DOI 10.15302/J-SSCAE-2021.03.007

多无人系统协同中的人工智能安全探索

施文[1]，王楷文[1]，俞成浦[1]，孙健[1]，陈杰[1,2]

（1. 北京理工大学自动化学院，北京 100081；2. 同济大学，上海 200092）

摘要：作为中国新一代人工智能规划中的重要组成部分，多无人系统协同是我国未来国防建设和社会发展的一项变革性技术。虽然多无人系统协同技术研究与系统集成已经达到了空前高度，但是其相关人工智能安全问题研究还处在萌芽阶段。本文阐述了统筹推进多无人系统协同赋能应用与风险防控的重大意义，提出了“四位一体”全面推进多无人系统协同安全发展的战略思路，探索了多无人系统协同在内生安全和衍生安全层面潜在的挑战与应对思路。研究提出了智能无人系统安全对策建议：构建国家级无人系统验证平台，推动人才队伍建设；逐步深化无人系统产业“放管服”，发展新一代人工智能安全生态；充分发挥多无人系统协同的优势，赋能保障和改善民生，服务构建人类命运共同体。

关键词：多无人系统协同；人工智能安全；安全风险防控

中图分类号：TP18　　**文献标识码：**A

Artificial Intelligence Security in Multiple-Unmanned System Cooperation

Shi Wen[1], Wang Kaiwen[1], Yu Chengpu[1], Sun Jian[1], Chen Jie[1,2]

(1. School of Automation, Beijing Institute of Technology, Beijing 100081, China; 2. Tongji University, Shanghai 200092, China)

Abstract: Multiple unmanned system cooperation is an important component of China’s new-generation artificial intelligence (AI) planning and it is a transformative technology for future national defense construction and social development of China. Although significant achievements have been made regarding the technological research and system integration of multiple unmanned system cooperation, research on AI security is still in its infancy. Promoting multiple unmanned system cooperation enables AI application and risk control. In this article, we propose a four-in-one strategy to promote the collaborative and secure development of multiple unmanned systems, investigate potential challenges and countermeasures for multiple unmanned system cooperation at the endogenous and derivative security levels, and propose several suggestions regarding the security of intelligent unmanned systems. Specifically, a national unmanned system verification platform should be established to promote the construction of talent teams; services need to be upgraded for the unmanned system industry to develop a new-generation AI security ecology; and the advantages of multiple unmanned system cooperation should be maximized to improve people’s livelihood.

Keywords: multiple unmanned system cooperation; artificial intelligence (AI) security; security risk prevention and control

收稿日期：2021-02-15；**修回日期：**2021-04-29

通讯作者：俞成浦，北京理工大学教授，主要研究方向为系统辨识与机器学习、分布式优化与控制、传感器网络与室内定位；
E-mail: yuchengpu@bit.edu.cn

资助项目：中国工程院咨询项目“新一代人工智能安全与自主可控发展战略研究”(2019-ZD-01)

本刊网址：www.engineering.org.cn/ch/journal/sscae

一、前言

智能无人系统种类多样，覆盖海陆空不同空间，正在全面深入国家安全和社会生活各领域，并推动新一轮产业变革和相关技术高度集成。多无人系统协同作为一项人工智能的颠覆性技术，将在空间上分布的无人系统有机连接起来，实现多系统在时间、空间、模式、任务等多维度上的有效协同，最终形成目标探测、跟踪识别、智能决策、自主控制和效能评估的完整链条。伴随着技术水平的不断提升，多无人系统的使命任务将不断拓展，将极大地改变日常生活方式和军事作战方式。

多无人系统协同在给社会创造价值的过程中存在着诸多安全隐患，如无人车的交通事故，无人机的扰航、恐怖袭击，机器人造成工人失业等。多无人系统协同可能将在军事作战、产业升级、政府监管、社会治理以及伦理等多个方面给国家安全带来新的挑战 [1]。

目前，国内多无人系统协同的研究仍处于起步阶段，其基础理论框架对未来无人系统发展和技术突破起着至关重要的作用 [2]。因此，本文针对这一空白领域展开前瞻研究，旨在揭示多无人系统协同中人工智能安全的重要意义，针对相应问题提出对策建议，以期为我国无人系统安全发展提供参考。

二、统筹推进多无人系统协同赋能应用与风险防控意义重大

（一）多无人系统协同研究持续高速发展的重要抓手

2017 年 7 月，国务院印发的《新一代人工智能发展规划》阐释了人工智能新时代战略的丰富内涵，这为我国多无人系统中人工智能安全改革指明了方向，进一步明确了中长期发展的目标 [2]。我国人工智能新时代战略实施以来迎来了很大起色，但关于多无人系统中的人工智能安全问题仍未给出明确解决方案 [3]。寻找各项问题解决方案，立足安全基础，推进多无人系统的稳步发展，有利于多无人系统人工智能落地。

（二）不断增强我国军事实力的有效途径

军事实力是综合国力最直接的体现，在多无人系统广泛应用于军事领域的背景下，其安全问题的重要性更加突出。一方面，越来越多的国家研发出了智能化武器，实现多无人系统协同作战的能力越来越强，未来的战争将由多无人系统协同作战主导；因此，在智能化战争中如何保证领土主权和国土安全具有重要意义。另一方面，在智能化战争中多无人系统自身的防护同样具有重要意义，如何保证自身系统的安全、保证数据不泄露、控制权在手、遭遇打击仍能完成任务是目前多无人系统研究的一大课题。

（三）提升我国社会安全保障水平的关键前提

人工智能安全是关系到我国经济社会发展的时代性、战略性问题。多无人系统协同将广泛应用于工业、农业、经济和国防领域，对国家安全也会带来深刻变革。由于多无人系统滥用门槛低，容易被极端组织和犯罪团伙利用，管理难度远大于从前 [4]。加强人工智能新时代多无人系统立法，形成数据、模型、应用等一系列相关的法律、法规，完善人工智能使用标准的制定，有助于带动国家整体社会安全保障水平的提升。

（四）实现未来高度智能化社会建设的必然要求

传统无人系统目前已应用于社会的智能化建设，如智能快递分拣、无人超市、交通违章识别等，节省了大量的人力。未来，多无人系统协同的广泛应用将会在更大程度上保障和改善民生。但相较于传统无人系统，应用具备通信和交互能力的多无人系统可能会引发更加严重的公共安全、伦理安全等问题 [5]。因此，重点加强多无人系统应用中的问题研究和风险防范至关重要，只有处理好上述问题，才能确保多无人系统在未来能够安全可靠地为社会做出贡献，推动我国新一代人工智能健康发展。

三、多无人系统协同安全发展概况

随着多无人系统协同理论体系的成熟，相应的产品与应用呈现出迅猛发展的势头。从应用领域的角度，多无人系统产品主要包括无人车集群，无人机集群和无人船集群。无人车集群不但能够将各类车辆的驾驶人员解放出来，极大地减轻汽车驾驶员的工作量，还能够通过智能优化算法合理安排道路

资源，缓解交通压力，并减少道路交通安全事故的发生。无人机集群的应用则涵盖了军事上的攻击、骚扰、侦查任务以及民用的灾害救援、监控巡查、环境监测、农业植保等领域。无人船集群则主要用于执行危险、枯燥以及其他不适于有人舰艇执行的任务，包括水质监测、航道测绘、海上巡逻等 [6]。相较于传统的有人系统，多智能体系统具有多方面优势，包括更低的操作门槛，更低的运维成本，更广泛的应用领域，更稳定的运行状况，更高效的资源分配等。在军事上，多无人系统更是能够极大程度地保障操作人员的安全，减少人员的伤亡，在进攻端还能够利用其数量优势形成长距离、大范围、高精度的饱和式打击，甚至有可能改变现代战争的模式。

随着多无人系统的飞速发展，很多发达国家目前正积极推进智能多无人系统安全框架研究以及法案的制定。美国在多无人系统中的人工智能安全方面的研究以及政策发布非常频繁，2019 年 6 月，美国更新了《国家人工智能研究和发展战略计划》，将人工智能系统安全列为战略目标之一 [7]；2020 年 1 月发布的《人工智能应用监管指南备忘录（草案）》提出了人工智能十项监管原则 [8]；2020 年 3 月通过的《2020 年国家人工智能计划法案》支持对无人系统的道德、法律、社会等安全问题展开研究 [9]；2020 年 11 月更新的《人工智能和国家安全》中详细写明了智能多无人系统在军事上的发展与伦理安全问题 [10]。

欧盟方面同样在智能无人系统安全上展开了积极研究以及政策制定，欧盟各成员国都纷纷出台法律法规以规范无人机运行。法国自 2019 年 7 月起规定无人机必须注册电子账号；德国规定所有无人机必须在机身刻上所有者的姓名与地址；英国把机场附近的无人机禁飞区半径从原来的 1 km 增加到 5 km；西班牙、葡萄牙、意大利等国都禁止无人机在夜间飞行。2019 年初，欧盟委员会发布了《关于欧洲人工智能开发与使用的协同计划》，将人工智能安全列为了一大关键发力领域，在全球人工智能伦理道德领域占据了领先地位 [11]；2019 年 4 月，欧盟委员会发布了《人工智能伦理准则——可信 AI 伦理指南》，提出了可信 AI 的七大原则 [12]；2020 年 6 月，欧盟新发布的无人机通用准则在欧盟全境正式启用，该准则取代了欧盟成员国各自的现行法规，为欧洲发展无人机行业提供了明确、统一的规则 [13]。

我国的多无人系统相关法案制定也在逐步推进。2017 年 7 月，我国国务院首次颁布的人工智能战略性文件《新一代人工智能发展规划》，提出了 2030 年人工智能核心产业规模应超过 1 万亿元，带动相关产业规模超过 10 万亿元的目标，并对多无人系统协同中的人工智能基础理论框架给出了定义，提出了“加强人工智能相关法律、伦理和社会问题研究，建立保障人工智能健康发展的法律法规和伦理道德框架”[2]。但该框架在自主协同控制与优化决策理论的定义中，更侧重于协同控制的实现与优化，对于多无人系统中可能存在的安全性隐患没有较多阐述。2020 年 12 月，中国信息通信研究院安全研究所发布了《人工智能安全框架（2020 年）》，制定了一个较为全面的人工智能安全框架，但其中对于多无人系统协同中特有的安全问题表述仍不详细 [3]。

四、多无人系统协同面临的挑战

区别于传统无人系统研究，多无人系统协同的核心要素包括通信交互，合作博弈，以及群体智能演化等。结合多无人系统协同的上述特点，坚持以问题为导向分析其具体战略举措，围绕多无人系统本身的内生安全和多无人系统对外界的衍生安全两大模块构建了多无人系统协同中的人工智能安全框架，如图 1 所示。

（一）内生安全

为了多无人系统任务的可靠执行，内生安全主要考虑的是系统本身是否稳定可靠，能否在通信交互过程中不泄密，能否保证控制权始终在自己手中，以及能否在出现故障后继续完成任务。多无人系统协同的内生安全要关注多无人系统工作的各个环节，从保证局部每个环节的安全以确保整体的安全，这其中涵盖了各无人系统单体间交互的数据安全、多无人系统所处的网络安全、搭载于多无人系统的软件及其算法安全、多无人系统本身的系统架构安全等。多无人系统协同的内生安全包括了通信与交互安全、协同决策与集群演化算法安全和系统架构安全三部分。

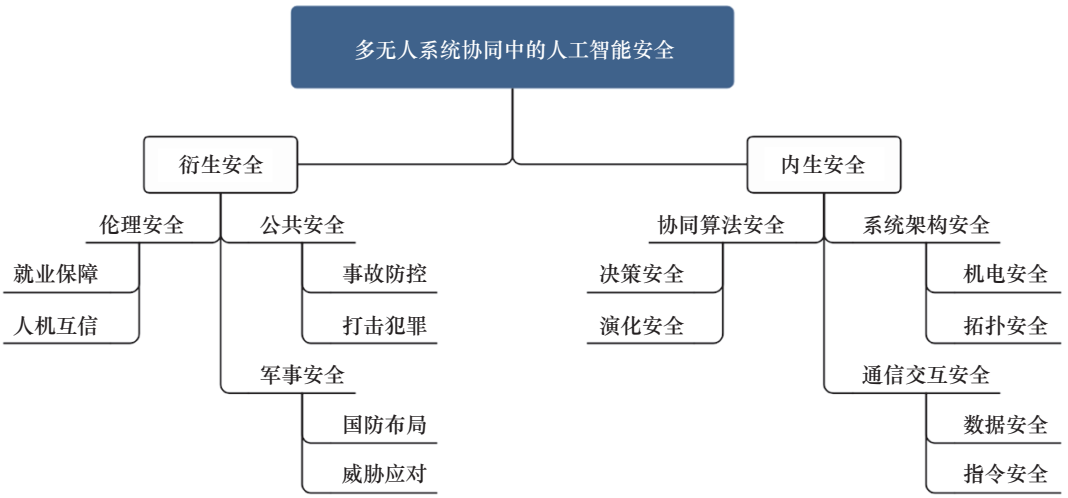

图 1　多无人系统协同中的人工智能安全框架

1. 通信与交互安全

多无人系统协同任务在执行过程中，需要频繁的进行通信交互，这其中包括各多无人系统个体之间的交互，还包括各多无人系统与其所有者之间的交互，多无人系统与各种实体任务对象交互等。因此，通信与交互安全是多无人系统协同内生安全的重要内容。通信网络安全的主旨是防范来自网络的攻击，保障多无人系统所有者能够安全可靠地控制多无人系统，保证数据不被窃取和篡改。一方面，多无人系统的协同中需要保障彼此之间的通信安全可靠，一旦数据传播受到截断，信息内容被他人窃取、解密或篡改，多无人系统将受到极大的威胁，我方战略意图也将受到严重打击。另一方面，如果通信网络的安全性不能满足要求，则多无人系统的控制权将不能得到保障，由于多无人系统极强的行为能力，与单纯的各种数据损失相比较，控制权不安全造成的后果往往更严重 [14,15]。

针对上述多无人系统存在的数据泄露及控制权丢失的问题，为系统个体搭载不可被外界直接访问的安全存储空间，对数据进行加密处理，保证通信过程中的数据安全；同时可以采用数字证书、密钥等认证材料进行双向的远程身份认证，以确保系统中每个个体身份的合法性以及指挥部的可信性 [16,17]。

2. 协同决策与集群演化算法安全

在算法安全上，一方面要考虑多无人系统能否做出正确的决策，另一方面更要考虑协同决策算法和自学习演化的方向是否自主可控。决策算法不成熟可能导致协同欠鲁棒，难以实现临机协同决策和行动，当系统结构受外界影响发生变化时，智能协同算法如未能实时完成控制和优化，则很难实现精准的协同控制任务，使协同一致性和稳定性降低，从而增加了协同任务失败和多无人系统在任务中损毁的风险。在未来的发展中，基于群体智能演化的多无人系统能够自主学习和换代，其演化方向的安全性更为重要，将成为多无人系统协同中算法安全的全新挑战。

针对上述问题，改进决策算法的训练过程，揭示无人系统集群的协同演化规律，设计主动防御的机制，在训练过程中加入大量可能出现的对抗样本，即在训练过程中添加假想敌，从而提高算法的鲁棒性，减少协同控制任务失败以及演化方向错误的可能性，更加安全可靠地实现协同决策和演化 [18]。

3. 系统架构安全

系统架构安全可细分为机电安全和拓扑安全两个方面。其中，机电安全要考虑多无人系统中每个个体的信息收发特性、信息处理能力是否足够，传感器、通信模块能否满足执行协同任务的需求。拓扑安全则是建立在机电安全的基础上，需要考虑多无人系统的整体响应速度和协同模式，能否在复杂场景下实时采集、处理和交换信息，进一步正确分配和执行任务，并且在部分无人系统单体出现故障时，能否正确检测故障，进行拓扑切换继续任务 [19]。

建立多层分簇的协同框架可以有效解决系统架构安全问题，多层分簇的框架可以帮助多无人系统

在面对变化时快速做出反应，即使遇到故障也能实现拓扑切换，继续完成好下一步任务，从而使得网络拓扑结构更加稳定，实现更加稳健和鲁棒的多无人系统协同 [20,21]。

（二）衍生安全

多无人系统协同的衍生安全主要考虑的是多无人系统在投入使用后，系统外部的人或其他事物可能面临的影响。在系统出现故障、受到干扰或出现决策失误时，除了任务失败和系统本身损毁的风险外，还可能引发衍生安全问题。同时，如果多无人系统控制权的所有者怀有恶意，对多无人系统下达了带有其不良企图的任务目标，可能产生更为严重的衍生安全风险。多无人系统协同中的人工智能衍生安全主要考虑公共安全、伦理安全和军事安全三个方面。

1. 公共安全

多无人系统协同工作时，事故的发生将会危害公共安全，不但会对社会秩序造成一定影响，更有可能会威胁到人身财产安全。当前多无人机协同系统在各行各业广泛使用，但安全性能评估体系还未完善，易出现各种事故，例如各种外界干扰导致的无人机群演示失败、无人车造成道路交通拥堵等。同时，多无人机协同具有低成本、用途广、使用门槛低、身份信息隐蔽、大面积杀伤等特点，非法使用将会严重威胁到人身财产安全，多无人系统的发展势必会带来新的违法犯罪形式，而与单无人系统相比，多无人系统便于无身份有组织犯罪，会极大地危害公共安全 [22]。

面对多无人系统可能对社会公共安全带来的冲击，加强监管无疑是最为有效的解决途径。加强对所有无人设备厂商以及持有者的监管，对于厂商严格检查其所有生产线、搭载算法以及设备流通对象，对于所有私人持有的无人设备实行严格的实名制登记管理，让所有合法的无人机拥有其自己的“身份证明”，对于未登记的无人机以及登记但不合法的无人机持有者进行严肃处理 [4]。

2. 伦理安全

社会伦理方面，在民用领域，多无人系统在从事重复性、规则性、可编程的工作内容方面更加快速、高效、精确，不仅可以替代体力劳动，而且可以替代大部分脑力劳动，在制造业、农业以及医疗中发挥主力军的作用，从而导致众多工人面临转业或者失业的问题；在军用领域，由于技术故障、判断失误等原因，在使用多无人协同系统作战时将出现对人类的误伤甚至是误杀。同时，多无人系统各个个体之间，以及多无人系统与人之间的交互建立在信任的基础之上，一旦智能无人系统具备了独立思维能力，将导致机与机甚至人与机之间的冲突。从远期来看，多无人协同系统智能化和自主化水平的不断提升，存在超出人类控制的风险，将可能对人类产生伤害。

人工智能的发展造成工人转业、失业的问题是必然会出现的，在产业结构转型的过程中，旧职业被新职业替代是不可避免的，工业革命的成功同样伴随着大量工人的转业。因此，将视角转向人工智能创造出来的新职业，不应去回避失业、转业的问题，而是在高新技术领域、新兴产业以及现代服务业中加大投入力度，主动推动产业结构的转型升级，鼓励劳动力从第一、第二产业转向第三产业。至于人工智能具备独立思维而对人类造成伤害的问题，以目前技术，这还只是一个遥远的假设，但在未来面对有自主学习能力的人工智能时，可以在其学习初期，将人类价值观中的协同合作、利他主义等内容让其学习，踏出人类与人工智能和谐相处的第一步 [5,23]。

3. 军事安全

当前，国际竞争形势错综复杂，不确定因素所致的安全隐患陡增，保护国家主权和领土完整，抵御外来武装力量的侵略是军事安全的核心，强大的军事实力一直以来都是我国强大的根本，军事安全的重要性不言而喻。多无人系统协同目前在军事上的应用最为广泛，未来的作战模式将由多智能无人武器协同的出现而彻底改变。在军事上，我们不仅要具备抵御外来武装力量入侵的能力，还要具备主动打击外来威胁源的能力 [24]。

我国要加强多无人系统在国防战略中的布局，夯实多无人系统协同技术发展的基础，密切关注世界军事科技和武器装备发展动向，努力抢占科技研发的战略制高点，牢牢把握多无人系统在军事领域发展的趋势，为未来战争中可能存在的各种风险挑战做好准备，推动国防建设跨越式发展，为实现中国梦、强军梦提供坚强力量，为和平与发展这一全人类共同愿望的实现贡献力量。

五、“四位一体”全面推进多无人系统协同安全发展

构建多无人系统安全治理框架，与国际接轨，构筑面向多种无人系统的生态系统。立足创新驱动发展战略，落实多无人系统协同相关理论基础，提升人工智能科技创新能力，充分发挥多学科交叉融合的优势，大力发展智能多无人系统前端技术，建设智能的经济社会体系。建设安全治理法治体系，完善智能多无人系统应用相关的法律法规，建立完善的人工智能社会责任制度，实现新时代的全面依法治国。制定伦理准则，完善人工智能技术研发规范，建设与人工智能和平共处的社会，实现智能化的新时代。

（一）推进无人系统的安全生态建设

为了保障多无人系统协同中人工智能技术的健康发展，构建完善的多无人系统安全治理框架势在必行。通过国际间的交流合作，建立一套面向无人机、无人车、无人艇等多种无人系统的健全的安全评估和监管体系。强化风险把控，针对多无人系统协同技术的内生安全和衍生安全问题，构建多无人系统协同风险评估指标体系，对可能产生的危害及其程度进行评估，划分危险等级，制定相应的安全标准和对策措施，并规范评估程序。建立专门的治理机构，如多无人系统协同安全委员会，统筹管理多无人系统协同的安全发展问题，对多无人系统中的人工智能技术进行安全评估和监管，保障国家人工智能相关安全政策落实到位，并对多无人系统中的人工智能可能带来的就业、公民生命财产安全、隐私安全等社会问题开展研究，并与社会各领域进行广泛的交流与合作，提出可操作的、建设性的政策建议。

（二）推进无人系统的先进技术建设

坚持国际合作与自主创新并举，基础研究与应用落地并行。持之以恒加强多无人系统协同的相关基础理论研究，集中力量突破基础理论和相关产业的薄弱环节，前瞻性瞄准多无人系统技术的新兴方向，重点关注量子人工智能密码 [16]、联邦学习 [17]、对抗样本生成 [18]、分簇自组网技术 [20]、区块链技术 [21] 等与多无人系统的架构安全、通信安全和数据安全等问题紧密相关的基础理论研究。提升人工智能科技创新能力，时刻关注国际上的多无人系统发展动向，学习先进知识和前沿技术，提升自主可控技术的创新能力，保证相关技术的安全性，进一步保障多无人系统协同中的人工智能安全。充分发挥多学科交叉融合的优势，探索多学科交叉融合的有效途径，大力发展智能多无人系统前端技术，建设智能的经济社会体系。立足走中国特色自主创新道路、坚持科技创新与制度创新协同发力、持续加强基础研究三个方面，贯彻新发展理念，彰显对加强自主可控技术与创新的信心与决心，增强自主创新能力，加快建设创新型国家。

（三）推进无人系统的法律规范建设

与时俱进制定并完善人工智能的相关政策和多无人系统协同的相关法律，坚持柔性的原则和规范化的法律相结合，构建以人工智能为特色的新法治体系，为实现全面推进依法治国，加快建设社会主义法治国家提供强力支撑。开展与多无人系统技术应用相关的民事与刑事责任确认、个人隐私安全、数据安全、产权保护等法律问题的研究，建立保障多无人系统协同技术健康发展的法律法规和伦理道德框架。建立健全问责追责制度，明确责任划分、强化责任落实，明确监管者、产品开发者和用户之间的权责关系。重点明确人工智能研究人员在人工智能安全领域的专业责任，要求其通过技术手段来保障多无人系统的安全。围绕自动驾驶、服务机器人等应用基础较好的细分领域，加快研究制定相关安全管理法规，为新技术的快速应用奠定法律基础。根据多无人系统的功能、用途和安全性，建立完善的多无人系统的分类和分级体系。加快推进技术安全标准的制定，细化指标的同时覆盖更多领域。加快国内安全技术标准与国际标准的衔接，向国际领先水平看齐。

（四）推进无人系统的社会伦理建设

多无人系统由于其频繁交互、协同作业的特点，一方面可以大幅改善人类的生活质量，另一方面也可能出现产生独立意识而不可控的安全风险。在多无人系统协同的研发过程中加入伦理设计，将人类价值观中的协同合作、利他主义等内容供其学习，使多无人系统在初始时就具备一定的道德判断

能力。在实际运行过程中，该系统能够遵循人们预设的伦理道德准则，以此杜绝危害人类社会的可能性。由人工智能安全管理机构提出的具体的伦理要求，在产品研发中通过技术手段嵌入伦理道德的要素，并通过政策要求和法律规范予以落实和保障，从思想源头上遏制多无人系统中人工智能技术的可能风险，实现科学技术和人文关怀的统一，踏出人类与人工智能和谐相处的第一步。

六、对策建议

（一）构建国家级无人系统验证平台，推动人才队伍建设

构建“产学研”于一体的自主无人系统公共技术验证平台，为复合型高端人才和高水平创新团队提供沃土。发挥“政产学研”主体活力，引进和培养一批服务基础创新研究和产业健康发展的青年人才，给予平台充分的开放性和资源支持，解决人才队伍后顾之忧。重点突破和验证可控智能演化、可信感知交互和可靠协同控制等与安全应用落地紧密相关的共性关键技术，引导和支持各方共研共建自主无人系统通用安全保障技术体系。

（二）逐步深化无人系统产业“放管服”，发展新一代人工智能安全生态

推动以民用无人系统为代表的人工智能行业准入标准和产品全面深度质检体系的建立，深化“放管服”，以保障实际投入使用的民用无人系统的安全可靠，促进产业生态健康发展。在此基础上，逐步细化无人系统在各细分领域应用的法律法规，制定某些特定领域中，无人系统设计、生产、使用和服务相关人员的资格认证标准，更智慧地把握机遇与应对挑战。

（三）充分发挥多无人系统协同的优势，赋能应用

深入调研以无人系统为代表的新一代人工智能技术和产业发展过程中伴生的社会治安、就业安置、产业安全和国防事业中的新风险，制定局部风险处置预案和总体安全发展规划。在制造业、农业、司法、教育、国防和医疗等领域促进无人系统逐步应用落地，趋利避害，赋能保障和改善民生，服务构建人类命运共同体。实现在无人系统及其协同技术的高速发展和应用阶段平稳过渡，牢牢把握机遇，从容应对挑战。

参考文献

[1] 吴勤. 无人系统发展及对国家安全的影响分析 [J]. 无人系统技术, 2018, 1(2): 62–68.
Wu Q. Unmanned systems development and analysis of the impact on national security [J]. Unmanned Systems Technology, 2018, 1(2): 62–68.

[2] 中华人民共和国国务院. 国务院关于印发新一代人工智能发展规划的通知 [EB/OL].（2017-07-08）[2021-04-27]. http://www.gov.cn/zhengce/content/2017-07/20/content_5211996.htm.
The State Council of the PRC. Notice of the State Council on issuing the development plan for the new generation of artificial intelligence [EB/OL].（2017-07-08）[2021-04-27]. http://www.gov.cn/zhengce/content/2017-07/20/content_5211996.htm.

[3] 中国信息通信研究院安全研究所. 人工智能安全框架2020年 [R]. 北京：中国信息通信研究院安全研究所, 2020.
Security Research Institute of China Academy of Information and Communications Technology. Artificial intelligence security framework 2020 [R]. Beijing: Security Research. Institute of China Academy of Information and Communications Technology, 2020.

[4] 陈伟光. 关于人工智能治理问题的若干思考 [J]. 学术前沿, 2017 (20): 48–55.
Chen W G. Some thoughts on the governance of artificial intelligence [J]. Frontiers, 2017 (20): 48–55.

[5] 杜严勇. 人工智能安全问题及其解决进路 [J]. 哲学动态, 2016 (9): 99–104.
Du Y Y. Artificial intelligence security issues and their solutions [J]. Philosophical Trends, 2016 (9): 99–104.

[6] 王伟嘉, 郑雅婷, 林国政, 等. 集群机器人研究综述 [J]. 机器人, 2020, 42(2): 232–256.
Wang W J, Zheng Y T, Lin G Z, et al. Swarm robotics: A review [J]. Robot, 2020, 42(2): 232–256.

[7] The National Science and Technology Council. The national artificial intelligence research and development strategic plan: 2019 update [EB/OL]. (2019-06-21)[2021-04-27]. https://www.nitrd.gov/pubs/National-AI-RD-Strategy-2019-printer.pdf.

[8] The White House. Guidance for regulation of artificial intelligence applications [EB/OL]. (202011-17)[2020-12-03]. https://www.whitehouse.gov/wp-content/uploads/2020/01/Draft-OMB-Memo-on-Regulation-of-AI-1-7-19.pdf.

[9] CONGRESS. National artificial intelligence initiative act of 2020 [EB/OL]. (2020-03-12)[2021-04-27]. https://science.house.gov/bills/hr6216-national-artificial-intelligence-initiative-act-of-2020.

[10] Congressional Research Service. Artificial intelligence and national security [EB/OL]. (2020-11-10)[2021-04-27]. https://crsreports.congress.gov/product/pdf/R/R45178.

[11] Council of the European Union. European coordinated plan on artificial intelligence [EB/OL]. (2019-02-18)[2020-12-03]. https://www.consilium.europa.eu/en/press/pressreleases/2019/02/18/european-coordinatedplan-on-artificial-intelligence/.

[12] The High-Level Expert Group on AI at European Commission.

Ethics guidelines for trustworthy AI [EB/OL]. (2019-04-08)[2020-12-03]. https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai.

[13] 叶纯青. 欧盟发布无人机通用准则 [J]. 金融科技时代, 2019, 288(8): 89.
Ye C Q. Notice of the European Union on general guidelines for UAVs [J]. Financial Technology Time, 2019, 288(8): 89.

[14] Derakhshan F, Yousefi S. A review on the applications of multiagent systems in wireless sensor networks [J]. International Journal of Distributed Sensor Networks, 2019, 15(5): 1–19.

[15] 王利, 王普, 闫峥. 无人机通信网络安全综述 [J]. 网络空间安全, 2019, 10(9): 13–19.
Wang L, Wang P, Yan Z. A survey on secure communication of unmanned aerial vehicles [J]. Cyberspace Security, 2019, 10(9): 13–19.

[16] 王宝楠, 胡风, 张焕国, 等. 从演化密码到量子人工智能密码综述 [J]. 计算机研究与发展, 2019, 56(10): 2112–2134.
Wang B N, Hu F, Zhang H G, et al. From evolutionary cryptography to quantum artificial intelligence cryptography [J]. Journal of Computer Research and Development, 2019, 56(10): 2112–2134.

[17] 杨强. AI与数据隐私保护：联邦学习的破解之道 [J]. 信息安全研究, 2019, 5(11): 961–965.
Yang Q. AI and Data Privacy Protection: The Way to Federated Learning [J]. Journal of Information Security Research, 2019, 5(11): 961–965.

[18] 刘小垒. 基于群体智能进化算法的对抗样本生成研究 [D]. 成都：电子科技大学 (博士学位论文), 2019.
Liu X L. Research on generation of adversarial examples based on swarm evolutionary algorithm [D]. Chengdu: School of Information and Software Engineering (Doctoral dissertation), 2019.

[19] 伍益明. 恶意攻击下的多智能体系统安全一致性问题研究 [D]. 杭州: 浙江工业大学 (博士学位论文), 2016.
Wu Y M. Research on secure consensus for multi-agent systems under malicious attacks [D]. Hangzhou: Zhejiang University of Technology (Doctoral dissertation), 2016.

[20] 崔朝阳, 孙甲琦, 徐松艳, 等. 适用于集群无人机的自组网安全分簇算法 [J]. 山东大学学报 (理学版), 2018, 53(7): 51–59.
Cui Z Y, Sun J Q, Xu S Y, et al. A secure clustering algorithm of Ad Hoc network for colony UAVs [J]. Journal of Shandong University (Natural Science), 2018, 53(7): 51–59.

[21] 臧义华, 李小娟. 基于区块链的无人集群作战信息共享架构 [J]. 指挥控制与仿真, 2020, 42(4): 19–22.
Zang Y H, Li X J. Unmanned cluster operation information sharing [J]. Command Control & Simulation, 2020, 42(4): 19–22.

[22] 范泉涌, 金茂菁, 黄玲, 等. 无人驾驶汽车的安全问题及对策 [J]. 科技中国, 2019 (6): 13–15.
Fan Q Y, Jin M J, Huang L, et al. The safety problems and countermeasures of unmanned vehicles [J]. Scitech in China, 2019 (6): 13–15.

[23] 李修全. 人工智能应用中的安全、隐私和伦理挑战及应对思考 [J]. 科技导报, 2017, 35(15): 11–12.
Li X Q. Security, privacy and ethical challenges in artificial intelligence applications and their countermeasures [J]. Science & Technology Review, 2017, 35(15): 11–12.

[24] Johnson J. Artificial intelligence, drone swarming and escalation risks in future warfare [J]. The RUSI Journal, 2020, 165(2): 26–36.