS 及其不断演变努力的潜力视角，本章首先展望了在 ABMS 和 JADC2 下未来空中和太空作战可能包含的内容，随后概述了 ABMS 的近期和当前活动、其动机、期望、时间表以及与 JADC2 其他军种元素的关系。

1.1 未来空中和太空作战的愿景

2018 年《国家防务战略》（NDS）描述了“一个日益复杂的全球安全环境，其特征是对自由和开放的国际秩序的公开挑战以及国家之间长期战略竞争的重新出现……我们面临着一个越来越致命和破坏性的战场，跨域联合，作战速度和范围不断扩大——从近距离战斗到海外战区，甚至延伸到我们的本土。一些竞争对手和对手试图优化他们对我们作战网络和

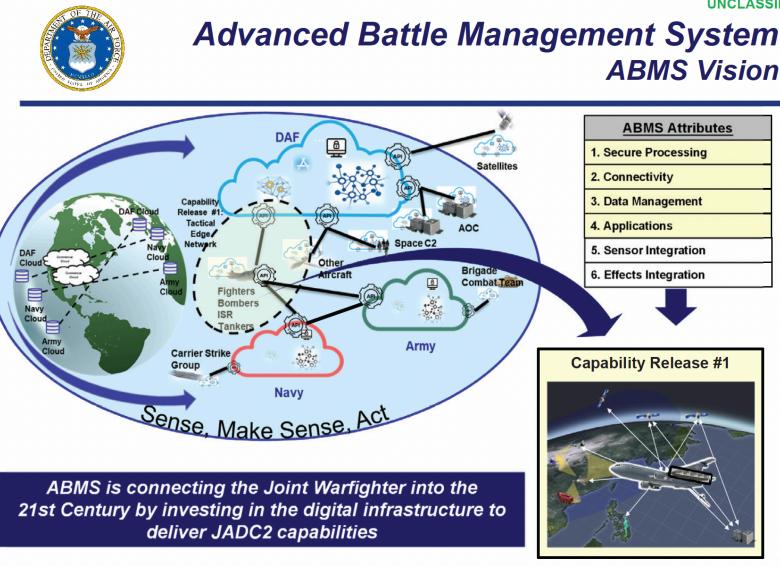
⁵See "DoD's Data-Driven Future: Shared Knowledge, Near Real-Time Answers," 2021, Air Force Magazine, <https://www.airforcemag.com/dods-data-driven-future-shared-knowledge-near-real-timeanswers/>, June 1. G.S. Fein, 2003, "New Meaning for 'OODA Loop,'" National Defense Magazine, <https://www.nationaldefensemagazine.org/articles/2003/10/1/2003october-new-meaning-for-ooda-loop>.

⁶See T. Hitchens, 2020, "Roper Mulls Name Change for Changing ABMS (Not Skynet!)," Breaking Defense, <https://breakingdefense.com/2020/09/roper-mulls-name-change-for-changing-abms-notskynet/>, September 4. S. Sirota, 2021, "Roper Caves to Demands, Establishing ABMS as a Traditional Acquisition Program," Inside Defense, <https://insidedefense.com/daily-news/roper-caves-demandsestablishing-abms-traditional-acquisition-program>, January 14. M. Mayfield, 2020, "Air Force's Advanced Battle Management System Takes New Step," NDIA Magazine, <https://www.nationaldefense magazine.org/articles/2020/11/24/advanced-battle-management-system-takes-new-step>, November 24. T. Hitchens, 2020, "Roper Targets Commercial AI, Data Analytics for Next ABMS Deals," Breaking Defense, <https://breakingdefense.com/2020/05/roper-targets-commercial-ai-data-analytics-for-nextabms-deals/>, May 14.

⁷See A. McCullough, 2019, "Life After JSTARS," Air Force Magazine, <https://www.airforcemag.com/article/life-after-jstars/>, March 21. S.J. Freedberg, Jr., 2019, "Air Force ABMS: One Architecture to Rule Them All?" Breaking Defense, <https://breakingdefense.com/2019/11/air-force-abms-one-architectureto-rule-them-all/>, November 8.

⁸A. Abadie, 2021, "Project Convergence Overview," Presentation to the Air Force ABMS Committee, January 8. D.W. Small, 2021, "Project Overmatch," Presentation to the Air Force ABMS Committee, March 3. See also K. Underwood and R.K. Ackerman, 2021, "Services Choose Independent Paths for JADC2," SIGNAL,

⁹For a definition on DOTMLPF-P, see Chairman of the Joint Chiefs of Staff Instruction (CJCSI), 2016, CJCSI 3010.02E, Guidance for Developing and Implementing Joint Concept, pp. A-3-A-5, <https://www.jcs.mil/Portals/36/Documents/Library/Instructions/CJCSI%203010.02E.pdf>, August 17. For more on the spectrum of ABMS requirements, see D. Allvin, 2021, "Why We Need the Advanced Battle Management System," DefenseOne, <https://www.defenseone.com/ideas/2021/05/why-we-needadvanced-battle-management-system/173861/>, May 6.



UNCLASSIFIED

Figure 1.1: ABMS 愿景。

来源：兰德尔·G·沃尔登，空军快速能力办公室，美国空军部。2021年1月22日向委员会做的报告。批准公开发布。

作战概念的攻击，同时在不公开战争的情况下利用其他竞争领域来实现他们的目的（例如，信息战、模糊或被拒绝的代理操作和颠覆活动）。”¹⁰值得注意的是，

安全环境还受到快速技术进步和战争性质变化的影响。开发新技术的推动力无休止地扩展到更多的参与者，进入门槛降低，发展速度加快。新技术包括先进计算、“大数据”分析、人工智能、自治系统、机器人技术、定向能、超音速技术和生物技术——这些正是确保我们能够在未来战争中战斗并取胜的技术。新的商业技术将改变社会，并最终改变战争的性质。¹¹

因此，“真正的关键在于谁能比对手更快地感知和理解环境并采取行动。胜利属于能够迅速决策并加速杀伤链的一方。我们称之为决策优势，并寻求这种优势。”¹²

2019年发布的国防部《数字化现代化战略》¹³强调了国防部认识到需要快速将当前技术推进到数字化未来，以应对这些紧迫挑战。随着现代战场向更远距离、分布式和日益复杂的互联作战域转变，确保通信、协调和执行变得愈加重要。确保在太空、网络空间、空中、陆地、地面和水下的部队能够有效且及时地通信，以支持动能和非动能作战至关重要。在过去二十年中，数字时代的爆炸性发展，特别是人工智能（AI）和普遍的通信与处理技术，已经并将继续显著改变战场。

例如，正如国家安全人工智能委员会（NSCAI）在其最终报告中所述：

¹⁰DoD (U.S. Department of Defense), 2018, Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge, <https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf>.

¹¹DoD (U.S. Department of Defense), 2018, Summary of the 2018 National Defense Strategy of the United States of America: Sharpening the American Military's Competitive Edge, <https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf>. p.3.

人工智能正在扩大美国已经进入的脆弱窗口。自第二次世界大战以来，美国的技术优势——其经济和军事力量的支柱——首次受到威胁。如果当前趋势不变，中国具备在下一个十年内超越美国，成为世界人工智能领导者的实力、人才和野心。同时，人工智能加深了网络攻击和虚假信息活动所带来的威胁，俄罗斯、中国及其他国家正在利用这些手段渗透我们的社会，窃取我们的数据，并干涉我们的民主。¹⁴

在俄罗斯，“人工智能的发展和使用被视为未来俄军成功的关键，也是其军事力量的关键……俄罗斯军事战略家非常重视建立他们所称的‘战场信息优势’，而增强人工智能的技术承诺利用现代战场上的数据来保护俄罗斯自己的部队，并剥夺对手的优势。”¹⁵

同样，“中国军方对人工智能的举措受到对全球军事技术和作战趋势的高度关注……以及对这一军事和技术变革中潜在机会的认识的推动。”¹⁶因此，中国军方和国防工业一直在机器人、自治系统和其他人工智能应用方面进行重大投资。国防部 2020 年提交给国会的关于中国军事和安全发展的年度报告引用了中国的《新一代人工智能发展规划》，该规划表明，中国力争在 2020 年与全球领导者在人工智能领域并驾齐驱，在 2025 年前取得重大突破，并在 2030 年前确立中国在人工智能领域的全球领导地位。“中国正在推进全社会的努力，成为全球人工智能领导者，包括指定中国的部分私营人工智能公司为‘人工智能冠军’，以强调特定双用途技术的研发。”¹⁸

除了利用人工智能，对手还试图通过使用混合战争来削弱美国在各个领域的主导地位。虽然混合战争并不是一个新概念，但对手“在作战战场上同时适应性地使用常规、不规则、恐怖主义和犯罪手段或活动的量身定制混合”，包括使用非动能工具来破坏国家，已经扩展了管理战争谱系所需的工具，超越了传统力量。¹⁹“我们的战略竞争对手研究了我们的作战方式，并采取了不对称措施来利用我们的弱点并击败我们。我们必须以紧迫感作出回应，但我们也必须花时间做出关于我们未来和投资的明智选择。”²⁰正如乌克兰外交部所指出的：

军事侵略只是俄罗斯对乌克兰混合战争的一部分。其他要素包括：

- 1) 基于谎言和伪造的宣传；2) 贸易和经济压力；3) 能源封锁；4) 恐怖和恐吓乌克兰公民；5) 网络攻击；6) 尽管有大量不可辩驳的证据，但坚决否认对乌克兰的战争事实；7) 利用亲俄势力和卫星国家为己所用；8) 将自己的罪行归咎于对方。²¹

此外，为防护和发射“快速”武器（例如高超音速导弹）的指挥与控制（C2）时间线也改变了可操作的时间线，不仅缩短了决策的可用时间，还削弱了计算最佳防御选项的能力。技术和作战变化（例如人工智能、无人平台和有争议空间的新“战场”）推动各军种（单独和联合）重新考虑未来的作战 C2 概念及其实现所需的技术手段。再加上美国将成为一支较小的部队这一新现实，国家将不再享有同时拥有规模最大和技术最先进的部队的奢侈。这些共同的挑战削弱了美国的信息优势，而 ABMS 旨在克服这些挑战。对于联合部队，新方法是服务于联合战斗概念（JWC）的 JADC2。²²

1.2 联合全域指挥与控制（JADC2）

联合全域指挥与控制（JADC2）是“在所有战争层次和阶段、跨越所有领域并与合作伙伴一起感知、理解和行动的作战能力，以在相关速度上提供信息优势。”²³它是国防部（DoD）将空军、陆军、海军陆战队、海军和太空部队的传感器连接成一个单一网络的解决方案。²⁴ JADC2 的核心在于“在整个联合部队的每个层级，从战略层到战术边缘，创建一

个具有弹性和适应性的通信线路（例如网状网络）。这个受保护和强化的网络将推动全球所有领域相关信息的无缝流动，使我们的作战指挥官和高级领导人能够比我们的对手更好、更快地做出决策和指挥行动——在可能的情况下威慑他们的行动和意图，并在必要时彻底击败他们。”²⁵ 图 1.2 展示了 JADC2 的基础。

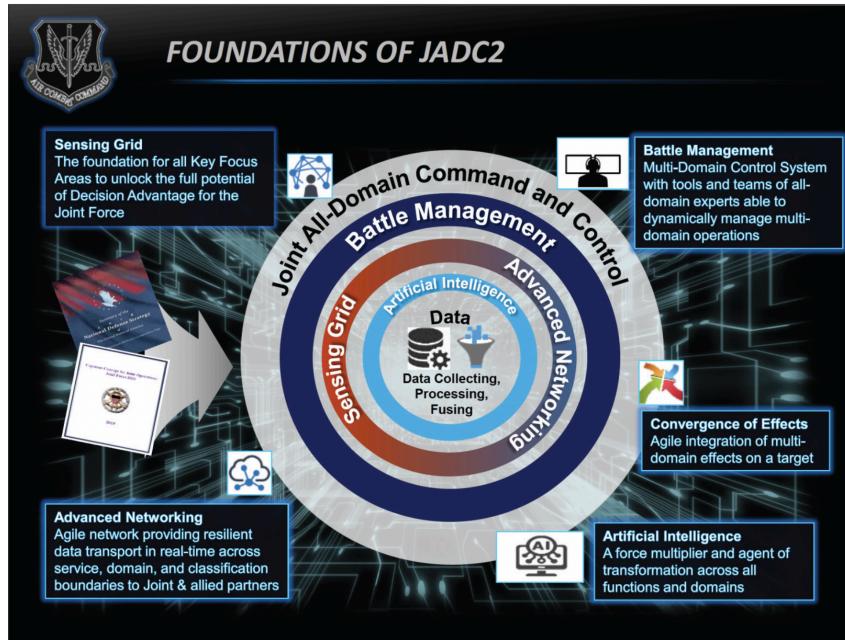


Figure 1.2: 联合全域指挥控制 (JADC2) 的基础。

来源：空军杂志，2020 年 10 月 28 日。

传统上，每个军种都开发了各自独特且通常在武器系统、平台和作战领域之间不兼容的 C2 网络。因此，决策时间周期和传递时间敏感数据以支持决策的速度较慢，有时还会重复和组织性孤立。JADC2 是国防部应对这一技术和操作挑战的企业级解决方案，它“设想为联合部队提供一个类似云的环境，以共享情报、监视和侦察数据，通过多种通信网络进行传输，从而加快决策过程。”²⁶ 此外，它还旨在重新设想通常远离作战战场的总部要素，如空中作战中心 (AOCs)，并赋予前线部署的作战指挥官与总部相同的态势感知和决策能力。“这一概念使部队管理能够响应甚至预先应对敌人或对手产生的效应、决策和机动。”²⁷

纵观历史，胜利往往属于那些能够比对手更快做出决策，并因此能够更适当地利用之前决策成果的实体。²⁸ 此外，拥有更好态势感知能力的部队通常占据主导地位。²⁹ 部队数量和作战能力是其他主要因素，但卓越的态势感知和响应能力已被证明是力量倍增器。这并不意味着这种感知在所有时候都是完美的，但在受限环境中拥有继续观察、决策和战斗的卓越能力的部队在实现成功方面具有更大的优势。JADC2 被提出作为联合解决方案，可以“在任务部队固有的作战武器资源集和跨域中同步处理数千个潜在目标”，³⁰ 从而“在未来与中国或俄罗斯的冲突中为美国军队提供决策优势，使美军能够比对手更好地理解、更加智能地决策和更快速地行动。”³¹

对于空军部 (DAF) 而言，ABMS 是其对 JADC2 的贡献。作为一种新的信息共享和决策管理方法，ABMS 使决策过程得以压缩，并在不受领域或地理边界限制的情况下实现效果的汇聚……这种速度对决策者和战斗人员至关重要。而且，随着技术的普及，未来的战斗人员将能够在几分钟内观察、定位、决策和行动——而不是数小时或数天。³²

空军部必须执行的指挥与控制（C2）职能——目前集中在空中作战中心（AOC）——必须同样适应这一加速的决策环境，并采用能够满足这些需求的技术。由于 ABMS 被提出作为新 AOC 的物资解决方案以突出这一变化，以下提供了当前 AOC 的简要概述以及在 ABMS 及其相关技术承诺下，AOC 可能的未来形态。

1.3 空军作战中心 AIR OPERATIONS CENTER (AOC)

1.3.1 AOC 现状

当前的空中作战中心（AOC）——其基础架构设计于 21 世纪初——“既是一个空军单位，也是一个武器系统……[它] 是联合或联合部队空中组成司令官（JFACC）的指挥与控制中心，提供规划、指挥和评估指定和附属部队活动的能力……并提供空中、太空、网络空间和 [信息作战]（IO）的作战级指挥与控制，以满足 JFACC 的作战目标和指导。”³³ AOC 是“设计、规划、执行和评估空中组成部分作战的焦点。”³⁴

AOC 的主要职能包括：

- 制定空中组成部分作战策略和规划文件，整合空中、太空和网络空间作战，以满足联合部队司令（JFC）指定的空中组成部分司令的目标和指导。
- 任务分配、执行和评估日常空中组成部分作战；提供快速反应、正面空域控制，协调和解除武器使用冲突，并整合整个空中组成部分的努力。
- 接收、汇总、分析、过滤和传播所有来源的情报和天气信息，以支持空中组成部分的作战规划、执行和评估。
- 整合太空能力，并在被指定为太空协调权威时协调空中组成部分司令的太空活动。
- 发布空域控制程序，并在被指定为空域控制权威（ACA）时协调空域控制活动。
- 在被指定为区域防空司令官（AADC）时，提供全面的防空指导，包括战区导弹防御（TMD）。
- 规划、任务分配和执行战区空中组成部分的情报、监视和侦察（ISR）任务。
- 进行组成部分级别的评估，以确定任务和整体空中组成部分作战的有效性，按 JFC 的要求支持战区评估工作。
- 根据战区优先事项，规划和分配空中机动作战任务。³⁵

这些职能显示了当前 AOC 的广泛责任和复杂操作，这些操作需要在未来的 ABMS 及其相关技术承诺下进行改进和适应。

作为一种武器系统，目前的空中作战中心-武器系统（AOC-WS），也被称为 AN/USQ-163 Falconer，是“一个包含众多第三方软件应用和商用现成产品的系统集成系统。每个集成到 AOC-WS 中的第三方系统都有其独立的程序文档。AOC-WS 的能力包括联合战区空中和导弹防御的指挥与控制（C2）；预先计划、动态和时间敏感的多域目标攻击操作；以及情报、监视和侦察操作管理。”³⁶ 此外，AOC-WS 包括：

- 用于语音、数字和数据通信基础设施的商用现成软件和硬件。
- 专门为 AOC-WS 开发的政府软件应用，以实现空中、太空和网络操作的规划、监控和指挥执行，包括：
 - 接受、处理、关联和融合来自多个来源的 C2 数据的额外第三方系统，并通过多个通信系统共享这些数据。
- 在需要时，AOC-WS 可以在多个不同的网络上运行，包括秘密互联网协议路由网络（SIPRNET）、联合全球情报通信系统和联盟网络。这些网络将核心操作系统和主要应用程序连接到联合和联盟伙伴。³⁷

目前，空军的 Kessel Run 实验室（KREL）负责开发和部署 AOC-WS Block 20 软件到现场。³⁸ 其目标是现代化 AOC，使其成为一个分布式的 AOC 武器系统，并废弃现有的 10.1 Falconer 武器系统。³⁹ 作为与操作员的集成伙伴，Kessel Run 开发人员了解用户需求，并能够开发和测试软件以满足这些操作需求。如果成功，这种将软件开发人员与最终用户嵌在一起的模式应更广泛地采用。

尽管取得了一些进展，但当前 AOC 的设计和构造仍存在显著挑战。特别是，空军部在 AOC 中的 C2 功能的基础架构设计不足以应对当前的操作和技术威胁，也无法支持加速的规划速度。正如最近 RAND 关于 JADC2 的研究所指出的，“AOC 10.2 现代化努力的取消推迟了向 AOC 交付关键硬件和软件升级的时间……对改进网络和空间集成的日益重视对 AOC 提出了新的功能和技术要求，并增加了对多域作战的兴趣。”⁴⁰ 结果是，“空军 AOC 72 小时的空中任务周期与当前的数字世界不一致。”⁴¹

当前的 AOC-WS 项目在资金优先排序方面也历来面临挑战。它受到了缺乏联合架构和人工智能政策指南的影响，无法按照这些指南进行构建。委员会从操作员和采办人员收到的证词强调了当前 AOC 未能对齐新的 JADC2、JWC 和威胁需求的担忧。显然，当前系统使用的固有过时技术和架构无法重新构建，因此系统的系统架构（按当前构造）不支持随时间的转变。⁴²

此外，显而易见的是，即使没有 JADC2 或 JWC，空军也需要一个创新和改进的 AOC，以便与新的美国太空司令部（USSPACECOM）和美国太空部队（USSF）操作系统互操作，并应对来自对手的广泛作战挑战。这些对手试图通过反介入/区域拒止（A2/AD）、电子战、网络武器、远程导弹、先进防空系统，甚至可能的 GPS 干扰来抵消美国的军事优势。⁴³ 所有这些因素都增加了需要更快决策的需求，以利用和整合所有美国军事能力。

1.3.2 未来下一代的空中作战中心（AOC）

技术的快速进步极大地改变了作战需求，并缩短了应对敌对威胁的响应时间。2018 年的《国家防务战略》指出：“这个日益复杂的安全环境由快速的技术变化、各个作战领域中敌对势力的挑战以及国家历史上最长连续武装冲突对当前战备状态的影响所定义。在这种环境下，我们不能自满——我们必须做出艰难的选择，并优先考虑最重要的事项，以组建一支致命、有韧性和快速适应的联合部队。美国的军队在战场上没有预定的胜利权。”⁴⁴ 美国空军参谋长也表达了相似的观点，他说：“当国家专注于对抗暴力极端组织时，我们的竞争对手专注于打败我们。他们研究、资源投入并引入专门设计来打败美国空军能力的系统，这些能力支撑了美国的战争方式已有一代人……在资源减少、全球竞争对手咄咄逼人以及技术迅速发展和传播的环境中，美国空军必须加速变革，以控制和利用空域。”⁴⁵ 技术进步和新出现的对空军部 C2 功能的敌对挑战因此需要重新设计当前的 AOC 架构和支持技术，以满足新时代的需求。

理想的结果是一个进化的 AOC，能够比对手更快地执行 OODA 循环，不受传统的相对固定的 44 至 96 小时空中任务指令（ATO）处理周期的限制。在 ABMS 的支持下，AOC 需要加速从所有相关来源收集数据，压缩其处理和路由的时间和复杂性，以更快、更灵活的周期进行规划和决策，并迅速动员部队执行计划，尽管持续作战节奏带来的部队生成和后勤限制。这样做不仅需要包括美国空军和太空部队在内的空军部和联合美国军事资产，还需要多国盟友和伙伴的参与，以在战术、作战和战略层面的规划、指挥和交战中提供决策优势。

1.4 先进战斗管理系统（ABMS）

ABMS 究竟是什么？它寻求实现什么目标？ABMS 是一个单一的采办系统还是涉及多个系统的战略概念？今天可以预期 ABMS 能够产生什么成果，实现 ABMS 和 JADC2 背后的完整概念面临哪些挑战？以下部分提供了初步的答案，并在后续章节中进一步详细阐述。

1.4.1 ABMS 的演变

ABMS 从最初作为指挥与控制（C2）和监视系统的概念演变为目前的企业级系统家族。作为一个平台，ABMS 最初于 2017 年作为“空中战斗管理和监视”系统推出，这是一个传统的采办项目，旨在替换和现代化老化的空中预警与控制系统（AWACS）平台和即将退役的 E-8C 联合监视和目标攻击雷达系统（JSTARS）机队。⁴⁶ 然而，鉴于《国家防务战略》（NDS），空军认为其最初的 ABMS 计划已不再符合 NDS 中概述的目标。空军领导重新评估了 ABMS 的需求，寻求开发能够在受限环境中运行的更为强大和可生存的新选项。⁴⁷ 空军得出结论，“单一平台，例如一架飞机，不再是提供跨多个领域的 C2 能力的正确解决方案。”⁴⁸

2019 年 4 月，空军部宣布，空中战斗管理系统将转变为先进战斗管理系统——一个多域分层的 C2 系统家族（而非单一的现代化项目），以实现“任何传感器都可以与任何射手对话，无论是在太空、陆地、海上、空中还是网络空间……[并] 执行与 JSTARS 和 AWACS 平台相关的任务集，并可能承担战区空中控制系统 [和] 地面移动目标指示器的其他角色。”⁴⁹ 这一转变推动了“空军的一种全新采办模式”，它“设想了多个贡献计划，如 ABMS 空间、ABMS 空中和 ABMS 网络与通信——每个计划都有自己的资金、项目经理和时间表。”⁵⁰ 此外，还涉及聘用一位“首席架构师……负责监督 ABMS 架构设计、企业通信和跨项目整合 [以及] 识别技术以实现跨作战环境和作战领域的横向和纵向整合。”⁵¹

然而，最近新任空军部长 Frank Kendall 审查了 ABMS 的重点。他特别认为，ABMS “在实现和部署可测量的具体作战成果方面没有足够的专注”，并主张“在定义的时间内开发具体、实用的军事技术。”⁵² 他认为，空军部需要首先确定 ABMS 应在何种作战环境下传输哪些具体类型的数据和信息。他还要求建立绩效指标，以确定 ABMS 是否在当前的 C2 能力上取得了显著改进，委员会对此完全支持。尽管部长指示对 ABMS 进行重新校准，但委员会的后续分析基于从 2020 年底到 2021 年春季进行的数据收集阶段提供的信息。因此，下面概述的许多细节基于早期的 ABMS 方法。然而，许多发现和建议在 ABMS 继续其进化之旅时仍然具有相关性。

1.4.2 非传统采办方法

作为一个系统集成概念和愿景架构，旨在整合从传感器到射手的全域联合指挥、控制、通信、计算机、情报、监视、侦察（C4ISR）和作战，ABMS 由“一个情报、监视和侦察传感器网络组成，并将利用基于云的数据共享，为战斗人员提供空中、陆地、海洋、太空和网络领域的战场态势感知。”⁵³ 空军设想将 ABMS 开发为一个不断演变的“多系统家族”⁵⁴，而不是传统意义上的单一采办项目（具有一组明确定义或固定的需求、全面的成本估算和单一的交付时间表）。相反，ABMS 旨在利用商业和集成的国防能力，成为一个程序集群或操作概念和架构，在该架构内，单个程序将获得特定能力。

这些能力在先前的大规模“上坡”技术评估和演示中得到探索，用于原型和测试利用商业技术的机会。⁵⁵ 示例包括云计算⁵⁶ 和具有 AI 和机器学习（ML）能力的通信基础设施，用于处理和路由信息给需要信息的指挥官、决策者和操作员，以及决策支持工具。定制的应用程序和硬件正在测试中，以互连以前无法共享信息的传感器和系统，并扩展最后一公里

战术边缘通信，以改善对传感器和射手的访问。⁵⁷ 到目前为止，空军已经进行了五次大规模的上坡演示，以展示其寻求最终部署的新 C2 能力；由于预算限制，第六次演示在 2021 年 3 月被取消。⁵⁸

ABMS 旨在随着时间的推移继续利用不断发展的（主要是商业）技术，而不是建立一个静态的系统集成，展示现有技术。这意味着 ABMS 作为一个空军部级别的总体活动，而不是一个传统的 C2 项目，因此没有一组固定的需求来构建，没有单一的成本估算，也没有一组单一的操作能力来部署。⁵⁹ 相反，重点主要是设计企业规模的架构，并制定要求以确保“在将构成 [ABMS] 的系统菜单中得到满足。”⁶⁰ 联合参谋部的 J6 指挥、控制、通信和计算机/网络组织正在制定总体战略需求，以通过 JADC2 展示 JWC，在此框架内，为随着时间推移将获得的特定要素制定具体的需求、系统设计和成本估算。⁶¹

空军部的战略性和非传统采办方法，加上向国会提出的大量资金请求（2020 财年为 1.365 亿美元；2021 财年为 3.023 亿美元；2022 财年为 2.038 亿美元），引发了关于如何核算跨多个项目获取、开发和全面整合 ABMS 元素的成本，以及将正在开发的技术转移到现有武器系统中的策略的问题。⁶² 委员会根据空军部提供的技术数据认为资金请求是适当的，但担心缺乏更清晰和更详细的项目规划将挑战 ABMS 满足作战需求的能力。根据政府问责办公室（GAO）的说法，“没有合理业务案例的武器系统更容易出现进度延迟、成本增加和集成问题。”⁶³ 他们引用了多个相关国防部项目的例子，如陆军的未来战斗系统、联合战术无线电系统和变革性卫星通信系统，作为由于技术不成熟和未经验证而被取消的项目的证据。⁶⁴

由于空军没有为 ABMS 建立固定的需求，也没有进行可承受性分析，国会选择将空军 2021 年 ABMS 预算削减一半，仅分配了 1.59 亿美元，而空军请求的为 3.023 亿美元。⁶⁵ 空军部长也表示怀疑，并要求“具有实质性军事能力，而不仅仅是展示你可以做什么酷炫的事情。”⁶⁶ 这导致空军的优先事项从大规模的上坡实验转向专注于交付具体能力，将 2022 财年 2.04 亿美元预算请求中的一半以上用于获取空中数据链吊舱，以使 KC-46 加油机能够改进 F-35 和 F-22 之间的数据流。⁶⁷ 空军部还在其 2022 财年预算提交中提供了比往年更多的细节和具体性，并将其原计划的预算请求减少了一半以上（从 4.493 亿美元减少到 2.038 亿美元）。⁶⁸

对于 ABMS 的技术基础也存在担忧。⁶⁹ 例如，正在考虑的技术的成熟度如何，如何在预期的威胁、不确定性和战斗人员需求之间优先考虑技术，如何将遗留技术和平台纳入新技术中？单纯为了技术而使用技术并没有价值；关键在于技术如何应对威胁下的作战优先事项。ABMS 的上坡演示（演示）可能有用，但需要解决“将传输哪些信息及其原因，目标是什么，以及这些结果将如何改进当前的指挥与控制能力。”⁷⁰

1.4.3 从演示到能力发布

在近两年的上坡演示之后，前空军部采办、技术与后勤助理部长在 2020 年 11 月指示将 ABMS 从空军部首席架构师办公室转移到空军部快速能力办公室（DAF RCO），作为整合项目执行办公室（PEO）。⁷¹ 这样做的目的是将重点从演示和实验转移到 ABMS 能力的部署和操作化。虽然空军部首席架构师将规范 ABMS 的技术要求，促进跨空军部的企业数字架构和标准的整合，建立并提供基于模型的系统工程工具，并继续指导未来的上坡演示，空军部快速能力办公室作为主要整合 PEO，将负责起草 ABMS 采办策略和业务案例，交付并整合所有 ABMS 能力以纳入架构评估上坡，并指导能力发布的开发。⁷²

在 2021 年 5 月，空军参谋长宣布空军部正在进入 ABMS 的下一个阶段。“近两年的严格开发和实验毫无疑问地展示了 ABMS 的前景。我们已经证明，ABMS 的努力可以从空中、

陆地、海洋、太空和网络领域收集大量数据，处理这些信息并以一种能够实现更快和更好决策的方式共享。”⁷³ 空军部宣布了 ABMS 的首次能力发布 (CR1)：在 KC-46 Pegasus 加油机上部署 4 到 10 个新的数据链吊舱，以促进 F-22 和 F-35 战斗机之间不兼容的无线电系统的通信。⁷⁴ 这些吊舱将作为空中的热点连接两架战斗机，实现实时通信。“最终目标不仅是为第五代战斗机提供‘翻译’软件，而是继续构建空军需要的能力，以管理未来的全域作战——从连接性到机器速度决策，再到远离总部的指挥官之间的实时数据共享。”⁷⁵ 此外，空军参谋长不仅希望将信息推送到战术边缘指挥中心，还希望将数据带回来。“我们每个平台上都有一定程度的数据……但有时，它被绑定在平台上，直到你把它带回地面。为什么要等几个小时才能拿回来……当你实际上可以实时推动这些信息和数据来驱动决策？”⁷⁶ 空军部计划在本财年投资 1.7 亿美元来执行 CR1。⁷⁷

虽然尚未正式确定，但第二次能力发布 (CR2) 可能会“使用云计算、光纤网络、人工智能 (AI) 和其他新技术”来加速国土防御任务和决策支持，以支持美国北方司令部 (USNORTHCOM) 和北美航空航天防御司令部 (NORAD)。⁷⁸ 这些主要是商业能力在 2020 年秋季进行的大规模演示 ABMS 上坡 2 期间进行了测试和展示。这次演习称为 Nellis 影子作战中心 (ShOC-N)，为商业供应商和国防部参与者建立了一个虚拟环境，与国土防御机构进行操作和连接，以提供一个共同作战图 (COP)。供应商测试了他们的连接性和在 USNORTHCOM 战区内提供实时态势感知的能力。⁷⁹

展望未来，空军部快速能力办公室 (DAF RCO) 计划在未来的上坡演示中，基于成功的能力展示，引入新的数字能力，以支持即将发布的能力。根据其主任的说法，“要构建 ABMS，首先必须建立存储、计算和传输关键数据的数字结构和路径。空军部需要一个智能、快速和具有韧性的‘系统之系统’来建立信息和决策优势，而 ABMS 将是该解决方案。”⁸⁰

1.4.4 ABMS 作为 JADC2 的贡献者

作为空军部 (DAF) 对联合全域指挥与控制 (JADC2) 的贡献，ABMS 被设计成“一个由传感器、融合和数据传输网络组成的生态系统，通过云处理能力和人工智能 (AI) 的辅助，赋能现代化的 C2。”⁸¹ 其目标是使分离且常常不兼容的设备能够在所有领域内无缝、安全地通信。

作为一种技术解决方案，ABMS 提供了跨越所有战场和领域的连接和理解，无需考虑边界，以确保“所有 11 个作战司令部都能基于相同的理解进行操作。他们可以共同规划，然后共同执行。”⁸² 技术能力通过 DevSecOps 快速开发方法得以推进，每 4 个月刷新一次。根据空军部领导的说法，ABMS 将通过“同时感知、理解并对来自 [所有] 领域的海量数据和信息采取行动，在机器学习 (ML) 和人工智能的帮助下融合和分析数据，并以前所未见的速度为战斗人员提供首选方案”来实现 JADC2。⁸³

虽然国防部 (DoD) 努力实现所有领域的网络连接，但近期的重点主要是建立与 JADC2 相关的训练和教义。在由空战司令部 (ACC) 司令领导的 2021 年空军部指挥与控制峰会上，讨论的重点是“如何通过教义和训练的创新来利用先进技术和人工智能，优化决策速度，调整组织结构以利用技术创新和效率，从而在竞争和冲突的各个层面取胜，并继续发展全域技能和决策导向的领导者，以规划和执行 JADC2。”⁸⁴ 为了满足这些需求，空军的联合作战整合跨职能负责人最近宣布完成了一个 JADC2 支持概念，指导空军部“基于概念驱动、威胁信息化的 JADC2 能力开发，包括教义、训练物资和人员。”⁸⁵ 此外，空军设立了一个新的 13O 空军专业代码 (AFSC)，旨在确保在空中、太空和网络空间领域的持续主导地位。被编码为 13O 的人员接受训练，以在多个作战领域的操作层面规划和执行多域作战。这些集体努力的目标是“培养我们的人员成为知识渊博、果断的领导者，能够在联合的高科技环境中进行规划和执行，在这种环境中，人工智能和机器学习也在与他们一起参与战斗。”⁸⁶

为了进一步指导 ABMS 及其对 JADC2 的支持，美国空军参谋长 Charles Q. Brown, Jr. 将军在 2021 年 5 月签署了 ABMS 活动计划。该计划包括空军部希望实现决策优势的八项作战能力：(1) 数据共享；(2) 人力资本发展；(3) 分布式决策；(4) 先进通信；(5) 先进感知；(6) 综合规划；(7) 效应汇聚的 C2；(8) 加速决策。⁸⁷ 这些能力共同使 ABMS 能够安全地从空中、陆地、海洋、太空和网络领域收集和传输大量数据，并在联合部队和多国伙伴之间处理和共享信息——这是 JADC2 任务的基石。

1.4.5 其他对 JADC2 的贡献者及其复杂因素

最初由空军部领导提出作为国防部（DoD）主要 JADC2 解决方案的 ABMS，自那时起其他军种和 DoD 机构也提出了他们对 JADC2 的贡献。陆军和海军部（DoN）都启动了类似于 ABMS 的努力。每个军种都寻求通过原型设计和实验技术与作战方法来支持全域联合战斗指挥（JWC）。陆军通过“融合项目”（Project Convergence, PC）来实现联合和联合优势，解决联合作战环境的需求，⁸⁸ 而海军部则通过“超越项目”（Project Overmatch）开发网络、基础设施、数据架构、工具和分析方法，以支持海上优势和 JADC2 的互操作性。⁸⁹

虽然支持 JADC2 的目标是每个开发的核心，但每个军种采用的方法却有很大不同。例如，PC 被提议为“一个积极追求 AI 和 ML 驱动的战场管理系统的学习活动”，⁹⁰ 并围绕五个核心要素设计：人员、武器系统、C2、信息和地形。⁹¹ PC 强调通过利用 AI、机器人技术和自治系统来大规模构建杀伤力。⁹² 负责领导该工作的组织是陆军未来司令部（AFC），计划每年运行 PC，通过技术、设备和士兵反馈进行频繁实验，最终在年度演习或演示中实现目标。⁹³

相比之下，海军“设想一个未来舰队，其中有人和无人驾驶的舰船、潜艇和飞机以分散方式操作，收集大量数据以填补共同作战图（COP），操作指挥官可以使用这些数据将最佳传感器平台的目标数据发送给最佳射手以攻击敌人。”⁹⁴ 超越项目是“海军的努力，旨在创建一个‘海军作战架构’，以连接舰船与陆军和空军资产。”⁹⁵ 并采用工程开发方法“使海军能够在海上进行蜂拥作战，从近处和远处、每个轴线和每个领域发出同步的致命和非致命效果。”⁹⁶ 其目标是“开发支持操作和开发环境的网络、基础设施、数据架构、工具和分析方法，从而实现我们持续的海上优势。”⁹⁷ 根据海军信息作战系统司令部司令和超越项目主任的说法，海军部将利用并整合最新的数字技术，包括 AI、ML 和信息与网络技术，进入现有的海军部网络和平台，以实现全球舰队战备的改进。⁹⁸ 这个目标不仅仅是为了获取新解决方案，而是为了利用现有 C2 网络和平台，提高其作战效能。

除了军种之外，国防高级研究计划局（DARPA）已经建立了马赛克战争⁹⁹，国防部（研究与工程）办公室也已建立了全面联网的指挥、控制与通信（FNC3），作为他们对联合全域指挥控制（JADC2）的贡献。¹⁰⁰ 美国特种作战司令部（SOCOM）也在开发其特种作战部队（SOF）专用的数据管理环境（数据结构），并配备一套通用标准和工具，以便 SOF 系统之间能够相互通信。¹⁰¹ 这些努力的目的是利用关键的商业技术来改进和增强 C2 操作；但同样地，几乎没有进行任何协调来确保全局解决方案的实现。

当然，挑战在于这些努力都在尝试跨服务和机构的联合互操作性，这涉及到各自的能力和资产，因此最终会出现控制和管辖权的问题。此外，尽管这些努力在松散地协调，但几乎没有进行协调来明确究竟谁的方法适用、使用哪个系统、在哪个战域操作，以及针对哪个威胁联合和服务指挥控制姿态。这一挑战更加复杂，因为 JADC2 旨在将多国盟友合作伙伴纳入规划（而不是在部署后才考虑），但与军种和支持机构的概念和系统之间未解决的差异相比，这些考虑还处于初期阶段。¹⁰² 因此，如果没有适当的协调、明确的角色和责任划分以及通用的操作标准，风险在于“每个军种、COCOM（作战司令部）或机构都会走自己的

方向，开发多个烟囱式的网络，而无法实现通过更协调的方法所能达到的互操作性和韧性。”

103

在接下来的章节中，委员会将详细审查计划中的 ABMS 数据和通信架构，回顾拟议的治理方法和支撑过程，并提出解决已识别技术差距和改进流程的路径，以更有效地实现 ABMS 能力。最后一章将总结委员会的主要发现和建议。

2 架构与数据

我们正在构建和使用的能力，其实是设计成像乐高积木一样能够拼接的，无论是我们的空军能力，还是我们的兄弟部队和国际合作伙伴的能力……这种架构的力量通过服务、盟友和合作伙伴共同努力，在机器速度下连接网络和共享信息来实现。这就是全域优势。

— Preston Dunlap, Chief Architect, U.S. Department of the Air Force¹

2.1 架构概述

高级战斗管理系统（ABMS）的架构指的是各个系统组件和能力之间的关系和互联。架构的细化程度通常在系统和子系统级别进行描述，每个子系统组件中都包含多个能力。这些子组件通过多种技术实现模块化和互联，包括有线和无线通信、单个平台内的互联框架、卫星通信（SATCOM）系统以及商用电信。其目的是整合所有组件和互联，以实现更大的系统目标——在本案例中，即跨越整个空军部（DAF）传感器、网络组件和武器系统的协调指挥与控制（C2），以及连接到更大的联合全域指挥与控制（JADC2）企业架构。图 2.1 提供了 ABMS 的概述，图 2.2 详细展示了 ABMS 的概念。

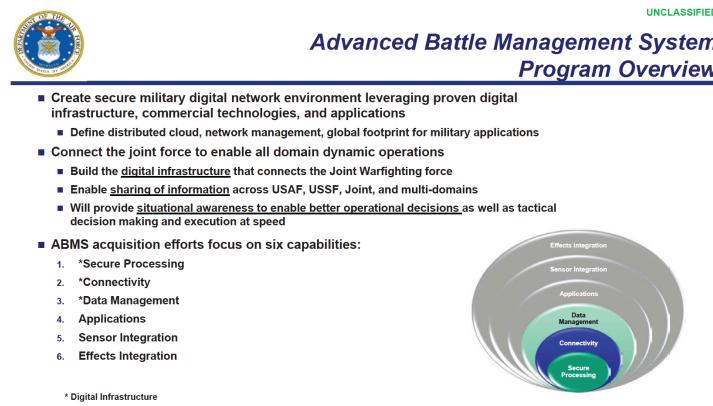


Figure 2.1: 高级战斗管理计划概述。来源：空军部快速能力办公室。已批准公开发布。

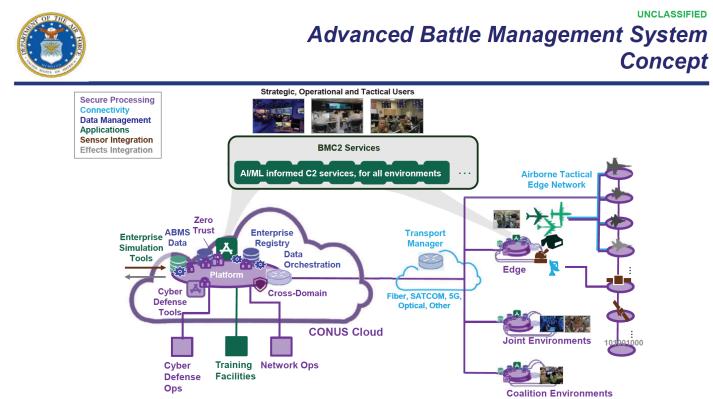


Figure 2.2: 高级战斗管理系統概念。来源：空军部快速能力办公室。已批准公开发布。

作为一个 C2 系统家族，ABMS 涉及支持计算、传感和执行的数据信息处理和通信，执行的定义为武器效果的应用²。在当前构架下，每个 C2 节点都具备在传感器、数据和执行

的使用中提供自主计算的能力。这一架构的成功根本上依赖于严格遵循应用程序接口（API）和数据标准，这些标准提供了一个通用的应用环境和一套灵活的协议。

ABMS 架构还旨在与 JADC2 的各个元素紧密联系，尽管委员会几乎没有看到这方面的证据。焦点似乎主要在于定义空军部（DAF）本身的 ABMS 特定平台、组件和互联。委员会强烈鼓励在联合层面上开发 ABMS 架构，以实现与其他军种和多国合作伙伴的互操作性。

还需要定义一个开放、模块化且（最重要的）可扩展的标准，以确保陆军、海军、海军陆战队、国防部各机构及多国合作伙伴的资产（或他们的 JADC2 系统部分）能够有效地与 JWC 设想的 ABMS 架构集成。创新和“智能”系统还需要与传统系统集成和/或互操作。此外，由于大多数美国武器系统由国防工业基地的主要系统集成商设计和供应，他们应在整个开发过程中积极参与。

发现 1：为了支持 JWC，必须将 ABMS 架构视为 JADC2 的一个不可或缺的部分，这需要明确界定。

发现 2：需要一个开放、模块化的设计来支持 ABMS 和 JADC2 的发展。

建议 1：空军部首席架构师办公室和空军部快速能力办公室应在联合全域指挥与控制（JADC2）层面上定义高级战斗管理系统（ABMS）架构，以确保与其他正在开发的类似 ABMS 系统的互操作性。

建议 2：联合参谋部 J6 或指定的美国国防部执行代理人应为所有参与联合全域指挥与控制（JADC2）的系统建立互操作性要求和性能指标，以便最终集成所有能力。

建议 3：空军部首席架构师办公室和空军部快速能力办公室应设计高级战斗管理系统（ABMS）架构，使其具有模块化特性，并包括开放标准和接口，以便与其他军种的变种系统进行配置。

ABMS 架构应具备在所有应用中实现通信、数据和计算的完整性、可用性和保密性的能力。目标不仅是建立一个共同作战图（COP），而且是建立一个可用于任何边缘战略或战术决策的数据全貌表示。如果战术边缘能够得到足够的相关数据支持，那么指挥官意图的速度可以在一定程度上得以维持。如果战术边缘得不到服务，而战略层面得到了服务，那么相关行动及其结果将最多受到限制，最坏情况下将无效。

还应强调在退化或拒绝环境中运行的通信、数据和计算，在这种环境中，断开连接或高延迟组件需要具备一定程度的自主运行能力。更重要的是，保护 ABMS——包括系统和数据——免受网络漏洞和对手攻击，需要将网络安全纳入整体架构设计的一部分。

发现 3：ABMS 架构需要为所有通信、数据和计算元素提供完整性、可用性和保密性。

建议 4：空军部首席架构师办公室和空军部快速能力办公室应设计高级战斗管理系统（ABMS）架构，制定具体的技术要求和解决方案，以确保在退化或拒绝访问环境中，通信、数据和计算能够继续运行。

2.1.1 架构和技术状态

简而言之，ABMS 架构由一系列平台、传感器、网络和数据链通过安全云³互联，以便在联合全域环境中实现感知、感知理解和行动。图 2.3 展示了 ABMS 架构。

ABMS 是一个系统家族，包括硬件和软件，通过技术支持来输入并连接到 JADC2 网络。在空军部首席架构师的原始管理下，它包括六个产品（即技术和能力）类别：⁴

1. 传感器集成，包括卫星和飞机上的传感器、地面雷达等；
2. 数据和数据管理；
3. 安全处理，涉及网络安全以及跨所有分类传输和处理数据的能力，同时允许广泛访问数据产品；
4. 连接性，包括军用和商用网络中的人工智能（AI）和机器对机器链接，适用于传统和新型武器平台；
5. 应用程序；以及
6. 效果集成。

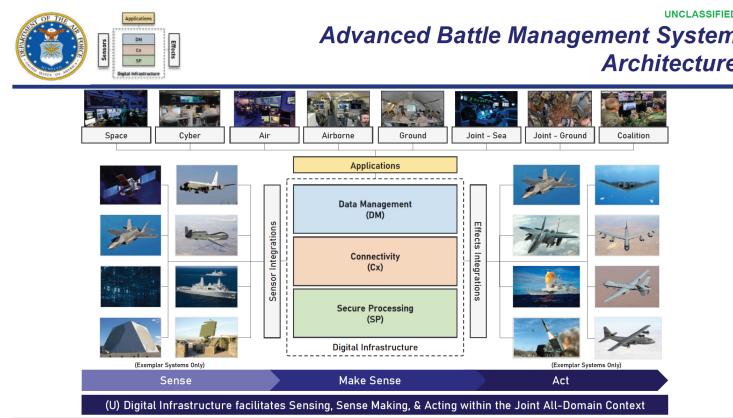


Figure 2.3: 高级战斗管理系统架构。来源：空军部快速能力办公室。已批准公开发布。

这些原始产品类别或能力中的每一个都是通过在上坡实验期间进行的每 4 个月一次的“演示冲刺”迭代开发的。⁵ 在空军部首席架构师向委员会作出介绍时，它们由多条软件产品线支持，包括：

- cloudONE：支持 ABMS 企业内多级分类的安全云；
- edgeONE：在数据链与 cloudONE 断开连接时作为本地云备份；
- dataONE：建立在统一数据库 (UDL) 基础上的数据库；⁶
- crossDomainONE：实现跨分类级别的数据传输；
- omniaONE：通过一个名为 fuseONE 的云端融合环境使用多个数据源合并的全域战场共同作战图；
- AI/smartONE：基于 omniaONE，通过人工智能提示用户潜在有用的信息；
- feedONE：来自所有来源的云端数据馈送；
- commandONE：使用 Link16e 网络的战斗管理指挥与控制系统；⁷
- gatewayONE：设计用于在多个平台和域之间确保双向数据路径的通信网关。⁸

ABMS 还由各种硬件产品线支持，包括：

- radioONE：用于接收 SATCOM 数据的新射频天线；
- apertureONE：用于通信和雷达的通用孔径；
- boxONE：用于访问 cloudONE 或 edgeONE 的工作站；
- phoneONE：用于访问 cloudONE 或 edgeONE 的智能手机；以及其他设备。⁹

目标是将所有这些元素连接成一个整体的数据集成和指挥决策辅助系统，以加速发现、定位、目标指示、跟踪、交战和评估（FFTTEA）杀伤链。委员会未对这些产品类别中的每一项作出评定，因为未提供有关其总体性能的信息。

ABMS 架构仍处于初期阶段，并在不断发展中。若不逐一检查每个组件，很难理解 ABMS 架构的全貌，因为它是从底层构建起来的。“当我们说‘从底层构建’时，我们的意思是这种迭代实验过程应该在战术层面进行。ABMS 的最终用户——联合传感器和射手——应当是那些在循环试验新技术和方法的人，这些将会形成 ABMS。”¹⁰ 需要注意的是，尽管每个组件都是作为构建模块开发的，ABMS 是设计为一个将每个模块集成到其核心架构中的庞大生态系统。随着新技术和能力的出现并在上坡演习中进行实验，经过验证的技术将在能力发布中投入使用。因此，ABMS 架构正在演变，并处于定义的早期阶段。

作为一个可能的连接框架，时间触发架构（TTA）可能是一个可行的选项。¹¹ TTA 是一种集成框架，为将组件集成到系统中提供了一个环境，在这种环境中，框架独立于组件为系统保证了某些属性。¹²

在此框架内具备快速适应变化的条件、任务需求、技术改进和威胁的能力。¹³ 使用 TTA 的优点在于“精确指定节点之间的接口，简化通信和协议达成，进行快速错误检测，并保证实时应用程序的及时性。”¹⁴ 它已经在汽车应用（如奥迪、标致等）和航空应用（如霍尼韦尔航空航天）中得到应用。¹⁵

此外，为了支持 JADC2 的目标，ABMS 架构需要保持可演化性，允许在时间上进行持续开发、部署、测试、改进和完善。虽然空军部领导人在开发 ABMS 时已经接受了灵活性，但国会决定将 ABMS 2021 财年的预算减少近一半，这可能会阻碍部门继续采取这一方法的能力。¹⁶ 根据空军部代理采购、技术和物流助理部长的说法，“我们正在尽全力保持工作的进行……但如此大规模的削减将产生影响。”¹⁷

ABMS 架构必须专注于保护数据、计算和通信免受对手访问或操纵；提供具有显著冗余和弹性的高带宽通信；部署具备多余或扩展容量的先进计算平台，以同时处理数千个并行的 C2 任务；提供大型数据管理和存储，使所有决策支持节点能够近实时访问数据；并允许与传统平台和跨军种系统及网络的互操作。此外，该架构应保持模块化，具有基于实际操作性并理想上有成功实施记录的标准化开放接口，以便随着技术进步，新组件可以轻松地集成到 ABMS 中，以更好地实现所有任务要求。使用开放标准和 API 将促进快速采用新技术，这对于实现未来通信、计算、数据和软件改进的集成至关重要。

发现 4： ABMS 架构必须具备适应性，以便在时间上实现持续开发、部署、测试、改进和完善。

发现 5： 按照目前的计划，如果要完全实现 JADC2 JWC，ABMS 架构可能会面临互操作性挑战。

2.1.2 数据中心战 (Data-Centric Operations) 技术

当前国防部的通信主要是点对点的。¹⁸ 在一个复杂而分散的国防部企业中推进指挥、控制、通信、计算机、情报、监视和侦察（C4ISR）架构，以利用更新、更灵活的战略和战术级别网络通信解决方案，将需要大量时间、资源和承诺。随着越来越多的操作转向数据中心

化，在企业架构设计中，考虑数据——更具体地说，数据的访问、存储、传输、验证和保护——至关重要。

支持数据中心作战的现代工具越来越多。这些工具范围从支持应用到应用接口的工具到使用云来提供按需计算、存储和共享的工具。¹⁹ 其他还包括预测分析、数据虚拟化、流分析、分布式存储、数据预处理等。²⁰ 尽管像 DARPA 的数据翻译和快速软件集成工具（即异构电子系统系统技术集成工具链，STITCHES）等能力可以支持架构转型并促进战术操作，ABMS 还必须支持高度敏感的战略任务的数据和计算需求，包括核指挥、控制和通信（NC3）操作。采用一系列能够支持各种能力的数据交换技术应始终是 ABMS 架构设计的核心目标。

随着人工智能/机器学习（AI/ML）技术变得越来越普及和强大，在可接受的时间范围内实现大规模的机器对机器数据共享（无论是计划内的还是意外的任务需求）将变得越来越重要，并且必须完全集成到 ABMS 和 JADC2 架构设计中。目前的机器对机器数据共享主要是点对点的，用于支持预定数据流的计划和预期任务。然而，随着对手快速推进其自身的 AI/ML 应用，国防部和空军部需要实施先进的 AI 能力，以提高从战术操作到战略规划层面的指挥控制（C2）和时间敏感的决策能力。²¹ 实施强大的机器对机器数据共享能力至少需要：

- 适当安排数据存储和计算，以便及时访问和获取数据，以支持军事行动；
- 数据存储的安全性和同步；以及
- 在退化环境中支持操作和重建的冗余性；等。

建议 5：空军部快速能力办公室应采用一系列数据交换技术，以支持从战术到战略的全部能力范围。

2.1.3 高性能处理：人工智能和机器学习

通信不仅需要网络化，还需要实现人与机器之间、机器与机器之间的直接连接和中继。作为一个指挥控制（C2）网络，ABMS 需要快速、准确、安全和有弹性的数据处理。这将涉及大量复杂数据和事件处理，并增加时间敏感性和服务质量需求，特别是在干扰和通信不良的争夺区域。如果没有机器的帮助，处理、验证和解释大量数据将会延迟并使用户不堪重负。

根据国家人工智能安全委员会的报告，“AI 是典型的‘双用途’技术。机器能够比人类更快、更准确地感知、评估和行动，这在任何领域——无论是民用还是军事——都是一种竞争优势。”²² 随着对手在这一领域的竞争（甚至超过）美国军方，采用 AI/ML 来加速数据传输和决策将变得越来越重要。

目前，决策过程涉及操作员手动观看数据流、在纸上做笔记、打电话与监控不同数据流的其他操作员核对信息、在计算机中心之间走动以讨论关键信息，并使用他们自己的（人类）分析来提供视觉和口头更新以传达这些信息给决策者。因此，这种方法需要大量人力，容易出现人为错误，并且由于传达的大量复杂数据而显著延迟决策。²³

为了解决这一缺陷，空军部首席架构师和空军快速能力办公室正在使用 AI 作为支持，并招募商业公司提供基于 AI/ML 的分析来转变 ABMS 的 C2 能力。他们将 AI 作为 ABMS 的 smartONE 能力的一部分，开发用于感知和综合数据的算法。在 ABMS 的 on-ramp 2 演习中，用户能够结合使用 smartONE 和 omniaONE（一个共同作战图），提示用户有关对手战略资产的潜在有用信息。²⁴ AI 也在 on-ramp 4 中进行了测试和应用，作为杀伤链的一部分。用户能够通过 cloudONE（战术边缘云）和 dataONE（ABMS 的通用数据标准化存储库）在不同平台之间快速传递数据。此外，演示还使用 AI 进行目标定位和火力打击。

最终目标是利用 AI/ML 提供更多的自动化和预测分析，以更快地加速数据传输和决策。空军战略、整合和需求局的联合部队整合主任解释道：“我们要做的是找出方法，将同样的信息通过系统实现机器对机器的传输。因此，通过自动化过程……帮助理解或以过去可能没有连接的方式连接这些点。这样，当这些信息呈现给决策者时，他们能够做出高度知情且快速的决策。”²⁵

最终目标是利用 AI/ML 提供更多的自动化和预测分析，以更快地加速数据传输和决策。空军战略、整合和需求局的联合部队整合主任解释道：“我们要做的是找出方法，将同样的信息通过系统实现机器对机器的传输。因此，通过自动化过程……帮助理解或以过去可能没有连接的方式连接这些点。这样，当这些信息呈现给决策者时，他们能够做出高度知情且快速的决策。”²⁵

委员会认为这些努力是将人工智能/机器学习 (AI/ML) 引入先进战斗管理系统 (ABMS) 的重要第一步。然而，需要在 ABMS 中更全面地扩展人工智能的应用。一个可以考虑使用的商业能力是高效处理技术，例如超级自动化或智能过程自动化。超级自动化是一种“以业务为导向的、有纪律的方法，组织用其来迅速识别、审查并自动化尽可能多的业务和 IT 流程。[它] 涉及多种技术、工具或平台的协调使用”，包括以下内容：

- 人工智能 (AI)；
- 机器学习 (ML)；
- 事件驱动的软件架构；
- 机器人流程自动化 (RPA)；
- 业务流程管理 (BPM) 和智能业务流程管理套件 (iBPMS)；
- 集成平台即服务 (iPaaS)；
- 低代码/无代码工具；
- 包装软件；
- 其他类型的决策、流程和任务自动化工具。²⁶

虽然主要用于商业系统，但在 ABMS 的背景下，超级自动化可以通过进一步自动化高级指挥与控制 (C2) 功能和数据处理来提高信息处理的准确性并加速决策过程。在商业部门，公司正在使用超级自动化来减轻操作员的负担，并在训练有素的多高质量数据集下，将预测分析的准确性提高多达 95%。²⁷

为了提高和维持数据收集的质量，可以考虑采用自动化机器学习 (AutoML) 过程。AutoML 是“自动化耗时的迭代机器学习模型开发任务的过程。它使数据科学家、分析师和开发人员能够以高规模、效率和生产力构建机器学习模型，同时保持模型质量。”²⁸ 这些结合的过程将使 ABMS 开发人员和用户能够提高数据处理的效率和效果，从而为国家的信息优势做出贡献。

建议 6：在最大可能范围内，空军部首席建筑师办公室和空军部快速能力办公室应设计并执行一项全面的人工智能战略，包括所有元素，如学说、指挥链、政策、联合环境中的武器释放授权、与联合全域指挥与控制的接口，而不仅仅是高级战斗管理系统的选定能力。

2.1.4 数据和数据标准

如国防部《数据战略》中所强调的，数据是一项战略资产。²⁹ 在 ABMS 中，数据构成了了解情况和指挥、控制、操作军队所需的情报、指示、警告、信号、状态、情况、命令、

控制和其他多模式信息。因此，“在国防部，数据是一种高利益商品，必须以带来即时和持久军事优势的方式加以利用。”³⁰

将数据视为战略资产需要始终保持数据的出处和安全性。原始来源和组合数据应立即被标记、编目和安全存储。“在一个依赖数据且数据饱和的世界中，胜利属于决策优越的一方——即能够感知、理解复杂且适应性环境，并采取更聪明、更快、更好行动的一方。”³¹

然而，没有一套企业级的数据标准，特别是每个军种和国防部机构都建立自己的 JADC2 贡献时，无法实现大规模的信息共享。国防部的《数据战略》提供了“转变为数据中心企业所需的总体愿景、关注领域、指导原则、基本能力和目标。”³² 但它指示每个军种和国防部组件/机构制定自己的数据战略实施计划。这可能会导致不一致和不必要的冗余。

联合参谋部 J6 是国防部为 JADC2 建立通用数据标准的主导机构。J6 通过其 JADC2 跨职能团队 (CFT) 举办了月度会议，CFT 由国防部机构、军种、美国国土安全部和北约的成员组成。CFT 于 2021 年 1 月举行了为期多天的数据峰会，目的是为 JADC2 开发一个通用数据结构³³，该结构包括标准词汇、性能指标和设定通用数据标准的要求。³⁴ 到目前为止，CFT 已经开发了一套通用词汇，并确定了数据结构定义的组成部分，这些组成部分将转化为指导后续 JADC2 支持工作的目标。这些组件包括元数据标记、通用数据接口、数据访问控制、数据安全和数据基础设施。³⁵ 尽管如此，由于制定既不太严格也不太开放的标准的挑战，通用数据结构尚未完成。

此外，J6 在 2021 年 6 月发布了一份机密的 JADC2 战略，“提供了必要的治理和框架，以实现人工智能、机器学习、预测分析和其他新兴技术的快速集成。”³⁶ 该战略侧重于五个具体的努力方向 (LOEs)，包括数据、人力企业、技术、核指挥与控制以及任务伙伴环境。³⁷ 最近，J6 正在敲定一项机密的 JADC2 实施战略的细节，该战略包括目标、任务交易、里程碑、服务贡献（包括 ABMS）以及战斗指挥和其他国防部机构正在进行的其他工作。近期（2022 财年）的重点将是开发最低可行产品和增强能力，如 DevSecOps、身份、凭证和访问管理 (ICAM)、零信任 (ZT)、传输层和云。³⁸ 为了确保通用软件标准，J6 还与联合需求监督委员会 (JROC) 合作，强制实施开放软件标准，以通过使用通用软件接口确保跨军种和跨域的兼容性和互操作性。³⁹ 这些集体努力为 ABMS（以及项目融合和项目超越）提供了支持其各自开发活动的指导基础。

**建议 7：联合全域指挥与控制跨职能团队应立即就通用数据结构
和数据安全级别达成一致，并在联合层面定义数据标准和工具。
如果没有一套公认的开放标准和已知接口交换要求且不限制创新，
军种可能会开发出不兼容和孤立的解决方案。**

2.1.5 容器化和 Kubernetes

为了在持续集成/持续交付和部署 (CI/CD) 环境中实现敏捷开发，容器化是最佳解决方案。容器指的是轻量级虚拟机，可以预配置并上传到云环境或本地 (on-prem) 环境，以立即提供所需的软件功能及支持操作系统库和依赖项，完全支持该功能。⁴⁰ 通过将所有依赖项封装在容器内，可以避免与不同操作系统和硬件平台的昂贵且耗时的集成。生产包含 CI/CD 软件的容器被称为容器化。容器化是一种成熟的商业实践，受到了许多政府和商业软件包的支持，这些软件包能够在操作环境中构建、测试和评估以及部署容器。这种灵活性显著提高了在更大系统（如 ABMS）上下文中对特定功能进行升级的信心，同时减少了对整体任务要求的风险。

在空军部（DAF）内部，开源的 Kubernetes¹已被广泛采用，以避免供应商锁定并提供弹性、安全性、适应性、自动化、自动扩展和抽象层。它已成功应用于 F-16 战斗机和 U-2 侦察机上，以满足按需先进系统和软件需求。据前 DAF 首席软件官（CSO）称，在 U-2 试验的情况下，“U-2 传统计算机系统与现代 Kubernetes 软件的成功结合是现有空军武器系统上软件容器化发展的一个关键里程碑。”⁴⁴

为了实现这些实验，DAF 必须创建一个便携的技术堆栈，包括（1）Cloud One 基础设施层，提供稳定和安全的通用开发、测试和生产环境；（2）Platform One，提供软件企业服务和强化的容器、CI/CD 选项，以及提供集成零信任（ZT）安全和启用微服务架构的 Istio²服务网格层；⁴⁶ 以及（3）应用层，允许开发团队轻松构建可重用的模块化软件或微服务，这些服务利用强化的容器在团队间使用。⁴⁷ 图 2.4 展示了这一技术堆栈的各层。

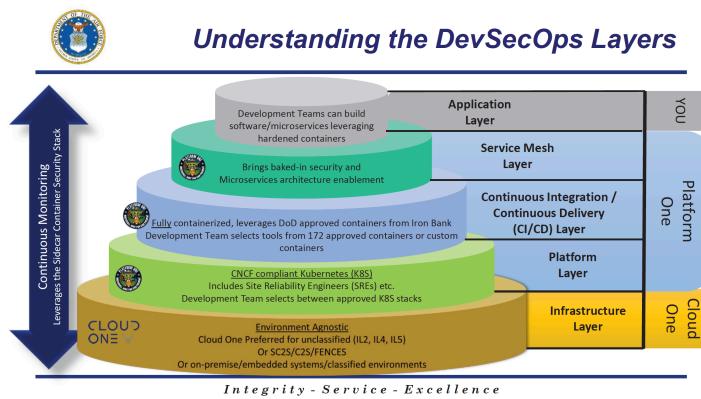


Figure 2.4: 了解 DevSecOps 层次。来源：美国空军部首席软件官。N. Chaillan, 2020 年，“DoD 企业 DevSecOps 计划和平台一号”，美国空军部首席软件官，<https://software.af.mil/dsop/documents/>, 9 月 15 日。

更具体地说，对于 ABMS，Kubernetes 被用于在开发中自动化安全和数据分析。在 2021 年 2 月于德国拉姆施泰因空军基地进行的多国演练中，成功展示了结合 Kubernetes 集群、DevSecOps（开发、安全和操作）、在边缘部署 AI/ML 应用以及将开发代码从非机密网络传输到机密网络的能力。⁴⁸ 其目标是使用 Kubernetes 通过持续扫描 ABMS 内的异常和潜在破坏点来实现安全自动化。一旦通过 Kubernetes 检测到异常或破坏点，它们可以被集成到容器中并像任何其他功能升级一样部署。这消除了单独且独特的安全缓解过程的需求，并将系统安全要求完全整合到 DevSecOps 开发过程中。此外，这种方法将减少手动测试的需求，并最小化人为错误的可能性。

发现 6：容器化和 Kubernetes 是成熟的开源编排系统，用于在 CI/CD 环境中实现和保障敏捷开发。

建议 8：空军部首席软件官、空军部首席架构师办公室和空军部快速能力办公室应协调合作，扩大容器化和 Kubernetes 的使用，以实现持续的高级战斗管理系统开发，并检测和缓解安全漏洞。

¹Kubernetes 是一个便携的、可扩展的开源平台，用于管理容器化的工作负载和服务，促进声明式配置和自动化。参见美国空军部首席软件官办公室，“Kubernetes”，<https://software.af.mil/training/kubernetes/>。容器和 Kubernetes 的关键区别在于，容器旨在一次编码、随处运行，而 Kubernetes 提供了从单个控制平面编排和管理所有容器资源的潜力。参见微软，“Kubernetes vs. Docker”，<https://azure.microsoft.com/en-us/topic/kubernetes-vs-docker/>。

²Istio 是一个服务网格——一种现代化的服务网络层，提供一种透明且与语言无关的方式，灵活且轻松地自动化应用网络功能。参见谷歌云，“What Is Istio？”<https://cloud.google.com/learn/what-is-istio>。

2.2 软件考虑事项

ABMS 需要复杂集成各种独立演进、定制化的武器专用软件元素。它们共同构建一个高度分布式的感知、及时聚合和分析功能框架，以提供增强的决策能力，实现灵活和有弹性的战斗和防御。具有异构物理、技术和时间特征的共享信息必须标准化，或至少可转换和互操作，以促进及时和准确的决策。还需要协调和分布的执行，即武器效果的应用，以产生连贯的致命效果。此外，遗留系统必须以连贯、分阶段和成本效益高的方式集成。

支持这样一个集成和多层次的指挥控制框架的软件可能会随着新的操作挑战和对抗策略的变化而演变。这要求软件具有敏捷性、适应性、可修改性和安全性。严格的测试以评估、验证和改进软件性能并降低开发成本也至关重要。

2.2.1 应用软件和 DevSecOps

现代应用程序需要最新的开发、安全和操作（DevSecOps）⁴⁹ 流程，包括自动化安全工具以及自动化测试和部署。手持数字设备的快速进步（集成了通信、计算功能和通过生物识别等手段加密的存储）引发了创新工具的爆炸性增长，这些工具具有低门槛，可以将洞察转化为原型，并在战术边缘处理数据。通过 DevSecOps 方法，收集这些可行的想法并将其转化为可用产品是可能的，在这种方法中，创新者、开发人员、集成商和最终用户在频繁的周期中相互作用，互相促进。

应用环境的目标是创建一个基于模型的软件工程系统，逐步结合不断演进的创新、采购和维持过程；提供从已部署代码反馈的遥测数据来更新模型；自动生成代码；提供自动化测试和集成；并部署代码。任何在开发过程中没有深入人类参与的自动化代码开发可能会导致操作范围有限和增加的漏洞。知识工程工具确实存在，但必须纳入软件开发过程中。

ABMS 的复杂性和不断演变的性质需要一种开放、敏捷、安全和适应性强的软件开发方法。空军部的首席软件官（CSO）已采取措施，将部门从传统的瀑布式软件开发方法（通常需要 3 到 10 年执行）转向更敏捷和安全的软件开发方法。在与国防部采购和维持副部长办公室（OUSD(A&S)）、国防部首席信息官（CIO）、国防信息系统局（DISA）以及其他军种的协调下，空军部 CSO 实施了国防部企业 DevSecOps 计划（DSOP），该计划详细说明了“结合 Kubernetes、Istio、knative⁵⁰，以及一个内部开发的用于‘强化’容器的规范，具有一套严格的安全要求，作为全军默认的软件开发平台。”⁵¹ 图 2.5 描述了这一计划。



What is the DoD Enterprise DevSecOps Initiative?

Joint Program with OUSD(A&S), DoD CIO, U.S. Air Force, DISA and the Military Services.

Technology:

- Avoid vendor lock-in at the Infrastructure and Platform Layer by leveraging FOSS with Kubernetes and OCI containers,
- Creating the DoD Centralized Artifacts Repository (DCAR) of hardened and centrally accredited containers: selecting, certifying, and securing best of breed development tools and software capabilities (over 170+ containers) - <https://dcar.dsop.dsop.mil> and <https://dcar.dsop.io>
- Baked-in Zero Trust Security with our Sidecar Container Security Stack (SCSS) leveraging behavior detection, zero trust down to the container/function level.
- Leveraging a Scalable Microservices Architecture with Service Mesh/API Gateway and baked-in security (Istio)
- Leveraging KNative to avoid lock-in to Cloud provider Serverless stacks
- Bringing Enterprise IT Capabilities with Cloud One and Platform One – Cloud and DevSecOps as Managed Services capabilities, on-boarding and support!
- Standardizing metrics and define acceptable thresholds for DoD-wide continuous Authority to Operate
- Massive Scale Training with Self Learning Capabilities (train over 100K people within a year) and bring state of the art DevSecOps curriculum
- Creating new Agile contracting language to enable and incentivize the use of DevSecOps

Integrity - Service - Excellence

Figure 2.5: DoD 企业 DevSecOps。来源：美国空军首席软件官 N. Chaillan, 2020, “DoD 企业 DevSecOps 倡议和平台一”，美国空军首席软件官，<https://software.af.mil/dsop/documents/>, 9 月 15 日。

通过转向这种企业方法，DAF（美国空军）能够在现有或新环境中（包括机密、离线和云环境）在几天内而非几年内部署强化的软件工厂；建立多个具有各种选项的 DevSecOps 流水线；为武器、C4ISR（指挥、控制、通信、计算机、情报、监视和侦察）和业务系统提供快速原型设计和更快的部署；从最终用户和作战人员处获得持续的学习和反馈；在几分钟内帮助进行安全修复；生成一个整体且集成的网络安全堆栈，以允许对所有资产、软件安全状态和基础设施代码的完全可见性；并通过使用微服务架构促进微服务的采用。⁵² 其目标是通过支持 ABMS（先进战斗管理系统）的 CloudOne 基础设施建立一个拥有多个创新中心的软件生态系统。⁵³ 图 2.6 展示了构成当前 DAF 软件生态系统的这些创新中心的位置。

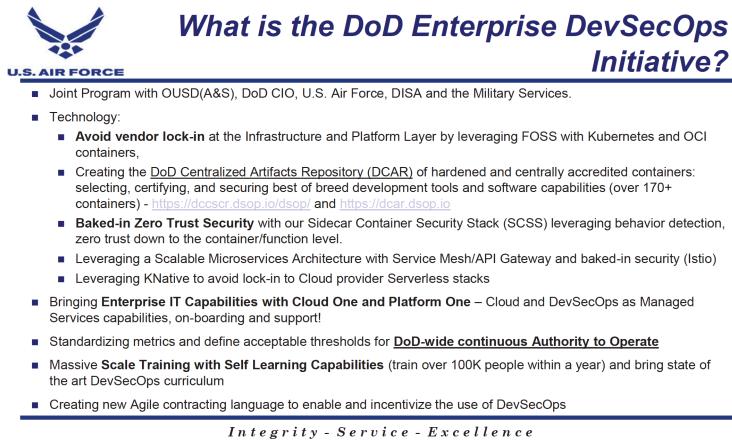


Figure 2.6: 软件生态系统。来源：美国空军首席软件官 N. Chaillan, 2020, “DoD 企业 DevSecOps 倡议和平台一”，美国空军首席软件官，<https://software.af.mil/dsop/documents/>, 9 月 15 日。

位于内利斯空军基地的影子作战中心（ShOC-N）被指定为负责创建和测试 ABMS 信息技术应用的主要机构。⁵⁴ DevSecOps 的使用对于 ABMS 的发展至关重要，它将软件开发人员、操作人员和最终用户汇集在一起，在“虚拟和物理信息收集和意义构建的游乐场”中使用数据。⁵⁵ 这种整合将使操作上相关且网络安全的软件能够迅速交付给部队。2021 年 6 月，ShOC-N 举办了 JADC2 21-1（联合全域指挥与控制 21-1）、J6 运动，召集了所有领域的专家并连接了 17 个不同的 DoD 战斗实验室，以交换操作上相关的数据。通过使用 DevSecOps 和实验性软件应用程序的组合，⁵⁶ 开发人员能够帮助“作战人员可视化并理解网络域，并获得相对于对手的决策优势……并从所有分支的角度更好地理解网络域。”⁵⁷ 通过利用新兴和实验技术为软件工程师提供实时反馈，使他们能够进行快速调整和改进，缩短了开发时间。

下一步是集成 AI/ML（人工智能/机器学习），以实现大数据处理和预测分析。根据美国北方司令部（USNORTHCOM）司令的说法，确保在未来全域战场上取得胜利的关键在于预测分析。“我们认为 JADC2（联合全域指挥与控制）对于我们防御本土的方式绝对核心……我认为会带来如此巨大变革的是我们真正利用预测分析并为未来决策提供信息的能力。”⁵⁸ 更具体地说，在 ABMS 中，预测分析将使开发人员能够“获得关于信息流向、数据损坏位置、信息传输困难以及这些问题如何影响决策的数字反馈。”⁵⁹

发现 7：在现有软件工厂中使用 DevSecOps 对于创建部分 ABMS 开发的 CI/CD（持续集成/持续交付）环境是有效的。

建议 9：美国空军首席架构师办公室和美国空军快速能力办公室应采用开发、安全和运营作为通用开发环境，通过容器化和持续集成/持续交付在整个先进战斗管理系统中应用。

2.2.2 数据权利

在国防采购中，政府倾向于向行业要求访问所有数据权利，包括技术数据和计算机软件数据。技术数据包括“任何具有科学或技术性质的记录信息（例如，产品设计或维护数据、计算机数据库和计算机软件文档）。”⁶⁰ 计算机软件包括“可执行代码、源代码、代码清单、设计细节、流程、流程图以及能够使软件被复制、重现或重新编译的相关材料。”⁶¹ 行业通常保留技术数据和计算机软件的所有权，但通过三种类别之一的许可安排将这些数据的使用权传达给政府机构：无限制权利、有限权利（技术数据）或受限权利（计算机软件），以及政府用途权利。⁶²

对于 ABMS，其架构由硬件、软件、旧系统和其他 C2（指挥与控制）基础设施的集合组成，拥有或访问数据权利可能不可行也不可持续。相反，应集中精力拥有连接这些不同组件的接口权利（而非所有知识产权）。⁶³ 这对使用开放系统架构（OSA）的系统尤为重要。“从数据权利的角度来看，模块化/开放系统方法的一个主要好处是性能和接口信息应符合 DFARS（国防联邦采购条例补充）的形式、适配和功能数据标准，从而没有政府数据权利限制。”⁶⁴

通过获取和维护性能和接口要求，政府能够利用它们从多个供应商处采购和支持模块化解决方案。这将反过来减少对单一来源采购的依赖，或昂贵的私人开发技术或计算机软件的许可权利采购。“虽然任何武器系统都可能从 OSA 方法中受益，但预期包含专有技术、频繁技术更新或有多个来源可用的子系统特别适合。另一个考虑模块化/开放系统方法的原因是，如果预期子系统具有数据权利限制，并且不太可能通过获取额外的数据权利来减轻这些限制。”⁶⁵

建议 10：对于具有强大接口规范的模块化开放系统设计，美国空军快速能力办公室应获取性能和接口要求，而不是所有知识产权。

2.3 安全性

2.3.1 网络可靠性、弹性和容错性

ABMS（先进战斗管理系统）在任何交战中的成功都依赖于通信基础设施。此基础设施的大部分由数据网络组成，这些网络负责将关键数据从传感器传输到计算、决策、执行和数据存储节点。作为 ABMS 的关键元素，始终监控整个网络基础设施的实时状态和弹性非常重要。如果网络性能受到任何干扰或降级，冗余和弹性系统必须自动重新路由和重建网络通信，以保持 ABMS 的能力。能够在很少或没有通信连接或带宽的情况下运行也很重要，应作为 ABMS 总体安全设计的一部分进行考虑。

网络的定义性能通常围绕带宽和延迟的实时度量进行结构化——无论是在网络的单个点对点链路内还是在端到端通信中。带宽和延迟的具体可接受指标在 ABMS 能力的战术状态下定义。在较低级别的交战中，带宽和延迟的某些降级可能是可以接受的。然而，在更高级别的交战中，网络攻击更有可能发生，此时必须提高带宽并减少延迟，或至少保持不变。因此，网络何时不能再支持优先流量的容量和及时性是一个动态问题。它还必须反映其服务于整体 ABMS 目标的程度，即使 DAF（美国空军）能够在对手的观察-判断-决定-行动（OODA）循环内操作。

网络最低性能要求的动态特性为使用冗余和弹性通信结构带来了新的挑战。虽然最低性能是动态的，但它不是随意的，而是基于 ABMS 在交战中的 C2（指挥与控制）要求预先定义的。一旦定义，ABMS 能力将能够自动调整网络能力（例如，使用软件定义网络和网络功能虚拟化）以在任何时候保持最低性能配置文件。

为每个操作场景定义最低性能特征将定义网络中断的方式以及每个场景的应急措施。需要注意的是，网络故障的来源可能是对手强加的，对手也可能预见到弹性和冗余能力。因此，任何应急措施必须现实地应对威胁模型，对手将直接攻击启用 ABMS 所需的网络和通信基础设施。

作为 JADC2 和国家 NC3 能力的贡献者，安全性、可靠性和弹性应成为 ABMS 的基本属性。众议院军事委员会主席 Adam Smith (D-WA) 代表表示，“我们必须能够保护我们的指挥和控制系统，理想情况下，我们必须能够建立一个系统，使我们的对手系统更容易受到攻击。这确实需要成为重点。”¹⁰ 参谋长联席会议副主席补充道，“重要的是要认识到 JADC2 和 NC3 是相互交织的，因为…NC3 将在 JADC2 的显著元素中运行。因此，NC3 必须通知 JADC2，JADC2 也必须通知 NC3。你必须有来回的接口，这是公认的。”⁷ 作为一个能够通过 crossdomainONE 桥接不同安全分类的 C2 系统，⁶⁸ ABMS 将需要提供安全、可靠和弹性的接口来连接 JADC2 和 NC3。这将需要美国战略司令部 (USSTRATCOM) 的参与。

如第一章详细描述，目前的空中作战中心 (AOC) 模块是基于现已过时的技术设计的——包括用于网络安全的技术。逐步开发和演变的 AOC 组件保护措施导致了一个由各种结构、流程和完整性构成的拼凑而成的系统。此外，当前 AOC 的设计和开发是在以前的威胁环境背景下执行的——与操作员今天遇到的环境大不相同。今天和未来的战场是高度复杂的，并将在战略、战术和操作级别上涉及所有领域。最难以预见和准备的是在和平与战争之间的“灰色地带”进行的竞争。⁶⁹ 全域战争的不可预测性和复杂性要求 ABMS 所支持的操作环境具备保密性、完整性和可用性。

为实现这一目标，应从多方面方法开发一个安全工程结构及相关实施策略，考虑操作、技术和风险评估（基于对威胁环境和技术限制的现实评估）等角度。安全结构应识别漏洞并支持以下内容：

- 安全性：ABMS 必须提供安全且准确的数据，并获得所有领域操作员的信任；
- 可靠性：ABMS 的能力必须按预期执行并在需要时可用；
- 弹性：ABMS 必须能够在反进入和降级环境中运行，并能根据需要迅速重建。

最终，安全工程必须根据当前的操作和技术基线进行设计、实施和评估。它不能仅仅是技术评估。

发现 8：ABMS 及其使用的作战部队必须具有应对技术故障和限制以及敌对攻击的弹性。

发现 9：ABMS 的带宽和延迟能力需要根据变化的操作条件和需求进行调整。例如，在高层次的交战中，网络攻击更有可能发生，此时必须提高带宽并减少延迟，或至少维持带宽或支持关键功能，在带宽可用性受到挑战时，相关数据传输需要优先处理。

建议 11：美国空军首席架构师办公室和美国空军快速能力办公室应在先进战斗管理系统架构中设计弹性，并指定所需性能的动态标准。

2.3.2 多级安全性

多级安全性 (Multi-Level Security, MLS) 指的是“处理具有不同分类和类别的信息，同时允许具有不同安全许可的用户访问，并拒绝未经授权的用户访问。”⁷⁰ 这种系统能够使各个平台处理不同安全级别的信息，并在适当情况下在这些级别之间移动数据。MLS 的优点是能够存储和共享混合分类的数据，并为拥有适当授权的人员提供对多种分类数据的安全访问。

ABMS 通过 CrossDomainONE 平台和由空军研究实验室 (AFRL) 建立的 ABMS DeviceOne SecureView (ADSV) 引入了这种 MLS 方法。⁷² CrossDomainONE 使数据能够在分类级别之间移动，而 ADSV 通过连接传感器和射手，支持 ABMS 和 JADC2，允许数据传输和/或访问多域和跨域数据。图 2.7 总结了 ADSV 的关键特性。

委员会认为 CrossDomainONE 和 ADSV 是增强 ABMS MLS 保护的重要初步步骤。然而，ADSV 使用虚拟机监控程序 (hypervisor) 进行安全增强，可能会使 ABMS 暴露于潜在的漏洞和风险中。一个关键的下一步是自动化数据传输和集成。传感器和平台的数据，特别是高度机密的情报和传感器数据，通常很少进行元标记 (标签)，以允许 MLS 系统有效评估机器对机器的数据传输和集成。为了弥补这一技术差距，各个平台和系统应能够在不同的分类级别上运行，以确保与在 JADC2 框架下运行的其他服务和多国合作伙伴及盟友的兼容性。在 MLS 设计中，还应解决对高度机密信息的子集进行净化以释放给操作用户的问题。

Capability
<ul style="list-style-type: none">Supports NIPRNet, SIPRNet, and Coalition access on a single PC or laptopIntuitive user interface that requires minimal training for end usersEnables secure mobility solutions for Executive Communication and traveling personnelSeamlessly supports high performance and high-bandwidth applications
Security
<ul style="list-style-type: none">Type I bare-metal hypervisor enhances the cyber defense posture of government workstationsMinimizes Type I encryptors by integrating support for NSA's Commercial Solutions for Classified (CSfC)Ensures 100% Trusted Boot and Secure Isolation in the hardwareHas received highest MILS evaluation to date against NIST 800-53 Criteria
Flexibility
<ul style="list-style-type: none">Supports either Standard Desktop Configuration (SDC) or Thin Virtual Desktop Infrastructure (VDI)Enables rapid provisioning, management, and re-configuration of workstationsGovernment off-the-shelf (GOTS) solution based on OpenXT which meets DoD's open-source requirement

Figure 2.7: ABMS DeviceOne SecureView®。来源：空军研究实验室信息局，SecureView 跨域访问解决方案。

- **能力**
 - 支持在单个 PC 或笔记本电脑上访问 NIPRNet、SIPRNet 和联合网络
 - 直观的用户界面，最终用户只需进行最少的培训
 - 为行政通信和出差人员提供安全的移动解决方案
 - 无缝支持高性能和高带宽应用
- **安全性**
 - 第一类裸机虚拟机监控程序增强了政府工作站的网络防御态势
 - 通过集成支持 NSA 的机密商业解决方案 (CSfC)，最大限度地减少第一类加密器
 - 确保硬件中的 100% 可信启动和安全隔离
 - 已根据 NIST 800-53 标准获得最高的 MILS 评估
- **灵活性**
 - 支持标准桌面配置 (SDC) 或虚拟桌面基础设施 (VDI)
 - 实现工作站的快速供应、管理和重新配置
 - 基于 OpenXT 的政府现成解决方案 (GOTS)，符合 DoD 的开源要求

2.3.3 网络安全与零信任

安全性对 ABMS 至关重要。因此，数据的存储、处理和通信必须同样安全可靠，通信必须在整个企业范围内实现和及时完成。为所有 ABMS 及其支持组件设计整体的网络安全架构至关重要；零碎的开发只会导致安全漏洞和缝隙，这些将（并且会）被我们的对手利用。根据第 16 空军/空军网络司令部（空军信息战司令部）副司令的说法，“我们真正开展 JADC2 的唯一方法是通过一个防御性的、有弹性的、完全有能力的网络作战通信网络……我们不仅需要启用它、设计它和操作它，我们还必须防御它，因为敌人会试图夺走它。”⁷³

为了应对这一安全挑战，ABMS 开发人员正在逐步采用零信任 (ZT) 架构，这种架构在不依赖于服务所在网络基础设施位置的情况下，在服务之间提供经过认证和授权的访问。⁷⁴ ZT 不是一组特定的技术，而是一种架构构造，要求在分布式系统中的各个节点之间进行所有交互的认证和授权。最常见的，ZT 涉及去边界化 (deperimeterization)，即通过加密、安全计算机协议、安全计算机系统和数据级认证的混合来保护组织的系统和数据的能力。去边界化减少或消除了在企业网络内操作的需求，通过提供用户与分布式服务（如数据、专业计算、传感器和位置服务）之间的访问。⁷⁵

对于 ABMS，ZT 被用于 deviceONE，该系统在系统的每一层都进行凭证检查。对于 DAF 首席架构师和空军快速能力办公室来说，将 ZT 和其他网络安全保护扩展到所有 ABMS 能力中，以确保最大限度地防范网络漏洞是非常重要的。

虽然 ZT 概念已经存在了一段时间，但最近在支持技术方面的改进使得通过多因素认证 (MFA)、授权服务和其他安全能力连接各种服务成为可能，从而实现了 ZT 的广泛应用。ZT 在分散的平台和用户之间提供经过认证和授权的访问，以在动态网络环境中实现指挥、控制和通信。它也常用于云计算环境，这适用于 ABMS 的军事物联网，从不可信网络环境中的端点到云计算和数据环境提供可信访问。

然而，不仅为 ABMS，而且为整个 DoD JADC2 企业采用 ZT 架构可能会充满挑战。能够支持整个 DoD 范围内 C4ISR 以支持广泛军事行动的 ZT 技术尚未被证明足够强大。此外，需要在 JWC 之间协调的各种能力和要求需要创建一个能够保持最新并连接所有用户、数据和技术平台的授权服务。即将出台的 JADC2 实施战略确实鼓励更加关注 ZT，但在解决跨越 DoD 企业的不连贯和断开的用户和系统采用 ZT 的技术和后勤挑战方面还不够。该战略也没有解决在 JADC 中访问和操作系统所需的具体权限，这是人机通信中的关键。因此，虽

然 ZT 应仍是 ABMS 的一个组成部分，但整体 ABMS（和 JADC2）安全架构将需要在平台和人机接口（HCI）之间定义明确的认证和授权要求。

另一个考虑因素是为具有不同和不规则漏洞程度的旧系统建立网络安全，因为它们的硬件、软件和操作技术已过时。这些系统通常与围绕访问的安全功能（包括 MFA、单点登录和基于角色的访问）不兼容。它们也缺乏保护数字数据机密性所需的足够加密技术。通过 ABMS 框架与这些旧系统建立连接至少需要进行漏洞扫描以识别和解决所有漏洞，采用网络安全控制措施对与 ABMS 组件联网的系统进行保护，并更新最新的系统补丁以尽量减少暴露。⁷⁶

需要认识到，尽管 ZT 提供了一层安全保护，但整个 ABMS 架构需要一个全面的网络安全计划。⁷⁷ 这需要包括进攻和防御计划，包括对 ABMS 的网络防御进行红队测试，以确保其弹性，防止敌对渗透和攻击。应利用空军的任务防御团队，这些专门的防御网络团队负责保护空军的关键任务和设施。⁷⁸ 此外，国会最近指示和授权防御网络人员在美国网络之外操作。该措施将使美国网络司令部（USCYBERCOM）通过其“前进狩猎”任务，更好地了解对手使用的恶意软件类型及其可能针对美国网络计划的行动类型。⁷⁹ 根据 USCYBERCOM 指挥官的说法，“我们不能等到网络攻击影响我们的军事网络。我们学到了保护我们的军事网络需要在我们的军事网络之外执行操作。威胁在演变，我们也在演变以应对它。”⁸⁰

发现 10：进攻和防御网络安全保护对 ABMS 至关重要，必须从一开始将全面无缝地整合到整个系统架构中。以零碎方式或事后考虑的方式处理网络安全只会产生漏洞，而这些漏洞将被恶意行为者利用。

发现 11：ZT 前景可期，但目前尚不够成熟，无法成为像 ABMS 这样的军事 C2 系统中的唯一安全保护措施。

建议 12：联合参谋部 J6、美国空军部及更广泛的美国国防部社区应为联合全域指挥与控制（JADC2）和先进战斗管理系统制定并实施一个强大的全企业进攻和防御网络安全战略。安全是一个基本要求，必须从一开始就设计并完全整合到所有 JADC2 支持系统的架构中。

建议 13：空军快速能力办公室应随着技术的成熟分阶段应用零信任（ZT），并整合 ZT 服务，包括在整个先进战斗管理系统中使用多因素认证。

建议 14：除了采用零信任，空军快速能力办公室还应利用最成熟的网络安全实践和能力，包括多因素认证、身份、凭证和访问管理、加密、渗透测试、管理检测服务、行为监控应用等。

建议 15：空军快速能力办公室（DAF RCO）应利用空军的任务防御团队对先进战斗管理系统的网络防御进行红队测试，以防备恶意行为者的攻击。根据这些红队演习，DAF RCO 应通过增强网络防御来解决漏洞。

建议 16：空军首席架构师办公室和空军快速能力办公室应与美国网络司令部合作，解决物联网防御和“美国网络司令部技术挑战问题集”文件中指出的其他网络漏洞和利用。

2.4 测试与建模

2.4.1 测试与评估

风险降低是测试与评估 (T&E) 的主要目标。通过评估系统性能与战斗人员和操作员需求的匹配程度，可以早期发现和缓解系统漏洞、缺陷和性能问题。作为更广泛的系统工程过程 (SEP) 的一部分，委员会认为 T&E 是必不可少的，应该在 ABMS 开发和部署周期的整个过程中进行，特别是在引入新产品和服务时。

根据 DAF 首席架构师的说法，ABMS 设计为随着新技术的出现而不断演变。因此，开发测试被集成到更广泛的 DevSecOps 过程中，而操作测试则通过大规模的试验和演习进行。⁸¹ ABMS 的首次实地测试于 2019 年 12 月 16 日至 18 日进行，涉及空军、海军和陆军在国土防御情景下操作。这次试验测试了新的软件、通信设备和用于在战斗机、驱逐舰、地面部队和指挥中心之间传输时间敏感信息的网状网络。“今天的演示是我们首次展示全军物联网连接。云计算、网状网络和软件定义系统是演示的亮点，所有这些都是以商业互联网速度开发的……目标是快速行动和快速交付。”⁸²

随后，2020 年 8 月 31 日至 9 月 3 日（第二次试验，重点是分类和非分类通信以及测试 28 条 ABMS “ONE” 产品线，通过安全数据网络连接传感器与武器）；⁸³ 2020 年 9 月 15 日至 9 月 25 日（第三次试验，测试将非传统战斗管理 C2 节点，如 KC46 加油机，与 ABMS 集成，以提供无缝的检测、跟踪和跨域作战能力）；⁸⁴ 以及 2021 年 2 月下旬（第四次试验，测试并观察联合部队、盟友和多国合作伙伴的能力，跨多个网络进行指挥和控制）。⁸⁵ 第五次试验原计划在太平洋战区进行，但由于预算限制于 2021 年 3 月取消。⁸⁶

此外，空军和陆军领导人于 2020 年 9 月签署了一项为期两年的跨军种协议，共同建立数据共享和服务接口的共同标准，以确保所有新通信设备、网络和人工智能的兼容性。该协议还影响联合部队的训练、演习和演示。⁸⁷

尽管这些活动值得注意，但最近对 ABMS 预算的削减正在阻碍 DAF 继续进行大规模实地演习和能力演示的能力。此外，空军部长已指示更多关注实现“真正的”操作改进，而不是原型和实验。⁸⁸ 因此，委员会认为 ABMS 可能需要通过模型驱动系统工程 (MBSE)、建模和仿真 (M&S) 以及数字孪生的组合来重新调整未来的测试。

发现 12：开发测试应集中于检测和纠正系统设计或实现中的错误；操作测试应集中于系统满足用户需求的能力。开发测试和操作测试都需要通过数字化和 MBSE、M&S 和数字孪生技术不断执行和评估，以在日益复杂的威胁环境中保持 DAF 的技术优势。

2.4.2 模型驱动系统工程

2016 年，国防部引入了“系统工程数字工程基础”以鼓励在数字生态系统中使用 MBSE 实践。⁸⁹ MBSE 被定义为“在概念设计阶段开始并贯穿开发和后续生命周期阶段，支持系统需求、设计、分析、验证和确认活动的建模正式化应用。”⁹⁰ 简而言之，MBSE 用于支持与复杂系统开发相关的需求、设计、分析、验证和确认。⁹¹ 使用这种方法的优点是降低开发风险、改善系统性能、将严谨性和精确性制度化到设计过程中并增强知识转移。与主要关注设计文档（文档密集型系统工程）的传统系统工程方法不同，MBSE 则专注于适合数字建模环境的复杂系统，如 ABMS。

作为一种多学科方法，MBSE 将建模、系统思维和系统工程结合到一个整体框架中。它涵盖了四个基本的系统工程领域，包括需求/能力、行为、架构/结构以及验证和确认。如果

应用于 ABMS，MBSE 将使 DAF 工程团队能够更好地理解设计变更的影响；传达设计意图；验证、变更、接受和维持功能能力；并在系统构建之前分析系统设计。此外，随着该方法的不断成熟，MBSE 可能会超越基本的工程模型，支持跨域模型集成和复杂的预测和基于效果的建模。⁹²

在 DAF 内部，一直在大力推动向企业采用数字工程（DE）方向发展，MBSE 是其中的一个子集。⁹³ 前空军部负责采办、技术和物流的助理部长（SAF/AQ）鼓励应用数字工程，通过“拥有技术栈”来实现对技术基线的所有权。⁹⁴ 其目标是：

- 在控制生命周期成本的同时实现主导能力；
- 增加原型和实验的使用；
- 改善需求定义；
- 增强 DAF 的有机工程能力；
- 提高 DAF 领导人理解和缓解技术风险的能力。⁹⁵

前 SAF/AQ 表示，数字工程使 DAF 能够采用以计算机为中心的设计和测试，以加快原型制作并降低新系统（如下一代空中优势（NGAD）战斗机）的成本。⁹⁶ 数字工程还被用于地基战略威慑系统（GBSD），其设计基于情报评估和技术预测，并在空间与导弹系统司令部的受保护反干扰战术卫星通信（PATS）系统家族中利用静态和动态模型进行测试、集成和设计。⁹⁷

此外，2021 年 6 月，DAF 在空军装备司令部（AFMC）成立了数字化转型办公室（DTO），负责开发数字治理结构并管理当前和新的数字化转型活动。DTO 主任还兼任 DAF 数字工程企业办公室主任，负责：

- 提供跨系统生命周期的系统需求可追溯性；
- 创建一个从概念开发到部署，促进创新、实验和演示的环境；
- 实现快速原型制作，以更快地交付能力并快速响应不断变化的威胁和需求；
- 促进协作以改进系统集成以满足任务需求；
- 开发一个平台和流程，以支持 DAF 在多个功能领域的现代化努力，包括敏捷开发和模块化开放系统架构（MOSA）。⁹⁸

整体上，DTO 和数字工程企业办公室旨在加速 DAF 企业的数字化现代化和转型。⁹⁹

发现 13： MBSE 和数字工程方法降低了开发风险并改善了系统设计和性能。

建议 17：空军首席架构师办公室和空军快速能力办公室应与空军数字工程企业办公室合作，将模型驱动系统工程（MBSE）方法应用于先进战斗管理系统的工程和维持活动，并使 MBSE 成为操作需求与开发团队之间的桥梁。

2.4.3 M&S 和 VV&A

建模是生成系统结构和工作表示的过程；仿真是模型的运行。¹⁰⁰ 结合起来，M&S 是系统工程中用于决策的信息工具。验证、确认和鉴定（VV&A）指的是三个相互关联但独特的过程，它们收集和评估证据，以确定模型或仿真的能力、准确性、正确性和可用性是否足以支持其预期用途。¹⁰¹ 与 MBSE 结合，M&S 和 VV&A 为贸易空间分析提供了选项，以支持设计决策并在系统开发过程中量化性能。与 T&E 叠加，M&S 和 VV&A 使系统工程师有机会自信地评估设计实施是否符合预期。¹⁰²

为了支持这些过程，DAF 在空军生命周期管理中心的架构和集成局（位于赖特-帕特森空军基地）建立了通用仿真训练环境（CSTE）。CSTE 的角色是创建一个协作环境，使训练系统和模拟器能够更好地连接，以支持操作员和战斗人员。此外，DAF 正在努力通过 2016 年建立的模拟器通用架构要求和标准（SCARS）来标准化训练平台要求，该标准实施模块化开放系统架构（MOSA）方法和一套通用标准。¹⁰³ 这些活动的目的是持续快速更新技术，同时支持 ABMS 和 JADC2。

2.4.4 数字孪生

数字孪生是“跨其生命周期的对象或系统的虚拟表示，基于实时数据更新，并使用仿真、机器学习和推理来辅助决策。”¹⁰⁴ 模型的类别包括系统模型、产品模型和过程模型。数字孪生和数字线程在基于模型的环境中将这些模型连接在一起。¹⁰⁵ 作为一种工程工具，数字孪生提供了关于系统或连接传感器未来性能的见解。

在 DAF 内部，多个项目和系统已经在其工程计划中采用了数字孪生。例如，PATS 系统家族使用数字孪生进行早期系统建模以降低风险，并作为系统集成和操作支持的构建模型。¹⁰⁶ 数字孪生还用于空军新型高级飞机教练机 eT-7 Red Hawk 的设计和初步测试，设计、建造和试飞都在首架教练机制造和交付之前进行。¹⁰⁷ 类似地，数字孪生被用于评估 B-52 发动机更换竞标方案，而无需进行飞行测试。¹⁰⁸ DAF 还宣布计划为 F-16 创建数字孪生，以改进其现有机队的维持和现代化。“目标是创建飞机的全尺寸 3D 模型……以帮助解决未来零件报废问题，并减轻供应链风险……[以减少对] 传统制造来源和工艺的依赖。”¹¹⁰

对于 ABMS，空军研究实验室（AFRL）的弹药局正在利用高性能计算系统和 AI/ML 辅助的数字孪生在数字企业 WeaponONE（W1）计划中，从飞行中的武器收集数据，将这些信息与战场数据结合，并通过 ABMS 无缝传输回数字孪生。¹¹¹ 目标是提高数字模型的准确性和实用性。AFRL 在 2021 年 1 月通过 Gray Wolf 原型展示了这一能力。Gray Wolf 是一种实验性巡航导弹，旨在针对敌方防空系统进行集群部署。在演习中，Gray Wolf 执行了 24 小时的空中任务指令，使导弹能够协作。W1 收集了飞行中的数据，并与战场信息进行交叉参考，然后使用 ABMS 网络安全地将信息传输回数字孪生进行分析。“全方位的、数字的、敏捷的、开放的生态系统计划将政府、行业和学术界的最佳实践和标准结合起来，并应用于武器开发。”¹¹³ 今后，W1 计划将进一步推进其数字孪生原型，以实现与其物理对应物的双向数据交换。

为了鼓励在数字孪生的应用中竞争，AFRL 正在建立一个在线斗兽场，商业供应商的系统可以在这里竞争。根据 AFRL 弹药局负责人的说法，“每个供应商可以提交一个提议的武器平台的数字孪生，以在‘某种角斗士对决……特定技术领域’中进行评估。”¹¹⁴ 供应商被指示使用政府的参考架构构建其数字孪生，该架构提供标准并定义数字模型需要使用的接口。

发现 14： DAF 正在全力推进在遗留平台和新兴系统中使用数字孪生。

建议 18： 基于现有的数字工程和建模与仿真活动，空军首席架构师办公室和空军快速能力办公室应扩大数字孪生在先进战斗管理系统开发中的使用，特别是在引入新能力和技术时。

2.5 联合任务指挥中心

一个复杂架构和系统集成的例子是 2010 年由前国防部采购、技术和物流副部长、前国防部采购、技术和物流副部长以及前空军 SAE 发起的系统家族 (FOS)。将大量现有和新开发的程序集合在 FOS 中，五个主要元素结合了新技术和主要程序元素的综合。

这一经过验证的过程导致认识到有强烈需求将指挥、控制、通信和情报 (C3I) 集成到不同的程序组件中。基于这一需求，在 DAF RCO 的主持下，一个政府和行业团队成功建立了一个支持 ABMS 元素的原型能力。该原型，联合任务指挥中心 (CMCC)，是一个软件、硬件和人机界面，能够在复杂的 C2 框架内指挥、任务和组合多个任务，包括大量武器系统。其重点是提供互操作性、任务管理、计划和任务分配、来自多个信息源的数据融合、地理位置状态和态势感知、产品管理和分发以及在安全 C2 环境中的机器对机器数据交换。¹¹⁵ 它是基于一个已建立的开放架构框架开发的，使用了开放任务系统/通用指挥和控制接口 (OMS/UCI) 应用程序。此外，DAF RCO 在保护通信和预警方面也做出了重大努力，这将增强 CMCC 的多层安全性。

2019-2020 年国防科学委员会关于 21 世纪多域效应的研究建议在联合 C3I 系统中建立一个开放架构基础，将跨军种的指挥和控制功能结合起来，以支持跨所有领域的复杂操作。¹¹⁶ CMCC 提供了这种类型的集成指挥和控制结构，并可能扩展以支持 ABMS 功能和 JADC2 任务需求。如果 CMCC 作为 ABMS 的零阶段，那么未来的升级将每一两年更新一次，以有纪律和共生的方式全面整合新能力发布。能力升级将是连续的，以防止过时并确保 ABMS 具备应对不断发展的对手威胁的能力。

建议 19：空军快速能力办公室应考虑扩展联合任务指挥中心，并将其指定为先进战斗管理系统的零阶段。

3 治理

不为联合部队指挥官整合的单一服务解决方案在未来的联合战争中几乎没有用处。

—美国空军副参谋长大卫·W·奥尔文将军¹

先进战斗管理系统（ABMS）的治理需要指挥结构和决策结构两者。指挥结构决定组织层次和跨组织的相互关系，而决策结构则侧重于决策和执行。作为一个多平台、多系统的构建体，ABMS 的指挥结构归属于空军助理部长办公室负责采购、技术和后勤（SAF/AQ）。当空军部（DAF）领导人于 2019 年重新引入 ABMS 作为支持联合全域指挥与控制（JADC2）框架的集成系统时，他们选择了一位首席架构师来“创建和管理系统族的贸易空间、设计余量，并定义接口和标准，以确保跨域互操作性，并适应从允许到高度争议的环境。”²他还负责协调由项目经理领导的各个项目（这些项目提供给 ABMS）的不同活动，这些项目有自己的资金和绩效计划。

在 2020 年 11 月，前 SAF/AQ 指示将 ABMS 的管理从首席架构师办公室转移到空军部快速能力办公室（DAF RCO），作为集成的项目执行办公室（PEO）。“战斗人员现在准备在他们的任务领域内部署和操作特定的 ABMS 能力。因此，ABMS 正在进入一个稳定的示范-部署阶段。”³

在新的指挥结构下，作为 ABMS 项目执行办公室（PEO）的空军部快速能力办公室（DAF RCO）负责以下任务：

- 在与首席架构师协调下起草 ABMS 采购战略及后续变更；
- 通过空军审计局进行全面的业务审查，以为 ABMS 采购战略提供信息；
- 起草总体 ABMS 架构和标准供首席架构师批准，而 ABMS PEO 将有权批准所有非系统级的低级标准；
- 主持所有 ABMS 架构审查委员会（ARB）以下的设计评审；
- 提供并整合所有 ABMS 能力，以便纳入架构评估通道；
- 根据批准的 ABMS 采购战略和 ARB 决定执行 ABMS 项目。

首席架构师将：

- 将从空军和太空军参谋长批准的需求文件和测试结果中得出的 ABMS 技术需求进行编码；
- 促进在空军部、战斗指挥部、合作服务机构、其他机构和任务合作伙伴之间整合企业数字架构和标准；
- 在测试之间主持 ABMS 架构审查委员会（ARB）；
- 为 ABMS 采购战略提供意见；
- 与空军部高级利益相关者和外部高级利益相关者互动，以确保努力统一和职责分工；以及
- 在空军部内建立并提供基于模型的系统工程（MBSE）和其他协作工具，以实现数字工程。

服务采购执行官（SAE）将：

- 保留 ABMS 所有方面的决策权，包括批准 ABMS 技术架构和采购战略及所有后续变更；以及
- 解决首席架构师、ABMS PEO 和相关 PEO 之间的分歧。⁴

委员会支持这一治理结构，并认为这是与 ABMS 这样复杂系统不断发展的性质相一致的积极进展。空军部快速能力办公室（DAF RCO）在利用商业技术和设备、国防范围内的

技术开发努力以及加速采购方法来应对威胁演变加速方面具有良好的记录。在其近 20 年的历史中，DAF RCO 成功开发了包括 X-37B 轨道试验飞行器、B-21 Raider 远程打击轰炸机、美国太空军的无人空间试验平台、地对空导弹系统和其他高度机密的系统在内的复杂和先进的武器系统。⁵

除了 SAF/AQ 详细描述的角色和职责之外，还需要注意的是，维持和支持 ABMS 的指挥结构也需要在初步部署结束前定义和建立。为了确保系统在初步部署之后的持续发展，维护和支持的角色、职责以及资金方案需要明确规定。

从决策结构的角度来看，ABMS 需要的不仅仅是内部的空军部协调和批准。作为 JADC2 框架的贡献者，ABMS 还需要与美国的伙伴和盟国进行跨服务和多国协调，依据一套共同商定的操作标准和政策。这将需要一个具有真正决策权的美国国防部（DoD）级别的治理结构。目前，由 J6 领导的 JADC2 跨职能团队（CFT）参与者过多，且未能有效赋权做出所需的高层决策。因此，需要建立一个更高级别的联合决策机构，以提供有关全域作战指挥权、人机决策、互操作性和共享技术的跨服务决策。JADC2 面临的挑战在于，每个军种、战斗指挥部和国防部机构都在开发各自的指挥控制（C2）系统，协调和排除冲突的工作极为有限。最终的结果是形成了一系列不相互连接的、孤立的网络，这些网络可能无法在多域环境中互操作。

在作战期间的治理也是一个值得关注的问题。尽管新的联合作战概念（JWC）已经制定，但仍不清楚如何利用 JADC2 支持的系统来优先处理数据流向所需的行动。例如，JADC2 的一个核心目标是通过优化数据流动来压缩观察-定位-决策-行动（OODA）回路。然而，在全球定位系统（GPS）受限、电子战（EW）或网络安全受损的环境下，尤其是当数据通过自动化传输时，决策过程如何进行仍不明确。

此外，战术层面的整合要求在与联合指挥部的通信被拒绝后，全域作战仍能继续。分布式单位必须具备在缺乏具体指令的情况下，根据指挥官的一般意图行动的理解和权限。这需要对权限的分配和分派进行重大重新思考，尤其是在作战决策有可能升级为核大国之间冲突的情况下。更重要的是，信任的考量必须与风险平衡：军队在何处以及如何依赖并接受未知或新代理的信息和能力，特别是在生命和重大资产处于风险时？下级单位能否被赋予做出战略级别决策的信任？当多国合作伙伴被纳入决策空间时，这些问题变得更加复杂。⁶

另一个令人关注的问题是，每个军种都在其控制范围之外开发和选择指挥控制（C2）解决方案，意图解决联合任务需求。陆军领导人已经表示担忧，地面部队不能采用以空中为中心的指挥系统来进行未来的全域作战。据陆军未来司令部前副司令兼未来和概念中心主任称，“ABMS 不能成为唯一的解决方案，因为它在某些情况下没有考虑到所有其他军种的规模或独特需求。……任何未来的框架都必须考虑陆军的规模问题。其他军种可能只需考虑数百的规模，而陆军则需要考虑数千的规模。”⁷ 委员会认为解决这些问题对于 ABMS 和更大的 JADC2 框架至关重要。

发现 15：由 J6 领导的当前 JADC2 跨职能团队（CFT）是一个积极的第一步，但它包含的参与者过多，且未能有效赋权做出所需的高层决策。

建议 20：联合参谋部 J6 或指定的美国国防部执行代理人应建立一个权威的联合级别机构，以解决和决策所有对联合全域指挥与控制框架的贡献者的技术、操作和指挥问题。

组织整合

除了建立联合指挥控制（C2）环境的技术挑战外，在 JADC2 框架内整合广泛的 ABMS 生态系统还需要考虑组织和人力方面的因素。从组织的角度来看，ABMS 需要具备跨军种、防御机构和多国合作伙伴合作的能力，每个合作方都有其独特的文化和操作规范。各组织之间的不兼容性需要军种的单独和集体承诺来解决。为了打破这些垂直分割并在从战术到战略的所有层面实现有意义和有效的联合互操作性，国防部需要创建一个由共同战术、技术和程序（TTPs）支持的统一愿景。J6 跨职能团队（CFT）在推进对联合互操作性的共同理解和制定通用标准方面是一个积极的第一步，但还需要做更多的工作。这是一个可以借鉴行业实践的领域。

大型组织往往由自主的单位组成，这些单位要么不愿意要么无法与其他单位协调和整合。⁸ 部门内部的个人往往更多地与本单位内部互动，而不是与外部群体互动。这导致了更广泛组织内部的碎片化、分裂和脱节，本质上形成了组织壁垒。造成壁垒的三个常见影响因素是：内部、组织和外部，这些因素相互作用，进一步加强了壁垒的力量。⁹

在国防部社区内部，内部影响因素是每个军种和机构的结构和文化；组织影响因素是特定于程序单元的 TTPs 和操作规范；外部环境则包括战斗指挥官、多国合作伙伴、其他军种、联邦机构等的要求。每个影响因素都对核心单元施加影响，最终强化了孤立、狭隘和独立的结构。当与 JADC2 这样的复杂框架叠加时，克服军种中心主义壁垒的过程变得更加具有挑战性。

为了实现一个有效且互操作的（不仅仅是互补的）联合 C4 企业架构，需要通过水平整合来降低组织和文化障碍。跨军种网络互连的挑战可以通过技术进步来解决，但跨军种组织互连的挑战则需要通过社会整合来建立合作伙伴关系和信任。有效的水平整合要求领导者“连接组织的知识库，建立人员之间的社会关系，并塑造共享的身份认同，所有这些都需要标准化的技术基础设施支持。”¹⁰ 这可以通过以下四个行动领域来实现：

- 通过技术基础设施的标准化实现操作整合；
- 通过建立共享的知识库实现智力整合；
- 通过集体绩效纽带实现社会整合；以及
- 通过创建共同的身份和目标实现情感整合。¹¹

图 3.1 提供了考虑组织整合的框架。为了进一步分解垂直壁垒，行业采用了六个基本步骤：

图 3.1 组织整合框架。来源：S. Ghoshal 和 L. Gratton, 2002, "Integrating the Enterprise," MIT Sloan Management Review, [https://sloanreview.mit.edu/article/](https://sloanreview.mit.edu/article/integrating-the-enterprise).

1. 传达统一愿景；
2. 创建共享责任；
3. 团队协作；
4. 争取领导支持；
5. 引入协作工具；
6. 通过培训转变思维方式和行为。¹²

对于 ABMS 和其他 JADC2 的贡献者来说，共享任务是通过帮助决策者在敌人的 OODA 回路内进行信息行动，从而维持联合部队的军事优势，这提供了一个统一的行动愿景。国

防部的各级领导者完全支持 JADC2，并通过军种间协议和实验共同推进这一概念。¹³ 例如，美国国家科学院、工程院和医学院的空军与海军研究委员会正在主办空军与海军之间的军种间会议，讨论他们对 JADC2 的贡献。会议建立在空军部快速能力办公室（DAF RCO）和海军信息战系统司令部（NAVWAR）之间的持续合作基础上，旨在 ABMS 和 Project Overmatch 之间建立综合方法。¹⁴ J6 在 JADC2 上的领导作用和各利益相关者在跨职能团队（CFT）中的参与鼓励了更大的合作和共享责任。然而，缺乏的是通过培训和激励措施来转变个人的思维方式和行为，以摆脱根深蒂固的组织文化和控制，促进联合和多国防御生态系统的更大利益。

2019 年，空中作战指挥部计划、项目和需求局（A5/8/9）要求兰德项目空军（PAF）检查并推荐应用人工智能（AI）以及更广泛的自动化技术于联合全域指挥与控制（JADC2）的深思熟虑规划的机会。如所设想，JADC2 整合了跨太空、信息、网络、空中、陆地和海洋领域的作战计划、任务分配和评估。

空中作战中心（AOC）是当今美国空军主要的作战级中央指挥与控制（C2）节点。尽管其历史上的有效性，近来 AOC 构建因多种原因而受到挑战。首先，AOC 系统和人员通常位于前沿部署的集中设施。这构成了显著的脆弱性和单一故障点。其次，许多 AOC 信息系统可以追溯到大约 2000 年 AOC 成立之初。AOC 10.2 现代化努力的取消延迟了对 AOC 的关键硬件和软件升级的交付。第三，对改善网络和空间整合的日益重视对 AOC 提出了新的功能和技术要求，并增加了对多域作战的兴趣。第四，AI 和机器学习（ML）领域出现了众多突破。这些领域的新兴技术可以启用新的能力，或者，可以构成新的威胁。因此，进行了这项关于 JADC2 AI 应用的研究，旨在解决空军如何结合 AI/ML 和自动化以实现 JADC2 的问题。一份不对公众开放的附加材料¹，提供了技术细节、评估过程信息以及情景描述。

这份报告可能对美国国防部领导层以及 AI 和/或 C2 的利益相关者，以及对 AI 和支持美国大国竞争感兴趣的国会听众有兴趣。

此项研究由空中作战指挥部 A5/8/9 委托，并在兰德项目空军的力量现代化和实施计划内进行，作为 2019 财年 JADC2 AI 应用项目的一部分。

RAND Project AIR FORCE

兰德项目空军（PAF）是兰德公司的一个部门，是美国空军的联邦资助研究和开发中心，专注于研究和分析。PAF 为空军提供独立的政策替代方案分析，这些分析影响当前和未来的空中、太空及网络力量的发展、使用、战斗准备和支持。研究涵盖四个程序：战略与条令；部队现代化和实施；人力、人事和培训；以及资源管理。这里报告的研究是根据合同 FA7014-16-D-1000 准备的。

关于 PAF 的更多信息可在我们的网站上获得：www.rand.org/paf/

此报告记录了最初于 2019 年 9 月与美国空军共享的工作。2019 年 9 月发行的草案报告已经过正式同行评审和美国空军主题专家的审查。

面临的问题

- 空军的一个关键担忧是空中组件指挥官整合空域之外其他领域能力进入多域作战（MDO）的能力。
- 空中组件指挥官和空中作战中心（AOC）成员整合 MDO 的能力受到流程、系统、训练以及规划和执行经验的限制。
- 鉴于 MDO 规划的复杂性增加和更大的数据需求，空军将需要新的工具，包括那些基于人工智能（AI）的工具，以启用联合全域指挥和控制（JADC2）。
- 聚焦投资需要理解哪些 AI 应用为识别的多域作战概念（CONOPS）提供了最大的作战效果增强。
- 引入 AI 工具要求适当的支持技术生态系统到位。

研究方法

¹ Sherrill Lingel, Jeff Hagen, Eric Hastings, Mary Lee, Matthew Sargent, Matthew Walsh, Li Ang Zhang, Dave Blancett, Edward Geist, and Liam Regan, Joint All-Domain Command and Control for Modern Warfare: Technical Analysis and Supporting Material, Santa Monica, Calif.: RAND Corporation, 2020, Not available to the general public.

- 空军作战融合中心 (AFWIC) 与太平洋空军和美国空军欧洲及非洲空军合作，应假设并继续探索多域作战 (MDO) 概念，以支持国家国防战略，通过战争博弈和桌面演习，并随后向更广泛的社区通报达成一致的多域作战概念。这将促进与其他军种和美国国防部机构的必要交流。
- 空军首席数据办公室应该制定跨运营中心的数据管理政策，以确保数据保存并妥善标记以供访问（包括标记的安全流）以及数据存储容量足够。通过标准化的试验可以帮助验证前进的道路。
- AFWIC 应该与空战司令部 (ACC) 一起评估用于支持多域作战的替代 C2 结构。需要进行额外的战争博弈和研讨会以比较和对比替代方案。ACC 的后续工作将开发、组织、训练和装备计划。
- JADC2 的进展应以一种连贯、渐进、互动的方式发生。整个企业 - C2 结构、数据管理以及工具、应用程序和算法开发 - 应遵循如图 S.1 所示的总体战略。作为作战融合中心，AFWIC 应确保遵守该战略，并向空军参谋长汇报。随着新的 MD 概念从战争博弈和桌面演习中出现，分析团队对其进行评估，而作战人员设计指挥所和其他演习来完善和使概念实现化。沿着多域作战 (MDO) 列向下移动，这些概念通过实际飞行演习、武器和战术努力进一步发展。CONOPS 从概念上升到成为部队的一部分。这些努力还应在三个支持因素之间的进展上提供信息。在每一列的顶部，来自领导层的指导为以下的作战和战术层框定了方向，以便着手推进工作，例如开发数据基础设施、数据访问和算法，以及培训和装备指挥官的工作人员。随着这些支持因素的发展，变化将有助于完善 MDO CONOPS。

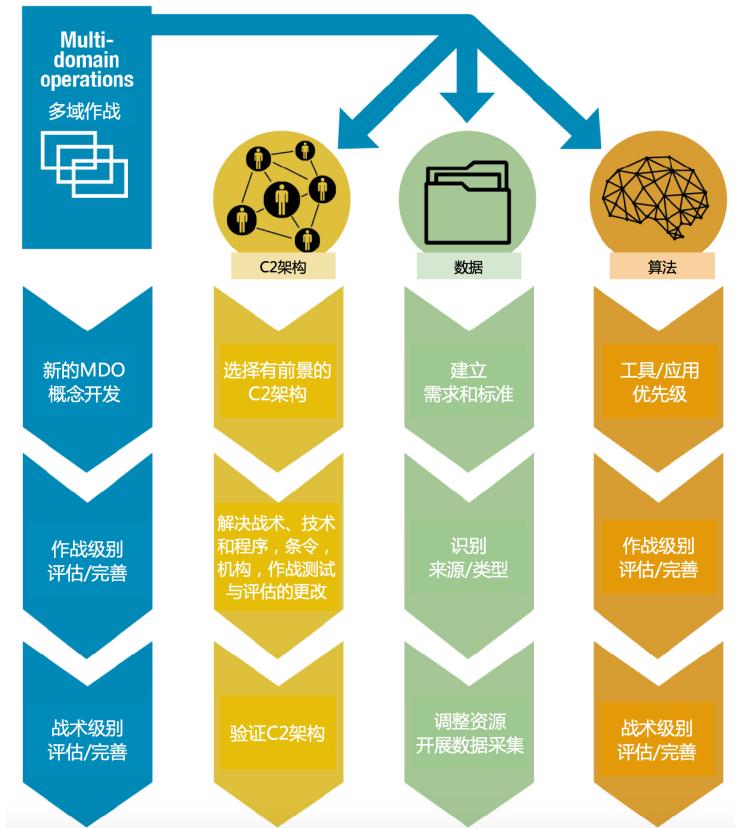


Figure 3.1: 多域作战信息指导 C2 架构、数据和算法进展

NOTE: TTP = tactics, techniques, and procedures.

缩略语

4 在美国空军当前作战体系内实施全域联合指挥与控制的挑战

4.1 当前作战级别指挥和控制挑战

Table 4.1: Air Force Air Operations Centers

Type	AOC	Major Command	Station
Regional	601 AOC	ACC	Tyndall Air Force Base, Florida
Regional	603 AOC	U.S. Air Forces Europe	Ramstein Air Base, Germany
Regional	607 AOC	Pacific Air Forces (PACAF)	Osan Air Base, South Korea
Regional	609 AOC; 609 AOC Detachment 1	U.S. Air Forces Central Command	Al Udeid Air Base, Qatar Shaw Air Force Base, South Carolina
Regional	611 AOC	PACAF	Joint Base Elmendorf-Richardson, Alaska
Regional	612 AOC	U.S. Air Forces Southern Command	Davis-Monthan Air Force Base, Arizona
Regional	613 AOC	PACAF	Joint Base Pearl Harbor-Hickam, Hawaii
Functional	608 AOC	Air Force Strategic Strike Command	Barksdale Air Force Base, Louisiana
Functional	614 AOC	Air Force Space Command	Vandenberg Air Force Base, California
Functional	618 AOC	Air Mobility Command	Scott Air Force Base, Illinois
Functional	623 AOC	Air Force Special Operations Command	Hurlburt Field, Florida
Functional	624 OC	Air Force Space Command	Lackland Air Force Base, Texas
Functional	625 OC	ACC	Lackland Air Force Base, Texas

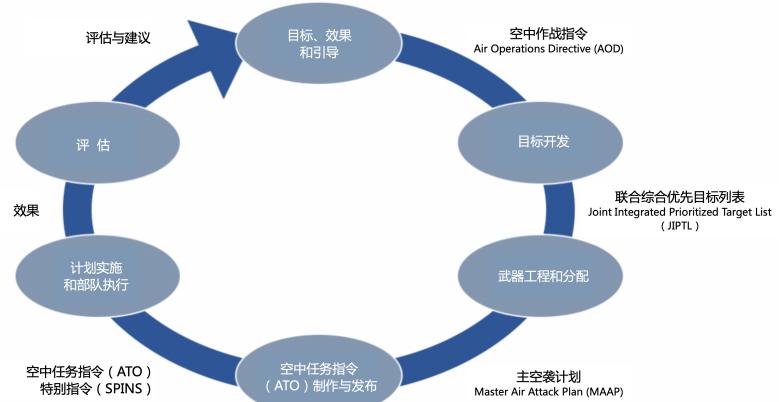


Figure 4.1: 空中任务循环

来源：美国空军，作战性雇用：空中作战指挥中心，*AFTTP 3-3.AOC*, 2016 年 3 月 31 日，一般公众不可获得。

4.1.1 规划速度

AOC 系统和流程已经发展到最佳状态，以便将指挥官的目标有效地转化为目标和出击任务，然后寻找并攻击它们。过去 20 年中使用 AOC 进行的冲突使得有合理的规划和反应时间。支援元素，如电子战、网络和太空，已尽可能地集成，并主要以手动方式进行。在高端冲突中，这将是一项挑战，并且随着多域作战范围的扩大，这种做法将变得越来越不可行。经典的 72 小时 ATC 在这种相对稳定状态的作战中效果良好，比如战略轰炸运动；对静止的、掩体深的部队的打击；支持预先计划的地面行动；以及规划对付叛乱的情报、监视和侦察（ISR）支援。这个规划周期的很大一部分用于在执行前长达 72 小时的时间里组织各组

成部分、指挥官和各级单位的协调会议。目标是使用多种情报和弹药仔细制定的，平台则是提前一到三天有意选择的，以最大限度地提高杀伤概率，同时最小化风险和附带损害。指挥官和法律审查在多个层面进行。联盟伙伴必须被整合、同步或至少进行解决冲突。计划还在执行前十小时以上发布给机群和中队级单位，以允许进行详细的战略级别规划，以最小化风险并最大化效果。

所有这些谨慎安排允许对风险进行管理，并有效地利用空中力量，但这些计划需要时间。这种全面的规划过程加剧了一个事实，即在大多数近等同对手的冲突中，美国可能处于防守地位，试图延迟和阻止对手已经启动的计划。除非预先计划几乎完美，否则，如果对手能够在 60 小时内实现其目标，那么 72 小时的 ATC 就不会很有效。

- 空军多领域作战必须包括从空中、太空和网络中产生的攻击和防御效果，能够独立和直接支持 JFC 的目标
- MDO 不仅仅是一个领域中的系统支持另一个领域中的作战（必要但不充分）
- MDO 是高速、作战灵活的行动，以一种对手无法匹敌的作战节奏对对手提出多种困境。
- MDO 要求在所有领域中产生效果的能力实现无缝、动态和持续的整合。¹

Table 4.2: 多域 C2 项目的产品开发

Cost Category Item	Performing Activity	Cost (in Millions)
MDC2 C2 common platform	KR	\$60
MDC2 enterprise data lake	Various	\$40
MDC2 ShadowNet experimentation	Various	\$36
MDC2 development	Various	\$7
Support, test and evaluation, and management	Various	\$8
Total		\$151

来源：美国国防部长财务报告，未标日期。

不向一般公众提供的配套报告描述了 KR 和 ShadowNet 以及国防高级研究项目局 (DARPA)、空军研究实验室 (AFRL)、AFWERX 等的角色和贡献，以及朝着 JADC2 的演进。

C2 的努力超出了 MDC2 PE 的范围。空军内部的空间和网络也有 C2 PE，陆军和海军也是如此。在 2018 年和 2019 年的财政年度，每年的累计支出最高的是空军的太空部门，其次是空军的网络部门，预计这种模式将在 2020 财年继续。特别值得注意的是，在联合太空作战中心进行的 RDT&E 投资，这是太空的主要作战级 C2 节点，以及投资于更好地将网络任务过程与 AOC 集成，增加网络行动对作战、服务和联合指挥官的可见性的能力。陆军和海军的 C2 支出与空军的支出数量级相同。C2 PE 并不能完全涵盖美国国防部 (DoD) 内的 JADC2 或人工智能的所有努力。其他利益相关者参与了相关工作，如表 2.2 所列。

1. 计算机视觉：涉及检测和分类视觉世界中的对象。Project Maven 中包含了用于检测和分类自然场景中对象的 AI 算法示例。
2. 自然语言处理 (NLP)：执行语音和文本识别及翻译，目前已在数百万美国家庭中使用，这些家庭使用谷歌 Home 和亚马逊 Echo。
3. 专家系统：基于规则的系统，使用大量专家知识创建。它们已在医疗和金融决策以及其他领域使用了数十年。
4. 规划器：解决调度和资源分配问题，例如，已被用于减少谷歌的能源使用，并在实时策略游戏中达到超人水平的表现。

¹ Italics original, Chance Saltzman, "MDC2 Overview," briefing for 2018 C2 Summit, June 2018.

Table 4.3: 空军 C2 的其他利益相关者和贡献者

Effort	Emphasis	Description
Common Mission Control Center (CMCC)	Capability	Central hub for battle management and C2 across a range of next-generation aircraft and in a multi-level, secure environment
Joint Enterprise Defense Infrastructure (JEDI)	Capability	Amazon Web Services—provided service of hosting and distributing mission-critical workloads and information to warfighters across the globe
AFWERX	Concepts and requirements	Catalyst for agile Air Force engagement across industry, academia, and nontraditional contributors to drive innovation
Combined Air Operations Center – Nellis	Concepts and requirements	Provides advanced training for operational C2 through MD and joint integration
Secretary of the Air Force/Chief Information Office (SAF/CIO) Air Force Chief Data Office (AF CDO)	Information	Advises the SAF and the Chief of Staff of the Air Force on IT, cyberspace, and national security systems
Air Force Knowledge Management Capability Working Group	Information	Manages the Air Force Knowledge Management (KM) community and KM-related requirements and interests
Cyber mission platform	Platform	Infrastructure and platform for the Air Force’s Offensive Cyber Product Line. Uses Agile acquisition strategy and has implemented rolling authorization to operate
National Space Defense Center	Platform	Creates unity of effort and information in space operations among DoD, the Intelligence Community, and interagency, allied, and commercial space entities. Provides data as a service (DaaS) to facilitate movement of data across classification boundaries and provides common, standard interfaces that facilitate large-scale integration
Open Architecture Distributed Common Ground System	Platform	Technology component of Air Force Distributed Common Ground System modernization framework. Provides computing hardware, server virtualization, data cloud, and service-oriented architecture stack to support rapid development and transition of incremental capabilities

5. 机器学习：通过在训练集中策划的示例（即监督学习）或通过与真实或模拟环境的互动（即强化学习）获取知识。机器学习已应用于信用卡欺诈检测等实际问题，并且是前一段中提到的许多 AI/ML 系统的组成部分。此类别中的方法是通用的，可以与前四个类别中的每一个结合使用。

6. 机器人技术：使用 AI/ML 的多种能力，包括感知、场景处理、规划和行动选择，使得具体化的系统能够与环境互动。此类别反映了从上述某些或全部类别中整合方法。

Table 4.4: Exemplar Domain Contributors to SEAD Vignette

Domain	Detect (Find)	Track and Identify (Fix)	Strike (Engage)	Support
Air	Airborne ISR (e.g., rivet joint)	Nontraditional ISR (e.g., F-35)		<ul style="list-style-type: none"> Decoys to stimulate radars EA-18G standoff jamming
Space	Overhead ISR			<ul style="list-style-type: none"> Navigation and timing Beyond-line-of-sight communications (e.g., from ISR to AOC)
Cyber	Integrated air defense system network monitoring			<ul style="list-style-type: none"> Delay integrated air defense system tracks sent to SAMs Insert false targets
Land		Long-range fires (e.g., guided multiple launch rocket system)		

图 3.1 绘制了我们 SEAD 情景的一个可能的高度自动化的交战序列，从左上角的初始 ISR 提示开始，到右下角的评估结束。² 从顶部开始，第一行聚焦于目标检测和作战行动方案 (COA) 选择，中间一行是执行 COA 的资源选择过程，底部一行详细说明了任务执行。红色矩形和文字指示适合应用 AI 的过程，而黑色平行四边形突出显示了可能需要人类参与的过程。黑色矩形显示了过程的外部输入，如 ISR 来源或其他领域的能力。

Table 4.5: 跨三个 MD 场景的现代化 C2 任务

C2 任务	SEAD 场景	HADR 场景	扩散的 ISR 场景
多边 MD COP	x		x
自动推荐计划		x	
自动资源识别	x		x
自动资源选择 (最小化机会成本)	x		x
自动空域清理	x		x
自动聊天和消息创建	x		x
自动收集计划		x	
自动撤离计划		x	
自动打击和支持计划	x		x
自动评估当前作战并提示修改	x		x

²Here, highly automated refers to the digital nature of the data and the machine-to-machine transference of information. We examine opportunities for using AI in these C2 processes in this section.

³Talon Thresher 是一个先进的多域传感平台，旨在增强军事和情报用途的空域态势感知 (ADA)。最初由现今的印太司令部 (INDOPACOM) 提出需求，设计目的是解决太平洋区域的空中威胁跟踪和

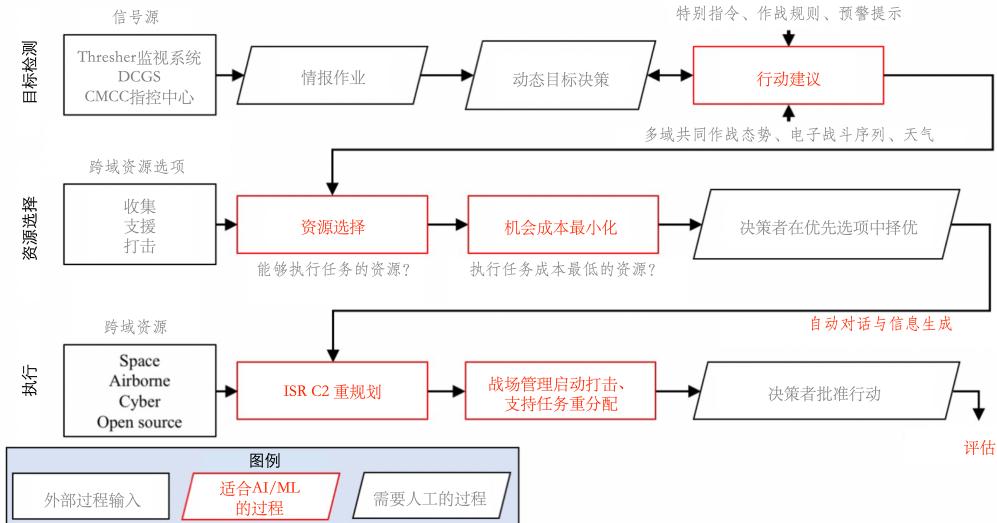


Figure 4.2: 针对多域压制敌方防空系统的现代化 C2 模型

注: BM= 战斗管理, DCGS = 分布式共用地面系统, EOB = 电子作战序列, ROE = 作战规则, WX= 天气.

References

- [1] Air Force Instruction 13-1AOC, Operational Procedures-Air Operations Center (AOC), Vol. 3, Washington, D.C.: Department of the Air Force, November 2, 2011, incorporating change 1, May 18, 2012.
- [2] Air Force Life Cycle Management Center, Battle Management Directorate, Descriptive List of Applicable Publications (DLOAP) for the Air Operations Center (AOC), Hanscom Air Force Base, Mass., April 1, 2019, Not available to the general public.
- [3] AlphaStar Team, "AlphaStar: Mastering the Real-Time Strategy Game StarCraft II," deepmind.com, January 24, 2019. As of July 31, 2019:
- [4] <https://deepmind.com/blog/alphastar-mastering-real-time-strategy-game-starcraft-ii/>
- [5] Bellingham, John S., Michael Tillerson, Mehdi Alighanbari, and Jonathan P. How, "Cooperative Path Planning for Multiple UAVs in Dynamic and Uncertain Environments," Proceedings of the 41st IEEE Conference on Decision and Control, Las Vegas, Nev., December 2002. As of July 1, 2019:
- [6] <https://www.semanticscholar.org/paper/Cooperative-path-planning-for-multiple-UAVs-in-and-Bellingham-Tillerson/8c9d12969607238d7071f2f45c99ab6bde88598d>
- [7] Brocchi, Chiara, Davide Grande, Kayvaun Rowshankish, Tamim Saleh, and Allen Weinberg, "Designing a Data Transformation That Delivers Value Right from the Start," McKinsey and Company, October 2018. As of December 26, 2019:
- [8] <https://www.mckinsey.com/industries/financial-services/our-insights/designing-a-data-transformation-that-delivers-value-right-from-the-start>

识别问题。这个基于云的系统利用融合引擎集成“大数据”，能够在近乎实时的情况下同时跟踪数千条航迹，提供全面的空域图像。Talon Thresher的功能覆盖多个分类级别，使情报界和国防部内的众多用户可以访问。它还包含海事态势感知信息，进一步增强了其实用性。该系统的特点是稳健性、可扩展性和易于访问，无需本地软件安装和维护。Talon Thresher代表了态势感知方面的重大进步，提供了全球范围内增强的航空器及其他空中物体的跟踪和识别能力。

Table 4.6: 现代化的 C2 数据需求在三个 MD 场景中的需求

数据来源和输入	SEAD 场景	HADR 场景	扩散式 ISR 场景
空域	x		x
ATC 跟踪	x	x	x
蓝方 COP		x	x
蓝方力量跟踪	x		x
蓝方计划	x		x
感兴趣的社区列表	x	x	x
当前空域控制命令	x	x	x
外交许可		x	
选择后的跨领域参与者	x		
电子作战序列	x		x
退出策略		x	
飞行计划	x		x
东道国	x	x	x
情报提示	x	x	x
ISR 收集	x		x
制图	x	x	
医疗服务	x	x	x
任务报告	x	x	x
非政府组织	x	x	
目标和预期效果	x	x	x
绩效指标	x		
防御威胁减少机构的信息			x
公开可用信息	x	x	x
选定的资源	x	x	x
交战规则	x		x
特别指示	x		x
美国国务院		x	x
目标位置		x	x
任务优先级	x		x
塔隆推送器 ³	x		x
天气		x	x

- [9] Bughin, Jacques, Brian McCarthy, and Michael Chui, "A Survey of 3,000 Executives Reveals How Businesses Succeed with AI," Harvard Business Review, August 28, 2017. As of September 1, 2019:
- [10] <https://hbr.org/2017/08/a-survey-of-3000-executives-reveals-how-businesses-succeed-withai?hootPostID=4247d7900bda767e984816fe65f00444>
- [11] Chen, Chaofan, Oscar Li, Chaofan Tao, Alina Jade Barnett, Jonathan Su, and Cynthia Rudin, "This Looks Like That: Deep Learning for Interpretable Image Recognition," 33rd Conference on Neural Information Processing Systems, Vancouver, Canada, 2019. As of April 15, 2020:
- [12] <https://arxiv.org/pdf/1806.10574.pdf>
- [13] Compoc, Jeffery, Obtaining MDC2 Capabilities Inside Technocratic Boundaries: Satisfying Multi-Domain Operational Desires Through an Acquiescent Technical Strategy, Nellis Air Force Base, Nev.: Air Combat Command, 505 Test and Training Squadron, Combined Air and Space Operations Center-Nellis/Shadow Operations Center-Nellis, March 1, 2019.

- [14] DoD—See U.S. Department of Defense.
- [15] Ernest, Nicholas, David Carroll, Corey Schumacher, Matthew Clark, Kelly Cohen, and Gene Lee, "Genetic Fuzzy Based Artificial Intelligence for Unmanned Combat Aerial Vehicle Control in Simulated Air Combat Missions," *Journal of Defense Management*, Vol. 6, No. 1, 2016. As of August 1, 2019:
- [16] <https://www.longdom.org/open-access/genetic-fuzzy-based-artificial-intelligence-for-unmanned-combat-aerial-vehicle-control-in-simulated-air-combat-missions-2167-03741000144.pdf>
- [17] Freedberg, Sydney J., "The Art of Command, the Science of AI," *Breaking Defense*, November 25, 2019. As of November 27, 2019:
- [18] <https://breakingdefense.com/2019/11/the-art-of-command-the-science-of-ai/>
- [19] Gao, Jingyue, Xiting Wang, Yasha Wang, and Xing Die, "Explainable Recommendation Through Attentive Multi-View Learning," presentation at the Association for the Advancement of Artificial Intelligence Conference on Artificial Intelligence, Arlington, Va., March 2019. As of April 15, 2020:
- [20] <https://www.microsoft.com/en-us/research/publication/explainable-recommendation-through-attentive-multi-view-learning/>
- [21] Goldfein, David, "CSAF Focus Area: Enhancing Multi-Domain Command and Control . . . Tying It All Together," Washington, D.C.: Chief of Staff, U.S. Air Force, March 2017. As of August 21, 2019:
- [22] [https://www.af.mil/Portals/1/documents/csaf/letter3/CSAF Focus Area CoverPage.pdf](https://www.af.mil/Portals/1/documents/csaf/letter3/CSAF%20Focus%20Area%20Cover%20Page.pdf)
- [23] Goldfein, David L., Multi-Domain Command and Control (MDC2): Enterprise Capability Collaboration Team (ECCT), Campaign Plan, Strategy Document, Washington, D.C.: U.S. Air Force, January 2, 2018, Not available to the general public.
- [24] Greene, Jay, and Aaron Gregg, "Amazon's Formal Challenge to Huge Pentagon Award Uses Videos That Mark Potential Influence Exerted by Trump," *Washington Post*, November 23, 2019. As of December 26, 2019:
- [25] <https://www.washingtonpost.com/technology/2019/11/22/amazon-files-protest-pentagons-billion-jedi-award-under-seal/>
- [26] Gregg, Aaron, "Pentagon Asks to Reconsider Part of the JEDI Cloud Decision After Amazon Protest," *Washington Post*, March 12, 2020. As of April 23, 2020: <https://www.washingtonpost.com/business/2020/03/12/pentagon-asks-reconsider-part-jedi-cloud-decision-after-amazon-protest/>
- [27] David Gunning, Explainable Artificial Intelligence (XAI), Arlington, Va.: Defense Advanced Research Projects Agency, 2016. As of May 13, 2020:
- [28] [https://www.cc.gatech.edu/alanwags/DLAI2016/\(Gunning\)%20IJCAI16%20DLAI%20WS.pdf](https://www.cc.gatech.edu/alanwags/DLAI2016/(Gunning)%20IJCAI16%20DLAI%20WS.pdf)
- [29] Headquarters U.S. Air Force, Financial Management and Comptroller, "Air Force President's Budget FY21," 2019. As of September 3, 2019: <https://www.saffm.hq.af.mil/FM-Resources/Budget/>
- [30] Hebert, Adam J., "Compressing the Kill Chain," *Air Force Magazine*, June 18, 2008. As of December 26, 2019:

- [31] <https://www.airforcemag.com/article/0303killchain/>
- [32] Jane's, "S-300V," Land Warfare Platforms: Artillery and Air Defence, last updated October 7, 2019. As of April 9, 2020:
- [33] <https://janes.ihs.com/Janes/DisplayFile/JLAD0110>
- [34] Joint Publication 3-0, Joint Operations, Washington, D.C.: Joint Chiefs of Staff, January 17, 2017, incorporating change 1, October 22, 2018. As of May 14, 2020:
- [35] https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_0ch1.pdf?ver=2018-11-27_160457-910
- [36] Joint Publication 3-01, Countering Air and Missile Threats, Washington, D.C.: Joint Chiefs of Staff, April 21, 2017, validated May 2, 2018. As of December 26, 2019: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_01_pa.pdf
- [37] Joint Publication 5-0, Joint Planning, Washington, D.C.: Joint Chiefs of Staff, June 16, 2017. As of August 19, 2019: https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp5_0_20171606.pdf
- [38] Lawrence, Craig, "Adapting Cross-Domain Kill-Webs (ACK): A Framework for Decentralized Control of Multi-Domain Mosaic Warfare," Strategic Technology Office, Defense Advanced Research Projects Agency PDF briefing slides, July 27, 2018. As of July 23, 2019: <https://www.darpa.mil/attachments/ACK-Industry-Day-Briefing.pdf>
- [39] Leggette, Wesley, and Michael Factor, "The Future of Object Storage: From a Data Dump to a Data Lake," IBM webpage, December 3, 2019. As of December 30, 2019: <https://www.ibm.com/cloud/blog/the-future-of-object-storage-from-a-data-dump-to-a-datalake>
- [40] Leskovec, Jure, Anand Rajaraman, and Jeff Ullman, Mining of Massive Datasets, 2nd ed., Cambridge, UK: Cambridge University Press, 2014.
- [41] Light, Thomas, Brian K. Dougherty, Caroline Baxter, Frank A. Camm, Mark A. Lorell, Michael Simpson, and David Wooddell, Improving Modernization and Sustainment Outcomes for the 618th Air Operations Center, Santa Monica, Calif.: RAND Corporation, 2019, Not available to the general public.
- [42] Lingel, Sherrill, Jeff Hagen, Eric Hastings, Mary Lee, Matthew Sargent, Matthew Walsh, Li Ang Zhang, Dave Blancett, Edward Geist, and Liam Regan, Joint All-Domain Command and Control for Modern Warfare: Technical Analysis and Supporting Material, Santa Monica, Calif.: RAND Corporation, 2020, Not available to the general public.
- [43] Macias, Amanda, "Pentagon Will Not Award JEDI Cloud Contract Until New Defense Secretary Completes Review," CNBC webpage, August 9, 2019.
- [44] McCullough, Amy, "USAF Looks to Create New Command and Control Structure," Air Force Magazine, June 6, 2018. As of May 13, 2020:
- [45] <https://www.airforcemag.com/usaf-looks-to-create-new-command-and-control-structure/>
- [46] McMurry, Robert D., "Use of Open Mission Systems/Universal Command and Control Interface," memorandum to the Air Force Program Executive Officers, Washington, D.C., October 9, 2018.
- [47] Moroney, Jennifer D. P., Stephanie Pezard, Laurel E. Miller, Jeffrey Engstrom, and Abby Doll, Lessons from Department of Defense Disaster Relief Efforts in the Asia-Pacific Region,

- Santa Monica, Calif.: RAND Corporation, RR-146-OSD, 2013. As of December 10, 2019:
https://www.rand.org/pubs/research_reports/RR146.html
- [48] Moseley, T. Michael, Operation Iraqi Freedom: By the Numbers, PDF slides, U.S. Air Forces Central Command, Prince Sultan Air Base, Kingdom of Saudi Arabia, April 30, 2003.
- [49] Russell, Stuart J., and Peter Norvig, Artificial Intelligence: A Modern Approach, 3rd ed., Upper Saddle River, N.J.: Prentice Hall, 2009.
- [50] Saltzman, Chance, "MDC2 Overview," briefing for 2018 C2 Summit, June 2018. As of July 23, 2019:
- [51] [https://www.mitre.org/sites/default/files/publications/Special-Presentation-Gen ChanceSaltzman MDC2 Overview for MITRE-June-2018.pdf](https://www.mitre.org/sites/default/files/publications/Special-Presentation-Gen%20ChanceSaltzman%20MDC2%20Overview%20for%20MITRE-June-2018.pdf)
- [52] Under Secretary of Defense for Acquisition, Technology and Logistics, Lessons Learned/Strengths: Operation Tomodachi / Operation Pacific Passage, undated. As of April 9, 2020:
- [53] [https://www.acq.osd.mil/dpap/ccap/cc/jcchb/Files/Topical/After Action Report/resources/Lessons Learned Operation TOMODACHI.pdf](https://www.acq.osd.mil/dpap/ccap/cc/jcchb/Files/Topical/After%20Action%20Report/resources/Lessons%20Learned%20Operation%20TOMODACHI.pdf)
- [54] Under Secretary of Defense (Comptroller), "DoD Budget Request: Defense Budget MaterialsFY2021," webpage, undated. As of April 23, 2020:
- [55] <https://comptroller.defense.gov/Budget-Materials/>
- [56] U.S. Air Force, Operational Employment: Air Operations Center, AFTTP 3-3.AOC, March 31, 2016a, Not available to the general public.
- [57] U.S. Air Force, Air Superiority 2030 Flight Plan: Enterprise Capability Collaboration Team, May 2016b.
- [58] U.S. Air Force, Virtual Distributed Laboratory, "Common Mission Control Center (CMCC)," September 27, 2017. As of September 3, 2019:
- [59] <https://www.vdl.afrl.af.mil/programs/uci/cmcc.php>
- [60] U.S. Congress, "Combined Congressional Report: 45-Day Report to Congress on JEDI Cloud Computing Services Request for Proposal and 60-Day Report to Congress on a Framework for all Department Entities to Acquire Cloud Computing Services," undated. As of December 26, 2019:
- [61] https://imlive.s3.amazonaws.com/Federal_Government/ID151830346965529215587195222610265670631/180510_Final_Cloud_Combined_Congressional_Report_vg7_PDF_Redacted.pdf
- [62] U.S. Department of Defense, "JAIC and DSTA Forge Technology Collaboration," press release, Singapore, June 27, 2019.
- [63] U.S. Forces Japan, Baseline Special Instructions (SPINs), Version 6, undated.