



边缘指挥控制： 网络信息时代指挥控制新范式

**Edge Command and Control:
A New Paradigm for Command and Control in
the Network Information Age**

信息系统工程全国重点实验室
National Key Laboratory of Information Systems Engineering
2025年8月



边缘指挥控制：网络信息时代 指挥控制新范式

**Edge Command and Control: A New
Paradigm for Command and Control in the
Network Information Age**

信息系统工程国家重点实验室

National Key Laboratory of Information Systems Engineering

2025 年 8 月



前 言

指挥控制（Command and Control, C2）的成效是战争胜负的决定因素，联合作战、全域作战的重心在于指挥控制，取得体系优势的关键也在于指挥控制。在战争中，任何一项其他活动的重要程度都无法与指挥控制相提并论。

指挥控制不是一成不变的，政治、经济、科技和战争规模等都在牵引着指挥控制的发展演变。特别是科技的发展加速了这种演变，催生了以智能无人为代表的新域新质作战力量，指挥控制的主体客体、要素结构、技术手段、系统形态等面临根本性的变化，整个领域正在经历一场深刻变革。这种演变呈现出清晰的脉络，从中心化组织形成中心化指挥控制，到一线自主协同形成边缘指挥控制，呈现出“集中—分布—自组—敏捷”的演化过程。

人类组织形态最开始以中心化为主，是集权的、层级制的、金字塔形的，马克思·韦伯将之归结为官僚制模型。这是一种严密、高效、精确的组织体系，指挥单元和行动单元严格分开，上下级之间形成指挥命令的层级关系，上级负责政策制定，有指挥、监督、命令之权；下级则必须依据官僚规则如实地执行上级命令。这种由中心化组织演化而来的中心化指挥控制也是一种自顶向下的指挥控制方式，它在解决静止性问题，以及不确定性较少的问题时得



心应手，长期被指挥员娴熟运用，并成为一种范式。随着战争形态的改变、不确定环境的显现和去中心化趋势的加强，中心化指挥控制范式的不足逐渐显现，去中心化的边缘指挥控制弥补了中心化指挥控制的不足。这种指挥控制方式是典型的自组织，也是一种自下而上的指挥控制方式，呈现出自任务、自组织、自行动、自适应等特征。

本报告主要聚焦边缘指挥控制这一新的指挥控制范式，分析其时代背景、概念内涵、实现途径，提出研究建议。报告由四部分组成。第一部分介绍边缘指控的时代背景，以及“边缘崛起”现象的观察与思考。第二部分概述边缘指控的概念内涵，包括定义、本质特征、过程模型、制胜机理。第三部分剖析边缘指控的实现途径，从指挥方式、网信支撑、开放共享、协同规则等四个方面进行阐述。第四部分提出相关的研究问题，涵盖组织设计、自主协同、指控支撑等方面。

本报告由张维明、朱承策划组织，朱承主笔撰写，主要内容基于实验室近年来开展的相关研究与实践，主要研究人员包括陈涛、朱先强、丁兆云、雷洪涛、周鋈、汤罗浩、刘斌、刘毅、罗来龙、张千桢、张胜、任棒棒、老明瑞、余正飞、冯清泉、吴亮等。其中，吴亮、冯清泉为本报告制作了插图。



Preface

The effectiveness of Command and Control (C2) is the decisive factor in determining victory or defeat in war. C2 serves as the center of gravity for joint and all-domain operations, and it is the key to achieving a decisive systemic advantage. In warfare, the importance of Command and Control is simply unparalleled by any other activity.

C2 is not static; it is continually shaped by factors such as politics, economics, technology, and the scale of warfare. Technological advancement, in particular, has accelerated this evolution, giving rise to new domains and novel combat capabilities, epitomized by intelligent and autonomous systems. Consequently, the subjects and objects of C2, its elemental structure, technical means, and systemic morphology are all facing fundamental changes, and the entire field is undergoing a profound transformation. This evolution follows a clear trajectory: from centralized Command and Control formed by hierarchical organizations, to edge Command and Control enabled by frontline autonomous collaboration. It demonstrates an evolutionary process of 'Centralization→Distribution→Self-Organization→Agility'.



Early human organizational forms were predominantly centralized, characterized by authoritarian, hierarchical, and pyramid-like structures, which Max Weber summarized as the bureaucratic model. This represented a rigorous, efficient, and precise organizational system wherein command units and action units were strictly separated. A hierarchical relationship of command was established between superiors and subordinates: the former were responsible for policy-making with the authority to direct, supervise, and command, while the latter were obligated to faithfully execute superiors' orders according to bureaucratic rules. The centralized Command and Control that evolved from these organizations was consequently a top-down approach. It proved highly effective for resolving static problems and those with low uncertainty, was skillfully employed by commanders over the long term, and eventually became a paradigm. However, with changes in the nature of warfare, the emergence of uncertain environments, and a growing trend toward decentralization, the deficiencies of the centralized C2 paradigm became increasingly apparent. Decentralized edge Command and Control emerged to compensate for these shortcomings. This method of C2 is a typical form of self-organization and represents a bottom-up approach. It exhibits characteristics



such as autonomous tasking, self-organization, autonomous action, and self-adaptation.

This report focuses on Edge Command and Control (Edge C2), a new paradigm in C2, analyzing its contemporary context, conceptual meaning, and implementation pathways, while also proposing research recommendations. The report is composed of four parts: Part One introduces the contemporary context for Edge C2 and presents observations and reflections on the "Rise of the Edge" phenomenon. Part Two outlines the conceptual meaning of Edge C2, including its definition, essential characteristics, process model, and principles of victory. Part Three analyzes the implementation pathways for Edge C2, elaborating from four aspects of command methods, network-information support, open sharing, and collaboration rules. Part Four proposes related research questions covering areas such as organizational design, autonomous collaboration, and Command and Control support systems.

This report was planned and organized by Zhang Weiming and Zhu Cheng, with Zhu Cheng serving as the lead author. The main content is based on the related research and practice conducted by National Key Laboratory of Information Systems Engineering in recent years. The principal researchers include Chen Tao, Zhu Xianqiang, Ding



Zhaoyun, Lei Hongtao, Zhou Yun, Tang Luohao, Liu Bin, Liu Yi, Luo Lailong, Zhang Qianzhen, Zhang Sheng, Ren Bangbang, Lao Mingrui, Yu Zhengfei, Feng Qingquan, and Wu Liang. Among them, Wu Liang and Feng Qingquan created the illustrations for this report.



目 录

前 言	i
一、研究背景	1
1.1 时代与战争之变	1
1.2 边缘崛起：从重心到边缘	2
二、概念内涵	6
2.1 定义与内涵	6
2.2 “四自”特征	10
2.3 涌现与反馈控制：双模过程模型	15
2.4 面向适应性优势的三重制胜机理	19
三、实现途径	23
3.1 动态授权：指挥方式的重塑	23
3.1.1 从静态身份到动态授权：指挥权的新范式	24
3.1.2 案例分析：俄乌冲突中的指挥方式对比	26
3.1.3 指挥方式转变的难点	28
3.2 网信支撑：“活系统”的基石	30
3.2.1 网络：坚韧自愈的连接	31
3.2.2 云计算：无处不在的计算	32
3.2.3 安全：“零信任”架构下的验证	33
3.2.4 数据：按需流动的资源	34
3.2.5 智能：数字生命体的决策引擎	34



3.2.6 软件：软件工厂与应用商店模式.....	36
3.2.7 标准化：开放架构下的通用语言	37
3.3 开放共享：指挥控制的新理念	37
3.3.1 开放共享：赋能边缘指控.....	38
3.3.2 案例分析：2025 年 5 月印巴冲突.....	39
3.4 协同规则：导向性涌现的源泉	42
3.4.1 协同规则设计的核心要素	42
3.4.2 协同规则的基本运行过程.....	46
四、研究建议	49
4.1 边缘指控组织设计	50
研究问题 1：边缘指控组织形态动态切换机制研究.....	50
研究问题 2：去中心化人机集群中指挥功能的定义、度量与临机实现	51
4.2 边缘自主协同技术	53
研究问题 3：大规模异构无人集群的跨域自主协商与冲突消解.....	53
研究问题 4：异构智能体在柔性集成中的涌现性行为预测与约束..	54
研究问题 5：自主智能体网络中合作行为的演化动力学研究.....	55
研究问题 6：多域作战空间的分布式拍卖与实时协商机制.....	56
4.3 边缘指控支撑技术	58
研究问题 7：支撑军事体系跨代演化的可进化开放架构设计原理..	58
研究问题 8：对人类队友信念、意图与注意力的建模与预测.....	59
研究问题 9：基于因果推理与叙事逻辑的作战规划方法.....	60
参考文献	62



一、研究背景

随着网络信息技术的快速发展，战争形态发生了显著变化，带来了军队组织形态的深刻变革。传统由“中心”（司令部）垄断感知、决策与控制权的金字塔模型正趋于瓦解，以“边缘”（前线小型作战单元）为基础，具备高度自组织能力和敏捷适变特性的“分布式生命体”正破茧而出。

1.1 时代与战争之变

每个时代有每个时代的战争。进入 21 世纪后，军事技术的迅猛发展，以及由此带来的新军事革命，不但使战争的内涵和外延发生了重大变化，也促使战争面貌发生了深刻变化，主要体现在以下几个方面：

一是战争形态发生改变。网络信息时代，高技术条件下的局部战争成为战争的主要形态。参战力量更加多元，多域资源之间联系更加紧密，时间窗口的重要性进一步提升，指挥控制周期更短，一线和边缘的重要性更为突出。网络信息时代，往往边缘地带一个旅级乃至更小规模的战斗，就可以决定一场战争的胜负。旅、营或更低级别的战术单位将成为主要的作战单元，并可能出现按作战职能编成的小型联合体。战术单位的重要性日益重要。



二是不确定性的凸显。纵观人类文明史，人类社会正在加速变革，不确定由以前的偶然状态变成了一种常态。同时，万物的关联性和互动的高密度使得系统呈现非线性运行状态。基于经验而制定的计划或规划在面对这种瞬息万变的环境时显得难以适从。对于战争而言，现代战争的不确定性较之以前也进一步凸显了，克劳塞维茨的战争迷雾不但没有减少，反而增加了。在这种情况下，敏捷性必须成为首要素质，而不是效率。敏捷、适应力强在正常情况下是边缘团队和小型团队才具有的特质。因此，必须按照快速重组、信息共享等原则重新进行组织设计，发挥边缘组织在应对不确定性环境中的独特作用。

三是去中心化趋势更为明显。中心化组织本质上是一种他组织，它在解决确定性和静态问题时得心应手，但弹性、灵活性、适应性显得不足，常会因一个点失败而崩溃。去中心化组织起源于互联网，它没有绝对的、固定的中心节点存在，每个节点都可以成为中心。这种组织能克服僵硬的、自上而下的组织的弊端，它看似没有中心，各自为战，但在围绕着一个目标开展行动时，这种自组织具有极大的弹性、灵活性和适应性。

1.2 边缘崛起：从重心到边缘

在当代军事变革的洪流中，最深刻且具颠覆性的组织形态革命，并非简单的扁平化或网络化，而是一场权力的



根本性逆转——边缘崛起。这标志着传统军队中，由“中心”（司令部）垄断感知、决策与控制权的金字塔模型正趋于瓦解，一个以“边缘”（前线小型作战单元）为基础，具备高度自组织能力和敏捷适变特性的“分布式生命体”正破茧而出。

（1）中心之“重”与边缘之“敏”：权力天平的逆转

传统组织形态下，“中心”是无可争议的大脑，而“边缘”则是执行命令的神经末梢。中心负责处理信息、制定计划、下达指令，过程漫长而笨重。然而，在当今传感器遍布、信息饱和的战场上，这种模式已然失效。决策的速度和质量，已取代火力的规模，成为决定胜负的首要因素。

边缘崛起正是对这一现实的适应性进化。随着先进传感器、边缘计算、人工智能和网络化精确打击武器向一线小型单元的全面赋能，权力天平发生了不可逆转的倾斜。

感知权下放：过去的边缘单元主要是信息消费者，如今，装备了大量无人机、传感器的士兵和平台，自身就成为高效、精准的信息生产者。

决策权前置：AI 的广泛应用，使得一线单元能够处理海量数据，形成局部态势感知，并获得足以支撑自主决策的智能辅助。

行动权融合：边缘单元不再是单一功能的“螺丝钉”，而是融合了侦察、打击、干扰、评估等多种能力的多面手，具备了独立发现即摧毁的闭环作战能力。



曾经的神经末梢，正在进化为拥有独立思考和反应能力的分布式神经系统，整个战场的智能化水平，不再由中心的计算能力定义，而是由成千上万个边缘节点的集体智慧所决定。

（2）自组织：从“链”到“网”

边缘崛起的核心机制，是自组织（Self-organization）。它标志着军队的协作模式，正从基于严格命令链的刚性控制，转向基于指挥员意图（Commander's Intent）的柔性引导。

在自组织模式下，中心不再下发“一步到一步”的详尽指令，而是清晰地阐明最终的战略目标、任务边界和交战规则。被充分赋能的各边缘单元，则像一个智能蜂群，在这个“意图之网”的框架内，根据瞬息万变的战场态势，自主协同、动态补位、主动行动。

这种模式的优越性是压倒性的：

韧性（Resilience）：即使中心指挥节点被摧毁，各个边缘单元仍能依据共享的意图继续协同作战，避免整个体系陷入瘫痪。

速度（Velocity）：省去了冗长的信息上传下达链条，决策与行动在问题发生的地方被即时完成，作战节奏（OODA 循环）呈指数级加快。

涌现（Emergence）：当大量智能化的边缘单元进行自主协同，往往能涌现出中心无法提前规划的创新战术和解



决方案，实现整体大于部分之和的作战效果。

（3）敏捷适变：走向“活的”学习型组织

自组织的最终目的，是实现整个军队的敏捷适变（Agile Adaptation）。这要求军队从工业时代的层级式机构，转变为一个能够实时学习和进化的“生命有机体”。

未来的组织形态，将类似于一个开源的软件开发社区。每一个边缘作战单元，都是一个可以被灵活调用和组合的功能模块。指挥员则像一个顶级的软件架构师，根据任务需求，快速编组、部署这些模块，并在执行过程中，根据战场反馈的数据流，实时调整编组、优化战术。

这种任务式弹性编组将成为常态，固定的师、旅、团建制将被打破，取而代之的是能够根据威胁变化，在数小时内完成重构的任务部队。军队的强大，将不再仅仅体现于其规模，而更多地体现于其边缘节点的质量、网络连接的密度，以及整个组织从战场变化中学习和进化的速度。

综上，边缘崛起不仅是一场组织结构调整，更是一场深刻的军事文化革命。它要求军队高层从“控制者”转变为“赋能者”，要求信任与授权下沉到前所未有的程度。驾驭这一趋势，克服传统军事文化中的惯性阻力，将是决定未来军队能否在智能化战争中立于不败之地的关键所在。



二、概念内涵

边缘指控是一种适应未来智能化、分布式战争的指挥控制范式与运行体系，具有自任务、自组织、自行动、自适应等鲜明特征，通过分布、并行、多模态的全新过程模型颠覆经典 OODA 单循环模型。其制胜机理并非传统军事力量的线性增强，而是基于复杂科学原理的根本性革命。

2.1 定义与内涵

边缘是相对于中心而言的，可以理解为一线、前沿、基层。边缘的内涵体现在三个方面：一是力量边缘，也就是这类体系的构成成员有较高的自主和智能化水平。传统的指挥决策、交互协作、行动控制等能力被授权和分散化到底层成员；二是结构边缘，这种结构是去中心化的，不具备一个重心，而是网状结构，且边缘结构韧性十足，能够自我压缩、自我伸展，演变成各种各样的形态；三是任务环境边缘，这类体系执行的是高、远、边、深、快环境下的严酷任务。

网络信息时代之前的指挥控制主要是他组织下的中心化指挥控制模式，也是一种自上而下的指挥方式。这种指挥控制模式的特征就是力量赋予中心，它往往存在着一个重心，也即决策和行动中枢，而这个重心又与战争的进程



和胜负息息相关。这种指挥控制模式在解决确定性和静止性问题时非常有效，在相当长的时期内被指挥员广泛采用，形成了一定的思维模式。从这个意义上讲，中心化指挥控制是工业化时代指挥控制的范式，随着战争形态的改变、不确定性的凸显，以及去中心化趋势加强，传统中心化指挥控制方式、组织设计、确定的流程以及锻造并培育的关系亟待改变。如果继续单纯地按照中心化的指挥控制方式，显然难以跟上时代的发展变化。为了在边缘作战中抓住宝贵的作战窗口，传统的指挥控制范式必须与时俱进做出适当调整。因此，一个关键问题随之浮现：如果权力被分散到末端，传统的、集中式的指挥控制模式已然失效，那么未来的军队将如何被驾驭？答案就在于一种全新的指挥控制范式——边缘指挥控制（Edge Command and Control，简称为边缘指控或边缘 C2）。

边缘指控是一种适应未来智能化、分布式战争的指挥控制范式与运行体系，基于统一的作战意图、共享的战场态势、共识的作战规则，通过边缘自主协作，实现自己发现任务，并在自身能力不足时快速识别并寻找伙伴或资源，达成有效的指挥或协作关系，实现多域作战资源的按需聚合，提升指挥控制的敏捷性和适应性。

边缘指控本质上是复杂系统在应对不确定性事件时的自适应、自组织，基于宏观的确定性（战略意图清晰）来驾驭微观的不确定性（战术灵活多变），其底层是一种基



于信任的赋能哲学。它承认单一“大脑”在未来战争中的局限性，转而寻求激活群体智慧。其实践，要求指挥控制从追求“确定性的掌控”，转向拥抱“受控的不确定性”，并最终掌握在混沌边缘进行创造性引导的艺术。这不仅是战术或技术的革新，更是对军事组织与指挥文化的一次根本性重塑。边缘指控并非指挥的消失，而是指挥形态的深刻进化：从决定论式的直接操控，转向概率论式的赋能与调节。我们可以借鉴经济学中政府与市场的关系，以及复杂科学的理论来理解其内涵。

（1）作为“市场”的边缘与作为“政府”的中心

我们可以将未来的战场想象成一个高效的市场，无数个被赋能的边缘作战单元（士兵、车辆、无人机等）是这个市场中自主的经济主体。而传统的司令部（中心），则从一个无所不包的计划委员会，转型为一个提供宏观框架的服务型政府。在这种全新的“军事市场经济”中，中心与边缘的关系被重新定义：

中心负责设定市场规则，而非干预企业经营：中心的职责，不再是向每个单元下达具体的操作指令，而是制定并维护整个战场的“法律与宪法”。这包括：①明确最终意图，如同设定国家的宏观经济目标；②划定交战规则，如同设立不可逾越的法律底线；③构建通用协议，如同推广普通话和度量衡，确保所有单元间能够无障碍地交易（通信与协同）。



中心负责提供公共产品，而非包办一切生产：边缘单元无法独立承担的战略性任务，由中心作为公共产品来提供。这包括：①全球情报网络，如同国家的基础设施；②战略运输与后勤，如同国家的能源与交通动脉；③天基信息支援与战略火力，如同国家提供的终极安全保障。

中心负责担当宏观调控，而非进行微观管理：中心通过调节关键资源的流向（如高价值情报、网络带宽、特种弹药），如同央行通过利率和准备金来影响市场流动性，对战场态势进行间接的、宏观的调控，以防止出现市场失灵（如局部溃败或资源滥用）。

在这种模式下，被赋能的边缘市场主体可以基于本地信息和总体市场规则，进行最高效的自主决策与自由交易（协同），从而在整个战场上形成一只“看不见的手”，自下而上地推动战局走向胜利。

（2）指挥员角色的转变：“培育”而非“规划”

如果说政府与市场的关系描述了边缘指控的外部结构，那么复杂自适应系统（Complex Adaptive Systems, CAS）理论则揭示了其内部的运转逻辑。

战场上的无数边缘单元，就是典型的自适应主体（Adaptive Agents）。边缘指控的核心，并非为这些主体设计一张精密的行动蓝图，而是为它们创造一个能够自我演化的生态花园。

遵循简单规则的复杂行为：指挥员不再需要设计复杂



的总体方案。取而代之的是，为边缘单元设定若干简单规则。例如，“发现任何符合特定信号特征的敌方目标，均可自主呼叫距离最近的火力单元进行打击”；“任何单元若失去与友邻的联系超过 2 分钟，则自动向备用节点回传信息”。正是这些被植入每个主体的简单规则，在成千上万次相互作用中，能够涌现出极其复杂、精妙且难以预测的宏观战术行为。

追求涌现秩序而非强加秩序：指挥员的目标，是培育而非规划。通过设定初始条件和互动规则，让最优的作战方案从边缘的集体智慧中自发涌现出来。这种涌现秩序远比任何中心化的顶层设计都更具韧性、适应性和创造力。

2.2 “四自”特征

边缘指控具有四个紧密相连的核心特征：“自任务、自组织、自行动、自适应”，如图 2-1 所示。这“四自”特征，共同勾勒出未来战场上，边缘力量如何从被动的棋子转变为主动的棋手。



图 2-1 边缘指控的“四自”特征

(1) 自任务 (Self-Missioning)：基于意图的机遇发现

自任务指的是边缘单元在深刻理解上级指挥意图的框架下，不再被动等待具体指令，而是主动发现并利用战场机遇，为自身生成任务的能力。这是从“被动执行”到“主动寻战”的根本转变。

传统的命令链中，任务是自上而下严格分派的。但在瞬息万变的智能战场，战机往往稍纵即逝，等待中心下令意味着错失良机。在边缘指控模式下，指挥员的核心工作是确保每位边缘成员都像他自己一样，理解战局的“为什么”。一旦边缘单元通过自身传感器（如无人机、声学传感器）发现了一个未被上级标定的、但对实现总体意图具有重大价值的目标（如一个意外暴露的敌方指挥员、一个关键的通信中继站），它有权也有责任立即将其作为优先任务进行处理。



案例：一支在城市区域执行扰乱敌方补给线的特战小队，其装备的微型无人机侦测到一幢民居楼顶出现了非正常的、高功率的通信天线。尽管这并非其预定任务清单中的目标，但小队指挥员判断这极有可能是敌方的临时指挥所，摧毁它对扰乱补给这一核心意图的贡献，远大于攻击一辆普通的补给卡车。因此，他自主决定将摧毁该潜在指挥所作为小队的当前首要任务。

（2）自组织（Self-Organization）：跨域资源的即时重组

自组织是指不同的、无预设隶属关系的边缘单元，为了一个共同的临时任务，能够跨越建制、跨越领域，快速、自发地形成一个临时的作战网络。这如同一个军事版的滴滴平台，需求方（发现任务的单元）发单，能力方（空闲或合适的单元）自动接单并组队。

实现自组织的前提是，所有边缘单元都成为网络中标准化的即插即用节点，并共享一套通用的通信协议与数据格式。当一个单元的能力不足以完成其自任务时，它可以向网络广播一个带有明确目标、所需能力标签的协作请求。网络中的其他单元（无论是友邻的步兵、空中的无人机群、远方的炮兵，还是网络空间的攻击小组）的系统会根据自身位置、状态和能力，自动评估并响应请求，瞬间形成一个最优的任务突击群。

案例：前述的特战小队决定攻击楼顶天线，但自身火



力不足。队长通过战术网络，向周边区域广播了一个“需要非直瞄精确火力与电子干扰”的请求。数秒内，附近一架游弋的武装无人机、一个后方炮兵阵地的智能火炮系统，以及一个网络战分队的电子压制模块，同时接单。它们瞬间自发组织成一个临时火力团队，共享目标数据，协同进行攻击。

（3）自行动（Self-Action）：基于规则的即时响应

自行动特指在人机协同的框架下，边缘作战单元在预设的交战规则内，执行部分战术动作的自主权，从而将指挥员从重复、繁琐，且对速度要求极高的战术决策循环中解放出来，专注于更宏观的判断。

指挥员的角色是规则制定者，预先设定好“在何种区域、针对何种特征的目标、在何种情况下、可以采取何种行动”的精细化规则。被赋予这些规则的边缘作战单元，一旦发现符合全部条件的目标，便能在机器辅助下快速完成识别、锁定、打击的流程。

案例：炮兵系统的 AI 在接到协同请求后，根据人类指挥员预设的最小附带毁伤规则，自主计算出最优的攻击弹道和弹药类型。同时，协同的武装无人机在进入指定攻击阵位后，其火控系统根据“仅攻击带有特定信号特征的非民用目标”的规则，自主锁定了楼顶的天线而非旁边的民用水箱，并在得到人类的最终授权或是在特定授权开火区域内，执行打击。



（4）自适应（Self-Adaptation）：源于数据的实时进化

自适应是指整个作战网络利用战斗中产生的实时数据，进行动态学习、修正战术，并快速进化的能力。战场不再仅仅是执行计划的地方，更是一个产生数据、迭代认知的学习实验室。

每一次攻击、每一次防御、每一次成功、每一次失败，都会被量化为数据流，在网络中高速传递。当一种战术被证明无效（如某种弹药被敌方新型防御系统拦截），该信息会立刻被标记并分享给所有相关单元。系统会立刻推荐或自主切换到备用战术。这种基于实时战况的集体学习和快速迭代，使得整个作战体系表现出强大的韧性和反脆弱性。

案例：炮兵的第一发炮弹被楼顶新出现的某种主动防御系统拦截。拦截事件的数据（弹道、被拦截位置、敌方防御系统特征）瞬间传遍整个临时火力团队。无人机捕捉并识别了该防御系统的型号，炮兵 AI 立即根据该型号的弱点，自主适应并重新规划了攻击方案——改用两发炮弹、以不同弹道、在极短时间间隔内进行饱和攻击，最终成功摧毁目标。

自任务、自组织、自行动和自适应，这“四自”特征，共同构成了一个完整的、从机遇识别到任务完成再到学习提升的闭环。它们环环相扣，将传统的、机械的军事机器，



改造为一个分布式的、充满活力与智慧的活系统，从而在未来战争的复杂与混沌中，赢得制胜先机。

2.3 涌现与反馈控制：双模过程模型

传统的军事行动，其过程模型被约翰·博伊德的 OODA 环（观察—判断—决策—行动）所主宰。这是一个线性的、封闭的、以单个决策者（无论是飞行员还是司令部）为核心的循环。其制胜逻辑在于，比对手更快地完成这个循环。然而，在边缘指控的体系下，这个经典的单核循环模型正在被一个分布式的、并行的、多模态的全新过程模型所颠覆。

（1）OODA 环的解体与重构

边缘指控并非简单地加速 OODA 环，而是从根本上将其解构并网络化重构：

观察无处不在：观察不再是一个独立的起始步骤，而是整个网络所有节点（士兵、无人机、传感器）持续不断进行的环境状态。信息从定时采集变为实时获取。

判断多层并发：判断不再是中心大脑的专有权力。边缘 AI 对局部威胁进行战术判断，中心 AI 对全局态势进行战略判断，而共享的数据平台则确保所有层级的判断都基于一个共同的、不断刷新的认知基础。

决策按需分配：决策权被彻底打散。中心负责战略意图、交战规则等顶层框架决策；边缘单元负责人机协同下

的战术决策；而机器则负责在规则内的高速执行决策。决策点被动态分配给网络中最适合的位置。

行动协同涌现：行动不再是单一指令下的个体执行，而是多个边缘单元自组织协同后，所产生的集体活动。

这种解构，催生了一个远比 OODA 环复杂的复杂适应系统。它并非单一循环，而是根据任务性质和实时战况，在两种主要的过程模型间动态切换与融合。

（2）过程模型一：“意图—涌现”循环（The Intent-Emergence Loop）

这是一种认知驱动、任务导向的循环，如图 2-2 所示，主要用于处理复杂、模糊、需要人类创造力与智慧的非对称场景，体现了自任务与自组织的精髓。



图 2-2 “意图—涌现”循环

1. 意图（Intent）：循环的起点。指挥中心发布并共享一个清晰的、目标导向的宏观意图，而非具体行动计划。



2.洞察(Insight)：边缘单元基于自身独特的局部观察，结合对上级意图的理解，洞察到稍纵即逝的、非预期的战机或威胁。

3.组织(Organize)：洞察到机遇的单元，立即发起一个“自任务”，并向网络广播协作需求，自发、快速地与其他可用单元（人或机器）组成一个临时的、最优的任务群组。

4.涌现(Emerge)：这个临时群组通过协同行动，达成了一个超越个体能力之和的、创造性的作战效果，从而实现了最初的宏观意图。这个结果是涌现的，而非预先规划的。

这个循环的核心是“慢思考、快协同”，它将人类的战略直觉和创造性（洞察与意图理解）与网络的快速重组能力结合，以应对不确定性。

（3）过程模型二：“规则—执行”循环（The Rule-Execution Loop）

这是一种数据驱动、条件触发的循环，如图 2-3 所示。其本质是一个高速的负反馈回路，主要用于处理明确、高时效性、可被预先定义的确定性威胁。它体现了自行动与自适应的精髓。



图 2-3 “规则—执行”循环

1.规则（Rule）：循环的预设条件。指挥员预先将交战规则、目标识别特征、威胁等级等，以“If... Then...”的逻辑，转化为机器可以理解的算法，植入武器与传感器系统。

2.刺激（Stimulus）：一个外部事件（如传感器探测到符合规则的敌方导弹信号）直接触发了循环。

3.响应（Response）：系统几乎没有时延地自动执行预设的应对动作（如启动电磁干扰、发射拦截弹）。判断与决策步骤在制定规则时已被预先完成，因此该循环的速度取决于数据传输和物理执行的速度。

4.适应（Adapt）：行动的结果（成功或失败）会作为新的数据输入，实时更新整个网络的威胁数据库和战术模型，从而优化下一次响应的规则。

这个循环的核心是“零思考、即刻行动”，它将人类的战术经验固化为机器算法，以换取宝贵的反应时间，应

对发现即摧毁的高速对抗。

（4）双模过程模型

边缘指控的过程模型，将是一个“意图—涌现”与“规则—执行”双模并存、无缝切换的复杂系统，如图 2-4 所示。

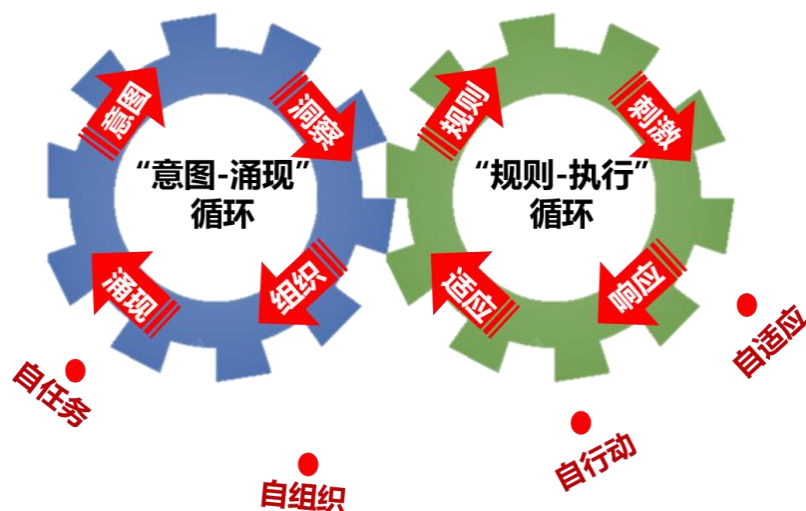


图 2-4 双模过程循环

指挥员的艺术，不再是拼命加速自己的 OODA 环，而是要成为一个高明的“系统切换师”：在需要创造力时，激活“意图—涌现”循环，以应对复杂；在需要速度时，相信并授权“规则—执行”循环，以赢得时间。这种双模驱动的过程，才是未来战争中实现决策优势的核心要义。

2.4 面向适应性优势的三重制胜机理

边缘指控的制胜机理，并非传统军事力量的线性增强（更快的速度、更强的火力），而是一种基于复杂科学原理的根本性范式革命。它不再追求成为一部完美、高效、



但脆弱的“战争机器”，而是致力于构建一个坚韧、智能且能够持续进化的“战争生命体”。其制胜机理源于其在三个核心维度上，对传统层级化军队形成了压倒性的适应性优势。

（1）反脆弱性：在混乱与打击中自我增强

传统军队是脆弱的。高度集中的指挥中心、通信枢纽和后勤节点，是其力量的源头，也是其致命的弱点。一旦这些大脑和心脏遭到打击，整个体系便可能陷入瘫痪。因此，传统军事思想的核心之一，是尽力保护这些节点，规避风险与不确定性。

而边缘指控体系则具备了复杂系统中一种极为宝贵的特性——反脆弱性（**Anti-fragility**）。它不仅仅是坚固或有韧性（即受到打击后能恢复原状），而是能够从混乱、压力和失败中汲取养分，变得更为强大。

其机理在于，每一次小规模受挫，对于整个分布式网络而言，都是一次宝贵的学习事件。当一个边缘单元的攻击被拦截、一条通信链路被干扰、一种战术被识破，这些失败数据会瞬间传遍全网。这相当于对整个系统进行了一次低成本的压力测试或免疫接种。网络中的其他单元会立刻将这些信息纳入决策分析，调整自身的行为模式，从而避免在更大范围内重蹈覆辙。敌人的每一次成功打击，都像一次疫苗注射，不仅无法摧毁这个分布式系统，反而激发了其集体免疫力，使其变得更加警觉、更富经验、更



难对付。它将整个战场，变成了自身的进化熔炉。

（2）必要多样性：以无穷的变化应对无穷的复杂性

复杂科学中的艾什比定律（Ashby's Law of Requisite Variety）指出：一个系统要想有效地控制另一个系统，其自身必须拥有不亚于对方的复杂性或多样性。战场，无疑是世界上最复杂的系统之一。

传统军队的多样性是有限的。其标准化的建制、层级化的指挥链，决定了其战术动作和应对模式，在根本上是可预测、可被穷举的。它试图用有限的、固化的最优解，去应对战场上无穷的、流变的问题集。

边缘指控体系则通过自任务与自组织，创造了近乎无穷的必要多样性。成千上万个具备多种能力、被赋予高度自主权的边缘节点，可以根据实时战况，排列组合成天文数字般的临时任务编组。这意味着，面对敌人的同一种威胁，边缘指控体系可以在同一时间，从不同维度、用不同方式，生成数百种乃至数千种不同的应对方案。这种以“多样性”对“多样性”，以“不确定性”对“不确定性”的策略，使得任何试图预测其行为对手，都会迅速陷入认知过载。它不是靠单一的杀手锏取胜，而是靠源源不断、出其不意的战术流淹没对手的应对能力。

（3）适应性引导：在动态博弈中寻找确定性窗口

我们可以将战争的态势想象成一个不断起伏、变形的“适应性景观（Fitness Landscape）”。地势的高峰，代表



着战术上的优势地位或最优解决方案。

传统军队的作战模式，如同一个登山队，在战前通过精心计算，选定一座自认为最高的“山峰”（即作战计划），然后倾尽全力、沿着预定路线向上攀登。但战争的残酷在于，这座山峰可能随时下沉，或者旁边会隆起一座更高的山峰。此时，笨重的登山队想要掉头转向，已是难上加难。

而边缘指控体系，则如同一个遍布整个景观的探索者蜂群。每一个边缘单元都在进行着小范围的、低成本的试探性攀登。它们不断探测周边的地势，一旦某个单元发现了一个更高的局部山峰（一种更有效的战术、一个未被发现的弱点），这个成功的信息就会像一种信息素，迅速吸引周边的其他单元向这个新的优势区域聚集。因此，整个蜂群能够始终、动态地、自发地向着景观中不断涌现的更高峰流动。它不执着于任何一个固定的计划，而是永远在进行着一场以整个战场为范围的、实时的“当前最优解”搜索，从而确保自身在长期消耗与动态博弈中，始终占据着适应性的高地。

综上所述，边缘指控的制胜机理，是通过适应性调节与分布式协调，引导系统从混沌边缘向目标有序演进，从而获取优势的过程。它以“反脆弱性”为生存之本，以“必要多样性”为博弈之术，以“适应性引导”为演化之道，最终实现以适应性本身，作为战胜对手的最根本武器。



三、实现途径

边缘指控的实现，首要在于指挥方式的转变，即从传统的基于预先设定的指挥关系，转变为动态临机授权的指挥方式。网络信息技术是实现这种动态变化的基石，开放共享是这一转变所依赖的全新理念，协同规则则是转变后实现导向性涌现的源泉。

3.1 动态授权：指挥方式的重塑

指挥方式的转变，是理解边缘指控革命性意义的关键所在。这不仅是技术的更迭，更是一场深刻的组织哲学与权力关系的重塑。

传统军事体系的灵魂，在于其固定、静态、与组织结构图严格绑定的指挥关系。权力从金字塔的顶端，沿着清晰的脉络逐级下放，壁垒分明，不可僭越。一名连长指挥其下的排长，一名营长指挥其下的连长，这种关系如物理定律般稳定。指挥权是职位赋予的、恒定的属性。然而，这种建立在工业时代大规模、同质化作战背景下的指挥模式，在今天瞬息万变、能力异构的智能战场上，已从力量的倍增器，沦为制胜的枷锁。

其弊病在于三大“错配”：

（1）速度错配：当发现即摧毁的窗口被压缩至秒级，



信息沿着漫长指挥链上传下达的往返时间，已经长到足以埋葬任何战机。

(2) 能力错配：战场上，最先发现威胁的侦察兵，身边往往没有最适合应对该威胁的武器；而掌握最强火力的作战单元，又往往远离信息源头，看不见、听不清。固定的指挥关系，在最优的传感器与最优的射手之间，筑起了一道难以逾越的障碍。

(3) 韧性错配：对关键指挥节点的过度依赖，使得整个作战体系极其脆弱。一旦高级指挥员阵亡或司令部被毁，下级部队便可能群龙无首，陷入瘫痪。

为了打破这些桎梏，边缘指控的核心，就是实现指挥权的解耦与流动，即指挥权不再与某个固定的职位绑定，而是根据任务的需求，进行动态、临机的授权与聚合。

3.1.1 从静态身份到动态授权：指挥权的新范式

在边缘指控的范式下，指挥权本身，从一种身份属性，转变为一种可以被按需分配、有时效性、有范围限制的數字凭证或临时权限。这种转变催生了两种核心机制：

(1) 指挥即服务 (Command as a Service, CaaS)

这个概念借鉴了云计算的软件即服务 (SaaS)。它意味着，指挥能力本身，可以被封装成一项可供全网调用的服务。

服务提供者：高级指挥员（如战区司令）。他不再直接指挥每一个具体行动，而是作为平台所有者，负责提供



最高阶的指挥服务。这项服务的内容包括：发布清晰的、所有人都可理解的作战意图；设定全局性的交战规则与法律/道义底线；提供强大的战略性公共产品（如天基情报、网络主导权等）。

服务消费者：任何一个需要为达成总体意图而采取行动的边缘作战单元。当一个边缘单元发现一个战机，但需要调动不属于其建制的资源时，它就可以向网络发起一个指挥服务申请。

（2）临机授权（Ad-Hoc Authorization）

这是实现指挥即服务的具体操作机制。当一个边缘单元（如深入敌后的一支特战小队）发现了高价值目标（如敌方机动导弹发射架），但需要一架不属于其指挥体系的重型轰炸机进行打击时，传统的流程是层层上报，耗时耗力。

而在临机授权模式下，流程被彻底颠覆：

①认证与请求：该特战小队队长通过其加密的战术终端，向网络发送一个经过数字签名的火力请求。该请求中包含了目标的实时数据、位置，并附带了其行动符合最高指挥意图的“认证标签”。

②验证与授权：网络中的指挥 AI 或拥有更高权限的人类指挥员，会立刻对该请求进行验证。验证的内容包括：请求者的身份是否可信（信任即协议）？其提供的目标数据是否与网络中其他传感器的数据交叉印证？该行动是否



在预设的交战规则框架内？一旦验证通过，系统会即时生成一个临时的、动态的指挥授权。

③权力转移：在接下来执行本次打击任务的几分钟内，那架重型轰炸机（及其飞行员）在战术层面上的指挥权，就临时、动态地从其原有的空军指挥链，转移到了地面上那位特战小队队长的手中。因为在这一瞬间，他才是全场最了解目标情况、能最好地引导攻击的人。

④授权终止：任务完成或中止后，该临时指挥授权自动失效，轰炸机回归其原有指挥链。

通过这种方式，最优的传感器和最优的射手被以任务为中心，瞬间聚合在一起，形成了一个临时的、高效的指挥关系。指挥权，如同学术会议中的主持人身份，在不同议题下，可以动态地交给最适合的专家。

3.1.2 案例分析：俄乌冲突中的指挥方式对比

2022 年以来的乌克兰战争，尽管并非边缘指控的完美样板，但其诸多实践，却清晰地映照出这种新型指挥方式的巨大潜力，并与俄军僵化的指挥模式形成了鲜明对比。

俄军的困境——静态指挥的失败：俄军在战争初期，严格遵循自上而下的传统指挥模式。其营级战斗群虽有理论上的合成化，但由于缺乏真正的授权文化和横向协同能力，导致各兵种间配合脱节。指挥链的僵化和信息传递的迟滞，使得部队无法应对乌军灵活的、分布式袭扰。大量俄军高级将官被迫亲临一线去推动停滞不前的部队，从而



导致惊人的阵亡率，这正是静态指挥模式在分布式协同、快速决策的战场上失能的极端体现。

乌军的创新—动态指挥的雏形：面对强敌，乌军在北约支持和自身创新下，采用了大量接近边缘指控核心思想的打法。

（1）“去中心化”的授权文化：乌军在很大程度上将作战自主权下放给了一线的小型、机动分队。这些分队在获得一个大致的作战区域和目标意图后（如“在基辅北郊迟滞俄军推进”），被允许以极大的灵活性自主选择目标、规划路线、呼叫火力。

（2）“数字游击战”中的临机协同：乌军大量使用 Signal 等加密商业软件，以及自研的 Kropyva（GIS Art for Artillery）等战术应用，让分散的侦察单位（包括特种兵、普通步兵乃至平民志愿者）、无人机操作员和炮兵单位，能够绕过传统的指挥层级，建立起扁平化的传感器-射手网络。一个在前线用商用无人机发现目标的士兵，可以通过手机应用，近乎实时地将目标坐标和视频流，直接发送给后方的炮兵阵地。在这一刻，这个士兵就对炮兵实施了一次事实上的临机引导与授权。

（3）跨域能力的即时聚合：一个典型的场景是，乌军一个步兵小组用无人机发现俄军一支装甲纵队，他们立即通过网络呼叫支援。几分钟内，附近的另一支携带“标枪”导弹的小组、更远处的炮兵以及在空中盘旋的 TB2 无人机，



就可能对该纵队发起一次多维度、饱和式的协同打击。这些单位分属不同建制，但在任务需求的牵引下，动态聚合成一个临时的、致命的火力集群。

从固定到动态，从身份赋予到临机授权，这场指挥方式的革命，其本质是将权力从僵化的层级式指挥结构中解放出来，使其能够像战场信息一样，高速、精准地流向最需要它的节点。乌克兰战场的实践，以一种残酷而真实的方式预演了未来：那些能够构建信任协议、实现指挥权按需流动、让一线“听得见炮声的人”拥有最大决策权的军队，将在适应性上获得决定性优势。而那些固守于工业时代权力金字塔的军队，即便拥有强大的装备，也将在未来“活”的、分布式的战争体系面前，变得不堪一击。

3.1.3 指挥方式转变的难点

指挥方式从静态向动态的转变，也意味着传统的“控制型”指挥向“赋能型”边缘指控的转型，其过程远比装备技术的更新换代更为艰难。真正的壁垒并非铺设更快的网络或部署更强的 AI（硬件），而是对军队数百年形成的组织文化、心理定势与制度体系（软件）进行一次痛苦的“基因重组”。其主要难点，集中体现在三个层面：

（1）文化上的“控制悖论”

军事文化的核心，长期建立在“层级、服从、确定性”的基石之上。指挥员的权威，体现在其对下属和战局的“绝对控制力”。然而，边缘指控的精髓，却要求指挥员主动



“放弃控制”，将决策权下放给充满不确定性的一线。这构成了一个深刻的文化悖论：在新的战争范式下，你越是想通过传统的中心化手段去控制一切，就越会因为反应迟缓而失去对战局的真正控制。反之，通过赋能与授权，在宏观上放手，反而能在微观上获得更强的适应性与掌控力。要让习惯了“一切尽在掌握”的指挥文化，去拥抱这种合理放权的方式，是一场极其困难的认知革命。

（2）心理上的“双重壁垒”

转型在心理层面，同时为高级指挥员与一线指挥员（士兵）设下了壁垒。

高级指挥员的“授权恐惧”：要求一位将职业生涯建立在承担责任之上的指挥员，将生死攸关的决策权，交给一位素未谋面、仅靠数据和协议建立信任的下级，这在心理上会引发巨大的不安全感和对失能的恐惧。一旦授权后出现失败，责任归属的模糊性，会成为悬在每位指挥员头顶的达摩克利斯之剑。

一线指挥员（士兵）的“决策重担”：长期被训练精准执行命令的一线指挥员（士兵），被突然推到前台，要求他们独立分析、判断、并承担决策后果，这同样是巨大的心理压力。从“执行者”到“决策者”的角色转换，对他们的知识结构、心理素质和风险承受能力，都提出了前所未有的要求。

（3）制度上的“系统惯性”



军队是一个庞大而精密的制度体系，其惯性巨大。边缘指控的实现，需要对整个系统运作进行重塑。这包括：彻底改写以集中控制为核心的作战条令；颠覆以按计划执行为目标的训练与演习模式，转向模拟高度不确定的复杂对抗；以及改革最为核心的人事晋升与评估体系。如果一个组织，仍然主要提拔那些最擅长上传下达和按部就班的军官，那么任何关于赋能与授权的口号，都将沦为空谈。如何建立一套能够识别、培养并奖励具备设计师而非建筑师特质的新型指挥人才的制度，是转型能否成功的根本保障。

综上，这场指挥方式的转型，本质上是一场关于信任的革命——如何构建人与人、人与机器之间，基于数据和协议的、可大规模复制的信任。这远比任何技术攻关都更加复杂，也更加深刻。

3.2 网信支撑：“活系统”的基石

实现从控制到赋能的指挥方式革命，绝非仅靠理念更新就能完成。它必须建立在一个高度发达、智能且坚韧的技术底座之上，如图 3-1 所示。这个技术体系的目标，是打造一个能够支撑“自任务、自组织、自行动、自适应”的分布式“战争生命体”。



图 3-1 边缘指控的网信支撑

3.2.1 网络：坚韧自愈的连接

边缘指控的首要，也是最基础的前提，是连接（Connectivity）。如果边缘节点之间无法有效通信，任何协同与自组织都无从谈起。未来的战场网络，必须具备两大核心特征：

多层立体的泛在连接：它不再依赖于单一的通信链路，而是由多个层次、多种手段构成的混合网络。这包括：由数千颗低轨道卫星（如星链）组成的、提供全球覆盖和低延迟服务的天基网络；由 5G/6G 技术赋能的、提供区域高带宽服务的地面战术网络；以及由无人机群、战车、单兵组成的，能够在无中心节点情况下动态组网的移动自组网（MANETs）。这三层网络相互备份、无缝切换，确保即使在部分节点被毁、部分频谱被干扰的恶劣环境下，边缘



单元依然永远在线。

智能自主的弹性自愈：网络本身必须是智能化的。它需要具备自主路由与流量管理能力。当某条链路受到攻击或出现拥塞时，网络协议能够像 GPS 导航重新规划路线一样，在毫秒之内自动寻找并切换到最优的备用链路，对边缘用户做到攻击无感。这种自我修复能力，是整个作战体系反脆弱性的技术根源。

3.2.2 云计算：无处不在的计算

如果网络是神经，那么云计算技术，特别是战术边缘云（Tactical Cloud at the Edge），就是分布于全身可随时取用的“外置大脑”。

传统的云计算将所有数据和算力集中在后方大型数据中心，这在战术上是不可接受的。边缘指控所依赖的，是一种“云-边-端”协同的架构：

战略云（国家级）：负责存储海量历史数据、训练复杂的 AI 基础模型、进行全局战略推演。

战役云（战区/战役级）：部署在战区内的前沿基地或大型平台上（如舰船、预警机），提供区域性的数据融合与协同服务。

战术边缘计算节点：将强大的计算和存储能力，前置到作战的最末端——战车、无人机乃至单兵的战术终端上。这使得 AI 推理、目标识别、威胁评估等任务可以在本地高速完成，无需将原始数据回传后方，极大地降低了对网络



带宽的依赖，并实现了近乎瞬时的反应能力，是自行动和自适应的技术前提。

3.2.3 安全：“零信任”架构下的验证

当指挥权被下放、数据被共享，安全问题便上升到前所未有的高度。传统的、基于边界防御的护城河式安全模型已彻底失效。边缘指控的安全基石，必须是“零信任”架构（Zero Trust Architecture, ZTA）。

零信任的核心思想是“从不信任，永远验证”。它不因用户处于网络内部就给予其信任，而是对每一次的数据访问、每一次的操作请求，都进行严格的、持续的身份验证与权限检查。

强化的身份认证：每个士兵、每台设备、每个 AI 代理，都有一个基于密码学、生物特征等多因素的、不可伪造的数字身份 ID。

最小权限原则：每个数字身份仅被授予完成其任务所必需的最小数据访问和操作权限。

微隔离：网络被分割成无数个微小的区段，即便一个区段被攻破，攻击也无法横向蔓延到其他部分。

这种架构，为我们之前提到的信任即协议和临机授权提供了技术实现。一个高级指挥员之所以敢于将一架轰炸机的控制权临时交给一个素未谋面的下士，就是因为零信任体系能够确保这个下士的身份、权限和请求，都是经过了严格技术验证的、可信的。



3.2.4 数据：按需流动的资源

在边缘指控体系中，数据不再是孤立的信息，而是像血液一样，在整个网络中按需、无差别流动的核心资产。实现这一点，需要构建一个联合全域数据编织。

数据编织是一种智能化的数据管理架构，它不去强求将所有数据都集中到一个物理位置，而是通过建立统一的数据目录、标准和接口，让被授权的用户和 AI，可以随时发现、访问、融合分布在任何地方的数据。一个在前线的士兵，可以无缝调用一架在高空的无人机所看到的热成像数据，并将其与后方情报部门提供的历史数据进行叠加分析。数据在这种架构下，从固态的信息孤岛，变为液态的、可被任意组合的战略资源，为所有层级的判断与决策提供养分。

3.2.5 智能：数字生命体的决策引擎

如果说网络是神经连接，云计算是外置大脑，数据是血液，那么人工智能（AI），就是注入这个数字生命体的决策引擎。智能并非一个孤立的功能模块，而是作为一种基础能力，深度嵌入到网络、计算、数据、安全、软件等每一个环节，赋予整个边缘指控体系以感知、理解、预测、协同乃至进化的能力。其核心作用主要体现在以下几个方面：

赋能感知理解：从“看见”到“看懂”。海量的原始传感器数据本身并非情报，而 AI 的作用，就是将这些来自



无人机、传感器、士兵的、碎片化的原始数据，实时地转化为可被理解、可被行动的战术洞察。它通过目标识别、行为分析、模式挖掘等算法，自动地从嘈杂的背景中识别出高价值目标、预测敌方意图、并发出预警。这是实现分布式判断功能，为自任务提供决策依据的根本前提。

驱动决策规划：从“辅助”到“生成”。AI 不仅是人类指挥官的参谋，更是能够自主生成方案的规划师。它能够根据指挥官设定的作战意图（目标函数），结合实时战场态势，在百万种可能性中，快速计算并推荐出最优的模块组合与行动序列。在“规则—执行”循环中，它更是能够基于预设规则，直接驱动武器平台完成发现即摧毁的自主行动，将决策与行动的延迟压缩至极限。

优化协同涌现：从“连接”到“编织”。在自组织过程中，AI 是那个“看不见的手”。它扮演着市场调度官的角色，运行着火力竞标、空间拍卖等协议，确保最优的传感器与最优的射手能够被瞬间、高效地匹配在一起。它将一个由无数独立单元构成的网络，从简单的连接状态，提升为一个能够根据任务，实时、动态地编织出最优作战形态的、高效的杀伤网。

加速学习进化：从“事后复盘”到“实时适应”。AI 是整个体系能够成为“活的”学习型组织的核心引擎。它通过对每一次成功与失败的战斗数据进行深度学习，不断迭代和优化自身的威胁模型、战术算法和协同规则。这种



由 AI 驱动的、近乎实时的“学习—适应”循环，使得整个作战体系能够从每一次与敌人的互动中汲取养分，实现“反脆弱性”，在炮火中完成快速的、集体性的进化。

智能化支撑的最终目标，是构建一个人机融合的“集体智能”（Collective Intelligence）。在这个体系中，人类的经验直觉与 AI 的强大算力深度融合，共同构成一个既能进行高速优化计算，又能处理复杂不确定性、并能持续学习演化的超级智能体。

3.2.6 软件：软件工厂与应用商店模式

未来的军事能力，将越来越多地由软件而非硬件来定义。为了支撑敏捷适变的作战需求，软件的开发与部署模式必须进行革命，核心是引入“开发—安全—运维一体化”（DevSecOps）的理念和军事软件工厂的模式。

持续迭代的软件工厂：借鉴硅谷经验，军队建立自己的软件工厂（如美国空军的 Kessel Run），由军人、政府雇员和承包商组成混合团队，以敏捷开发的方式，在数周甚至数天内，就能完成一款新软件（如一个新的目标识别算法、一个改进的协同工具）的开发、测试与部署。

容器化与 API 优先：软件被打包在容器（如 Docker）中，使其可以脱离底层硬件，在任何系统（从云端到边缘）上运行。同时，所有功能都通过标准化的应用程序接口（API）来提供，这让不同的软件、系统之间可以像积木一样轻松地相互调用和组合，是实现自组织的技术黏合剂。



3.2.7 标准化：开放架构下的通用语言

以上所有技术的融合，都离不开一个最终的，也是最关键的基础——标准化。美军近年来大力推行的模块化开放系统架构（**Modular Open Systems Approach, MOSA**），正是这一思想的体现。

标准化的目标是打破不同军种、不同承包商之间的技术壁垒，确保所有硬件和软件都遵循共同的接口标准、数据格式和通信协议。这如同规定了整个国家的官方语言和插座标准。只有实现了高度的标准化，A 公司的无人机才能无缝地将数据传递给 B 公司的火炮系统，C 公司的 AI 算法才能运行在 D 公司的战术计算机上。这是实现跨域能力即时重组的先决条件，也是边缘指控体系能够真正成为一个高效整体，而非一盘散沙的根本保证。

这七大技术支柱，共同构建了边缘指控得以实现的物质基础。它们相互交织、缺一不可，共同将一支军队，从一个由齿轮和杠杆构成的、僵硬的机械集合体，转变为一个由神经、血液、免疫系统和学习能力构成的、充满智慧与韧性的数字生命体。这场深刻的技术变革，正是未来战争制胜机理的底层代码。

3.3 开放共享：指挥控制的新理念

如果说动态临机授权是边缘指控在权力关系上的革命，那么根植于体系每一个角落的开放与共享理念，则是支撑



这场革命得以发生，并确保其不至于崩溃的、更深层次的技术源代码与文化世界观。任何脱离了开放共享的边缘赋能，都将是无源之水、无本之木，最终只会形成一个个更小、更混乱的信息孤岛，而非一个强大、智能的作战网络。

3.3.1 开放共享：赋能边缘指控

边缘指控的活力，源于其自任务、自组织、自行动、自适应的“四自”特征。这四大特征并非孤立存在，其每一步的实现，都以开放共享为前提。

开放共享赋能自任务：一个前线单元之所以敢于自主生成任务，其信心来源并非单纯的勇敢，而是基于对全局意图的深刻理解。这要求它能够通过一个开放的数据架构，无缝共享到更高层级的指挥意图和覆盖整个战场的态势图。只有将本地的“我看到了什么”与全局的“大家看到了什么”以及顶层的“我们要做什么”进行比对，它才能判断出自己发现的这个新机遇，究竟是无价值的干扰，还是足以改变战局的关键节点。没有这种开放共享的“上下文”，自任务就是危险的无的放矢。

开放共享赋能自组织：不同军种、不同建制的单元之所以能自组织成一个临时的作战团队，其技术基础是开放的通用标准。这包括通用的通信协议、数据格式，以及标准化的应用程序接口（API）。当一个陆军特战队员需要空中火力支援时，他不是去联系某个特定的飞行员，而是在网络中广播一个标准化的火力支援服务请求。任何符合条



件的、来自空军或海军的、空闲的攻击机，都能像网约车接单一样听懂并响应这个请求。这种即插即用式的协同，只有在所有参与方都遵循模块化开放系统架构，共享同一套语言和接口规范时才能实现。

开放共享赋能自行动：机器之所以被信任可以自主行动，是因为它所遵循的决策逻辑是完全透明并被全网共享的。指挥员通过一个开放的平台，设定并实时更新机器可以遵循的交战规则与行为算法。边缘单元在行动前，会基于一个共享的、由全网传感器共同维护的、可信的敌我识别数据库进行判定。指挥员的信任，并非给予某个“黑箱”AI，而是给予这个开放、透明、共享的“规则—数据”验证系统。信任由此从感性的个人关系，转变为理性的技术协议。

开放共享赋能自适应：整个作战体系之所以能自我适应，是因为它建立了一个开放共享的学习机制。任何一个边缘单元的成败经验，都会被作为标准化的数据包，立刻共享到整个网络的数据湖中。后方或云端的AI模型会实时分析这些海量数据，一旦发现某种敌方战术或我方弱点，便会立刻生成应对策略或改进算法，并将其开放给所有节点进行系统升级。A部队的牺牲，能够立刻转化为B部队的能力提升，整个体系在炮火中共享式地学习和进化。

3.3.2 案例分析：2025年5月印巴冲突

2025年5月上旬，因克什米尔地区的恐怖袭击，印巴



之间爆发了激烈的武装冲突。这场冲突持续时间不长，但其展现出的技术对抗形态，为我们观察“开放共享”的实战价值，提供了一个极为严酷且清晰的最新案例。

（1）印方之困：万国牌装备的体系性内耗

此次冲突中，印度武装部队动用了其几乎所有最先进的装备，包括法制阵风、俄制苏-30 战斗机，以及首次大规模使用的布拉莫斯和 SCALP-EG 巡航导弹。然而，在冲突的开端，特别是 5 月 7 日的空中对抗中，印方据报遭受了不成比例的损失，巴方宣称击落了包括阵风在内的多架战机。

核心问题在于体系的封闭与不兼容。尽管印度拥有众多先进平台，但这些来自不同国家、基于不同技术标准的瓦片，始终未能有效地拼接成一幅完整的“马赛克画作”。

1.数据链的不兼容：苏-30、阵风、本土预警机、以色列无人机，各自使用着独立甚至相互不兼容的数据链。这导致在激烈的多机对抗中，信息无法高效、无缝地共享，难以形成统一、可信的战场态势图。飞行员可能需要依赖语音等低效方式进行协同，这在超视距空战中是致命的。

2.传感器-射手链路的断裂：分析指出，即便部分平台能探测到目标，但将这些高质量的探测数据，实时、精准地导向最优的射手（如另一架位置更好的飞机或地面防空系统），仍然存在巨大的技术和流程障碍。这种开环作战，使得印方空有强大的侦察能力和火力，却无法将其转化为



敏捷、高效的杀伤链。

3.后续调整的体现：据《外交家》杂志报道，印军参谋长承认，在首日遭受损失后印军被迫修正了战术。在后续的对抗中，印军更多地采用防区外导弹攻击和无人机渗透等非接触手段，并声称其一体化防空系统成功拦截了巴方后续的无人机和导弹攻击。这从侧面反映出，印方可能在首轮强对抗中暴露了短板，转而采用更能发挥自身单体平台优势但对体系协同要求相对较低的战术。

（2）巴方之利：体系集成的非对称优势

相比之下，巴基斯坦空军在此次冲突中，据报道，其新引进的中国制歼-10CE战斗机与PL-15E远程空空导弹发挥了关键作用。其优势的核心，正是在于一个相对更开放和兼容的作战体系。

1.统一的数据链整合：分析普遍认为，歼-10CE与巴方原有的预警机、地面指挥控制中心，以及可能存在的其他中方技术体系，通过一个整合度更高的战术数据链连接在一起。这使得巴方飞行员能够获得更清晰、更完整的战场态势，从而能更早地发现目标，并在有利的阵位上发射远程导弹。

2.体系赋能的杀伤效果：PL-15E导弹的射程优势，只有在强大的体系支撑下才能完全发挥。预警机或友机在前沿探测，通过高速数据链将目标信息传递给后方的歼-10CE，后者在相对安全的距离上发射导弹，并由体系内的



其他节点持续提供中继制导。这种“A射B导”的协同战术，是典型的网络化作战，其前提正是体系内不同节点间的开放与信息共享。

2025年5月的这场短暂而激烈的冲突，再次以实战结果明确昭示：现代战争的胜负，已不再由武器装备的纸面性能决定，而是由其背后整个作战体系的开放度、兼容性与信息流转效率所决定。一个由众多明星拼凑而成但彼此隔阂、数据不通的封闭体系，在面对一个平台也许并非最顶尖，但内部高度整合、信息共享顺畅的开放体系时，很可能遭遇惨败。对于任何致力于在未来战争中取胜的军队而言，打破技术与文化的壁垒，全力构建一个真正开放、共享、智能化的作战体系，已经不是一个选项，而是唯一的出路。

3.4 协同规则：导向性涌现的源泉

从复杂科学的角度看，自组织、涌现的前提是规则，简单的规则可以涌现出复杂的行为。从根本上说，设计协同规则，并非编写一部包罗万象的法典，而是要设计一个能够自我演化、催生智慧的生成式系统(Generative System)。这个系统的目标，不是去预设所有问题的标准答案，而是要构建一个能让最优答案自发涌现的生态环境。

3.4.1 协同规则设计的核心要素

协同规则设计包括主体、环境、交互协议、目标函数、



选择机制等五大核心要素，如图 3-2 所示。

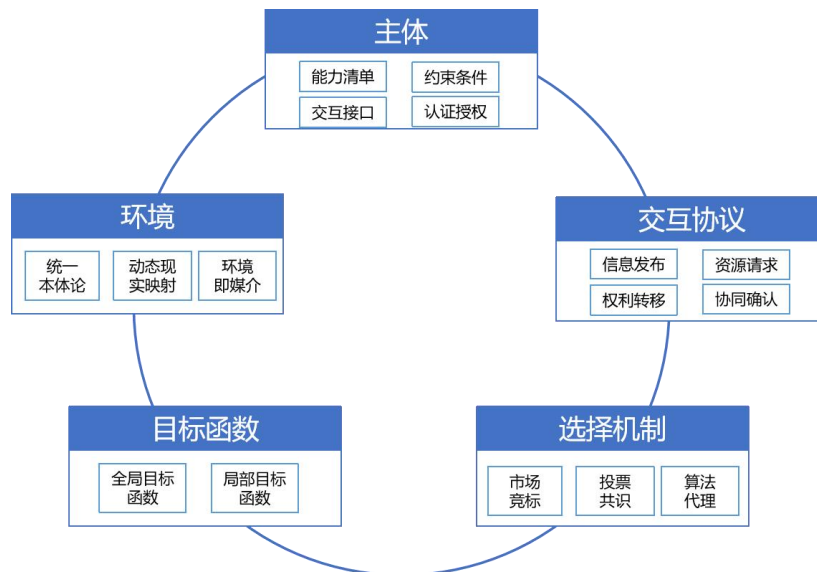


图 3-2 协同规则设计的要素

(1) 主体 (Agent)

主体是系统中最基本的行动单元。它可以是一个人类士兵、一架无人机、一个地面传感器、一个武器平台，甚至是一个纯粹的 AI 决策代理。在设计规则前，必须对主体的属性进行标准化、接口化的精确描述：

能力清单：每个主体能做什么？（如：侦察、打击、干扰、计算、中继通信等）。

约束条件：每个主体的局限是什么？（如：航程、弹药、算力、通信带宽等）。

交互接口：每个主体如何与外界收发信息和指令？这需要定义统一的 API（应用程序接口）。

认证授权：如何确保每个主体的身份是真实可信、不可伪造的？



设计要点：将每一个作战单元，都抽象成一个标准化的、可被网络调用的服务或对象，清晰地定义其输入与输出。

（2）环境（Environment）

环境是所有主体赖以生存、感知和互动的共享空间。在边缘指控中，这主要指一个统一的、实时的、机器可读的数字化战场空间。

统一本体论（Ontology）：必须有一套通用语言，用来描述战场上的一切事物（如敌方 XX 型号坦克、友方补给车队、雷区、禁飞区等）及其状态。

动态现实映射：这个数字环境必须能实时、准确地反映物理战场的变化，所有主体的传感器数据都会源源不断地汇入、共同维护。

环境即媒介：环境不仅是被动地图，更是主动的通信媒介。主体通过改变环境中的对象状态来进行间接通信。

设计要点：构建一个高保真、低延迟且所有主体都能读懂和写入的共享作战环境。

（3）交互协议（Interaction Protocols）

交互协议是主体之间以及主体与环境之间进行互动的语法。其设计的精髓在于极简主义，即用最少的规则，催生最丰富的行为。这些协议主要包括：

信息发布协议：一个主体如何向环境中添加或更新信息？（如目标提名规则）。



资源请求协议：一个主体如何向网络请求自身不具备的能力或资源？（如火力支援竞标规则）。

权力转移协议：在何种条件下，一个主体的指挥权或控制权可以临时转移给另一个主体？（如临机授权规则）。

协同确认协议：不同主体间如何就一个共同目标达成行动上的一致？

设计要点：设计一套清晰、无歧义、计算成本低的微语言，让复杂的协同意图，可以通过简单的标准化对话来完成。

（4）目标函数（Objective Function）

目标函数是整个系统需达到的目的要求。它将指挥员抽象的战略意图，转化为一个可被 AI 和人类共同理解并用以评估所有行为优劣的量化指标。

全局目标函数：在最高层面，它定义了整个战役的终极目标。例如：最大化（敌方指挥节点毁伤率） - $k \times$ （我方弹药消耗成本 + 我方战损风险）。

局部目标函数：对于具体的战术行动，它可以被分解为更具体的目标。例如，对于一次近距空中支援（CAS）任务，目标函数可能是：最大化（目标摧毁概率 $\times$ 目标价值） - $k \times$ （附带毁伤风险评估值 + 行动时间）。

设计要点：将指挥员的意图，从模糊的自然语言，翻译成清晰的、可计算的数学模型，为系统的自我优化提供一个明确的指南。



（5）选择机制（Selection Mechanism）

选择机制是系统在面对多个可能的行动方案时，如何做出抉择的规则。它是一个发现最优解的引擎，确保整个系统能够沿着合适的路径前进。

市场竞标机制：如前述 CAS 案例，让能力提供方（射手）进行竞标，由需求方或中立方选择性价比最高的方案。

投票共识机制：在需要多个主体达成共识时（如决定一支小队的进攻路线），可以通过投票或加权投票的方式来决策。

算法代理机制：由一个专职的调度 AI，根据实时数据和目标函数，自动匹配网络中的需求与供给。

设计要点：建立一个公平、高效、能够快速从众多可能性中筛选出最优解的机制。

3.4.2 协同规则的基本运行过程

基于以上五大要素，一个有效的边缘协同过程，将呈现为一个持续循环的、自下而上的“感知—评估—行动”闭环，如图 3-3 所示。

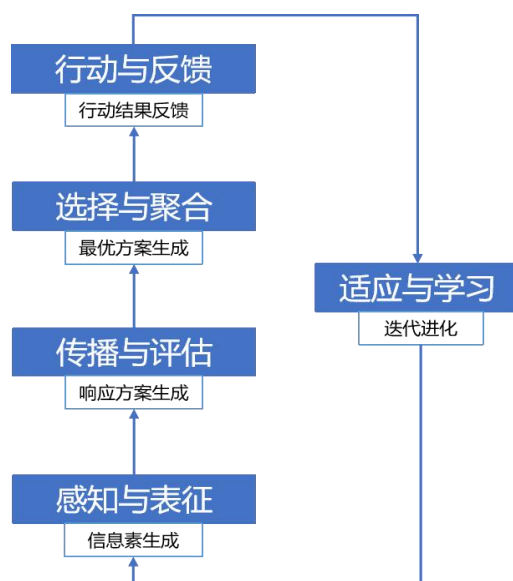


图 3-3 协同规则的基本运行过程

(1) 感知与表征：某个主体在其局部环境中，感知到新的变化（如出现敌情），并遵循交互协议，在共享数字环境中生成一个信息（如一个待确认目标）。

(2) 传播与评估：环境中的这一变化，被网络中其他相关主体感知。它们根据自身的能力清单和约束条件，评估自己对该信息能够做出何种响应。每一个可能的响应方案，都会依据目标函数，被赋予一个适应度分值。

(3) 选择与聚合：选择机制（如市场竞标）启动，对所有响应方案进行比较，选择出适应度分值最高的方案。围绕这个最优方案，相关的主体被动态地、临时地聚合在一起，形成一个任务群组。

(4) 行动与反馈：该任务群组执行协同行动。行动的结果（成功、失败、对环境造成的新变化）会立刻被系统感知，作为新的信息，更新到共享环境中。



(5) 适应与学习：这个“结果—反馈”闭环，会实时调整整个系统的状态，甚至可能修正目标函数的权重（如发现某种威胁的优先级需要调高）。系统完成了一次学习和迭代，并准备好进入下一个循环。

通过这一过程，指挥员的角色，从一个事必躬亲的棋手，转变为一个设计并维护这个棋盘和规则的游戏设计师。他所设计的，不再是一次具体的胜利，而是一个能够不断赢取胜利的、充满生命力的智能系统。



四、研究建议

为实现边缘指控,需要研究解决一系列科学技术问题。基于对国内外发展现状与趋势的分析,本报告提炼了 9 个代表性研究问题建议,给出了研究目标和内容的建议,如表 4-1 所示。

表 4-1 边缘指控的研究问题建议

	研究问题
边缘指控 组织设计	研究问题 1: 边缘指控组织形态动态切换机制研究
	研究问题 2: 去中心化人机集群中指挥功能的定义、度量与临机实现
边缘自主 协同技术	研究问题 3: 大规模异构无人集群的跨域自主协商与冲突消解
	研究问题 4: 异构智能体在柔性集成中的涌现性行为预测与约束
	研究问题 5: 自主智能体网络中合作行为的演化动力学
	研究问题 6: 多域作战空间的分布式拍卖与实时协商机制



	研究问题
边缘指控 支撑技术	研究问题 7: 支撑军事体系跨代演化的可进化开放架构设计原理
	研究问题 8: 对人类队友信念、意图与注意力的建模与预测
	研究问题 9: 基于因果推理与叙事逻辑的作战规划方法

4.1 边缘指控组织设计

研究问题 1: 边缘指控组织形态动态切换机制研究

当前关于边缘指控的讨论，往往倾向于用一种去中心化的理想模型，去完全替代传统中心化层级模型。然而，军事组织的根本使命决定了其必须在纪律、统一和战略服从上，保持高度的中心化节制；而未来战场的复杂、动态、不确定性，又要求其必须具备极高的去中心化涌现能力。

（1）研究目标

摒弃非此即彼的思维定式，探索一种能够在层级化与网络涌现两种组织形态之间，根据任务情境进行动态、无缝切换的组织理论与实现机制。我们不再寻求一个单一的最优组织形态，而是研究一个组织如何能像变形金刚一样，在需要严格执行命令时，呈现为传统的金字塔；在需要最大化适应性与创造力时，又“液化”为一个分布式的网络。

（2）研究内容



①组织二元性的理论构建：借鉴组织行为学中的“组织双元性”（Ambidexterity）理论和复杂科学中“混沌边缘”理论，构建适用于军事领域的“二元并存”组织模型。研究并定义两种形态的临界点：在何种条件下，一个组织应该保持层级形态？在何种条件下，又应该切换到网络形态？

②动态切换的触发器与协议设计：识别切换触发器：研究哪些关键变量可以作为组织形态切换的开关。例如：威胁的紧急程度、任务的清晰度、战场环境的确定性、通信网络的稳定性，以及上级指挥意图的授权等级等。

③设计切换协议：研究组织形态转换的具体流程和规则。当从层级切换到网络时，指挥权的下放、信息共享的范围、行动的自主权是如何被激活的？反之，当网络需要重新收敛为层级结构时，指挥权如何被快速、有效地回收？

④仿真建模与效能评估：利用基于主体的建模方法，构建一个二元组织的计算机仿真模型。通过在仿真环境中进行大量不同情境的对抗演习，量化评估二元组织相较于纯粹层级组织或网络组织，在生存力、任务完成效率、适应性等方面的综合效能优势。

研究问题 2：去中心化人机集群中指挥功能的定义、度量与临机实现

指挥权一直被视为一种被预先赋予某个特定人类指挥员的稳定身份属性。然而，在一个人与 AI 高度混合、大规



模分布式的边缘指控网络中，指挥本身是否还必须与一个固定的人类节点绑定？本课题提出一个大胆的假设：指挥权可以被重新定义为一种在特定任务情境下，由网络中多个主体（人或机器）的互动，而临时涌现出来的一种系统状态或功能，而非个体属性。

（1）研究目标

探索指挥功能与指挥员身份解耦的可能性。研究在一个没有固定指挥员的集群中，如何通过设计底层规则，让有效指挥作为一种集体智能现象自发产生，并能在任务完成后自动消散。

（2）研究内容

①指挥功能的数学定义：将指挥这一概念，分解为若干个可被量化和度量的功能模块，如目标设定、资源分配、风险评估、行动裁定等。

②基于网络中心性的临时指挥席位：运用网络科学理论，研究是否能根据一个节点在特定任务信息流中的中心性（如介数中心性、特征向量中心性），来动态、临时地赋予其部分指挥功能。例如，此刻掌握最关键信息的侦察无人机，便临时拥有了最高的目标设定权重。

③分布式决策共识协议：借鉴分布式计算（如 **Raft**、**Paxos** 共识算法）和生物学（如蜂群决策）的原理，设计一套协议，让一个去中心化的集群，能够在没有固定中心的情况下，就一个复杂的战术目标快速、鲁棒地达成行动



共识。

4.2 边缘自主协同技术

研究问题 3：大规模异构无人集群的跨域自主协商与冲突消解

当前蜂群研究多集中于一个蜂王（中心控制器或人类）如何控制一个同质化的蜂群。但未来战场上，必然会出现多个分属不同任务、由不同算法驱动，甚至目标存在潜在冲突的蜂群相遇。一个前所未有的科学问题是：在没有一个更高层级总指挥的情况下，这些自主集群之间如何自主地进行协商、避免冲突，甚至达成新的更优协同？本课题旨在探索一种“计算治理”框架，即为智能体集群设计一套内在的社会规则或协商协议。

（1）研究目标

设计一套允许大规模、异构、无主的智能体集群，能够自主进行目标对齐、资源分配和冲突解决的分布式协议。其目标是让秩序从集群间的互动中自发涌现，而非依赖于外部强加的控制。

（2）研究内容

①基于博弈论的自动协商协议：研究如何让不同的集群，通过一种类似多边外交谈判的自动协商协议，在任务、资源和物理空间上达成纳什均衡。

②数字产权与资源分配：为网络中的关键资源（如特



定的电磁频谱、地理区域的优先通行权)定义一种数字产权,并设计一套基于市场拍卖或投票的分布式资源分配机制。

③涌现式领导与功能分化:研究在一个无主的集群网络中,是否会因为节点能力和网络位置的差异,而自然涌现出临时的领导者节点(负责协调)和追随者节点,以及如何引导这种自发的结构分化。

研究问题 4: 异构智能体在柔性集成中的涌现性行为预测与约束

开放架构允许不同功能的异构智能体即插即用组合在一起,但这隐藏着巨大风险:两个或多个独立验证过的智能体,在组合后其相互作用可能会涌现出灾难性的、未曾预料的系统级故障。本项目旨在探索一种能够从数学上预测并约束异构智能体组合行为的理论与方法,确保集成的安全性和稳定性。

(1) 研究目标

建立一套形式化的理论与工具,使得系统在集成多个异构智能体之前,能够自动验证它们的组合是否会产生危险的、破坏性的涌现行为,从而确保集成的柔性不会以牺牲系统的安全性和稳定性为代价。

(2) 研究内容

①行为契约的形式化语言:设计一种语言,让每个智能体都能以一种机器可读且在数学上无歧义的方式,精确



地宣告其自身的行为契约，包括：承诺提供什么服务、需要消耗什么资源、响应时间上下限，以及在异常情况下的行为模式等。

②组合行为的形式化验证：研究如何运用模型检测、定理证明等形式化方法，在智能体实际组合前，对其行为契约进行组合推演。系统会自动分析：“如果将 A 和 B 组合，是否存在任何一种情况，会导致它们的契约相互冲突，或产生违反系统级安全规约的组合行为？”

③基于数字孪生的涌现风险发掘：构建一个高保真的体系数字孪生环境。在该环境中，利用 AI 驱动的技术，对即将集成的异构智能体进行虚拟组合，并进行自动化虚拟测试，主动发掘潜在的、难以通过理论推演发现的负面涌现效应。

研究问题 5：自主智能体网络中合作行为的演化动力学研究

协同主要依赖于人类预先设计的、自上而下的“硬编码”规则。然而，这种刚性规则在面对复杂、不确定的对抗时，显得脆弱且缺乏适应性。一个大规模的智能体群体，能否在没有被预先编程的情况下，仅仅通过重复的、局部的互动与学习，像人类社会一样，自发地演化出高效的、不成文的社会规范或行为默契？例如：在没有明确指令的情况下，无人机群可能会自发演化出“遇到友军时，自动向右偏航”的避让惯例？



（1）研究目标

本研究旨在通过借鉴演化博弈论和社会学理论，探索在没有中心化控制下，高效、坚韧的合作行为与社会规范如何自发涌现、传播和收敛，从而为构建反脆弱的作战体系提供理论基础。

（2）主要研究内容

①基于演化博弈论的规范形成建模：在仿真环境中，运用演化博弈论模型，观察在不同的“收益—成本”结构下，何种协同或避让行为（如合作、谦让、自私等）会成为最终的演化稳定策略。

②声誉系统与规范的强制力：引入声誉系统对规范形成的影响。一个主体的合作行为会为其增加声誉分，而背叛行为则会降低。其他主体在选择合作伙伴时，会优先选择高声誉的，从而在群体中形成遵守规范的正向激励。

③规范的文化传播与引导：研究一种规范如何在群体中进行传播（学习与模仿），以及如何通过引入少数遵循高级规则的榜样节点（精英智能体），来加速优良规范在整个群体中的扩散速度，实现对群体行为的软引导。

研究问题 6：多域作战空间的分布式拍卖与实时协商机制

传统的空域/频域管理类似于计划经济，由一个中心节点进行审批和分配，效率低下且不具弹性。一个新颖的思路是，引入市场机制来解决去中心化环境下的空间资源冲



突问题。本课题的核心科学问题是：我们能否设计一套类似于高频交易市场的分布式拍卖与协商协议，让成千上万的无人机、导弹、地面部队等自主单元，能够在没有中央管制塔的情况下，自行、高效、公平地解决对物理空间和频谱资源的实时使用冲突？

（1）研究目标

建立一个去中心化的、基于市场规则的作战空间管理框架。其目标是让空间资源的分配，从基于审批的模式，转变为基于竞价和协商的模式，从而实现资源利用效率和作战节奏的最大化。

（2）研究内容

①空间使用权的通证化（**Tokenization**）：将特定地理空域或特定无线频谱在特定时间段内的使用权，定义为一种可被交易的数字通证。

②分布式实时拍卖算法：设计一种轻量、高效的拍卖协议。当多个主体需要同时使用同一块稀缺的空间资源时，它们会自动进入一个拍卖程序。每个主体会根据其任务的紧急程度和重要性（由其目标函数决定），提出一个“报价”。出价最高的，获得该资源在下一秒的优先使用权。

③多方协商与利益互换：研究当拍卖无法解决复杂冲突时，相关主体之间如何启动一个自动化的多方协商程序，进行利益互换。例如，A 无人机可以向 B 无人机发送请求：“你若愿意将此航路让给我 30 秒，我将与你共享我获取的



全部侦察数据”。

4.3 边缘指控支撑技术

研究问题 7：支撑军事体系跨代演化的可进化开放架构设计原理

当前的开放架构，主要解决了在同一代技术框架内的柔性问题。但一个更深刻的问题是：当出现一种颠覆性的新技术（如量子计算、生物传感器），其原理与现有体系完全不同时，当前的开放架构是否具备自我进化以兼容这种未来的能力？本课题旨在区分灵活性（Flexibility）与可进化性（Evolvability），探索具备跨代韧性的架构设计原理。

（1）研究目标

定义并构建一套可进化开放架构（EOA）的核心设计原理。该架构的“基因组”——即其最底层的、最核心的抽象层与规则，必须足够稳定和普适，以确保在未来数十年内，能够持续、平滑地吸收和融合今天无法想象的新技术，而无需对整个体系进行推倒重来。

（2）研究内容

①架构不变量的识别与设计：借鉴互联网 TCP/IP 协议等技术生态的成功经验，研究在军事体系中，哪些要素是跨越技术代际的不变量（如对可信身份、安全通信、任务意图的抽象需求），并将其设计为架构中最稳定、最核心



的基因。

②多代际共存的抽象层设计：研究如何设计足够强大的抽象层与适配器模式，使得基于未来新原理的子系统，能够被封装成符合核心架构基因的形式，从而与老旧的子系统在同一架构下共存和协同，实现“优雅的”新陈代谢。

③架构演化的治理与评估：建立一套用于评估架构健康度与可进化潜力的量化指标体系，并设计一种治理机制，来决定何时、何处，以及如何对架构的“基因组”进行迭代式的“基因编辑”，以引导其向正确的方向演化。

研究问题 8：对人类队友信念、意图与注意力的建模与预测

在人机协同中，真正的默契源于“我懂你”。一个仅仅被动执行命令的 AI，仅是工具；而一个能理解并预测人类队友在想什么、要什么的 AI，才能成为真正的队友。本课题旨在为边缘 AI 智能体，构建一个计算化的、功能等效的心智理论模型，使其具备对人类队友认知状态的感知和预测能力。

（1）研究目标

设计一种能够构建并实时维护其人类队友认知模型的 AI 代理。该 AI 能利用这个模型，主动适应人类的行为，预判人类的需求，并使自身的行动对人类而言，更具可预测性和可解释性，从而实现真正深度的人机互信与协同。

（2）研究内容



①人类意图的逆向推断：基于逆向强化学习等技术，让 AI 通过观察人类队友的一系列行为（如移动路线、观察方向、武器选择），反向推断出其背后最可能的、未言明的战术意图。

②注意力与认知负载的实时建模：综合分析人类队友的交互数据（如其在地图上关注的区域、下达指令的频率和速度），甚至生理数据（如果可得），来实时评估其当前的注意力焦点和认知负载水平。

③主动式、适应性协同行为：基于对人类队友意图和认知状态的预测，AI 可以采取一系列主动的协同行为。例如，预判性信息推送：在人类队友开口询问前，就将他可能最需要的情报推送过去。适应性行为调整：当预测到人类队友认知负载过高时，AI 可以自主减少非关键信息的汇报，或主动接管一些重复性的操作。

④可解释性自我表达：AI 在行动前，可以主动向人类解释：“根据我推断出的‘您想包抄敌方侧翼’的意图，我将自主移动到此位置提供火力掩护，请确认。”

研究问题 9：基于因果推理与叙事逻辑的作战规划方法

当前 AI 擅长在给定规则下进行优化，但人类指挥员的规划能力，本质上是一种创造“战术剧本”的能力。一个好的计划，是一个逻辑自洽、因果相连的“故事”：“我们首先要压制敌方火力，以便于我方装甲能够安全前出，



然后利用装甲的突破来吸引敌方预备队，从而为我方侧翼的决定性攻击创造条件”。这种基于因果关系和叙事逻辑的思维，是当前深度学习等统计 AI 方法的短板。本课题将符号 AI 的因果推理能力与现代机器学习相结合，教会无人指挥节点如何“写剧本”，而不仅仅是“算最优解”。

（1）研究目标

研发一种能够自主生成多个、内部逻辑一致且具备因果可解释性的作战方案的 AI 规划引擎。该引擎生成的方案，不仅在战术上可行，更重要的是，其每一步行动的理由及其与其他行动之间的因果联系都是清晰、可被理解的。

（2）研究内容

①战术知识的因果图谱构建：将军事条令、战史战例中的战术知识，转化为因果知识图谱。例如，“压制防空系统”是“夺取空中优势”的原因之一。

②基于因果推理的规划算法：研究一种能够在该图谱上进行推理的规划算法。当给定一个高级任务目标（如“占领 A 高地”）时，算法能够反向推导出所有必要的前置条件，并自动构建出多条可行的、逻辑上没有断点的行动链。

③方案的叙事化解释：研究如何将 AI 生成的、形式化的行动链，自动翻译成人类指挥员能够理解的、带有“因为…所以…”逻辑的自然语言战术叙事，以供人类进行最终的评估和选择。



参考文献

- [1]. 张维明, 朱承, 黄松平, 阳东升. 指挥与控制原理[M]. 电子工业出版社, 2021.
- [2]. 黄松平, 张维明. 边缘战及边缘指挥控制[M]. 电子工业出版社, 2025.
- [3]. 胡晓峰. 战争科学论—认识和理解战争的科学基础与思维方法[M]. 北京: 科学出版社, 2018: 302.
- [4]. 阳东升, 张维明. 边缘崛起: 边缘 C2 背景、概念与模式机理分析[J]. 指挥与控制学报, 2020, 6(2): 113.
- [5]. 张维明等. 多域作战及其指挥控制问题探析[J]. 指挥信息系统与技术, 2020, 11(1): 5.
- [6]. 王海宝, 贺幸福, 阳东升. 智能化“OODA”环路: 重塑与颠覆[J]. 国防科技大学学报, 2023, 45(6): 1-10.
- [7]. U.S. Department of Defense. Summary of the Joint All-Domain Command and Control (JADC2) Strategy[R]. Washington D.C.: DoD, 2022.
- [8]. Van Creveld M. Command in War[M]. Cambridge: Harvard University Press, 1985.
- [9]. Taleb N N. Antifragile: Things That Gain from Disorder[M]. New York: Random House, 2012.
- [10]. Freedman L. Command: The Politics of Military Operations from



- Korea to Ukraine[M]. Oxford: Oxford University Press, 2022.
- [11]. DARPA. Persistent Close Air Support (PCAS) Program Information[EB/OL].
(<https://www.darpa.mil/program/persistent-close-air-support>).
- [12]. Deptula D, Penney H, Stutzriem L, Gunzinger M. Restoring America's Military Competitiveness: Mosaic Warfare[R]. Mitchell Institute for Airpower Studies, 2019.
- [13]. Radoman R, Henshaw M, King M, Rabbets T. Enabling Open Architecture in Military Systems: A Systemic and Holistic Analysis[J]. Systems, 2025, 13(3), 207
- [14]. South Asia Investor Review, Pakistan's Homegrown Link-17 Kill Chain Helped Shoot Down India's Rafale Fighter Jets[EB/OL],
(<https://www.southasiainvestor.com/2025/05/pakistans-homegrown-link-17-kill-chain.html>)
- [15]. The Asia Live. Pakistan's Precision Strike Network: How a Coordinated Kill Chain Took Down an Indian Fighter Jet[EB/OL].
(<https://theasialive.com/pakistans-precision-strike-network-how-a-coordinated-kill-chain-took-down-an-indian-fighter-jet/2025/06/20/>)
- [16]. Slusher M. Lessons from the Ukraine Conflict: Modern Warfare in the Age of Autonomy, Information, and Resilience[R]. Center for Strategic & International Studies (CSIS), May 2025.