以公安机关新质战斗力引领“AI+”时代的新型数字警务生态建设

■ 郭启全

摘　要　“AI+”时代已经来临，数字化智慧化建设和低空经济等新生态迅猛发展，公安机关新质战斗力正逐步形成，本文就如何以公安机关新质战斗力引领“AI+”时代的新型数字警务生态建设，提出参考、意见和建议。

关键词　公安机关新质战斗力　“AI+”时代　新型数字警务生态建设

一、准确把握公安机关新质战斗力规律特点和发展方向，全面提升公安机关新质战斗力

2024年全国公安工作会议对提升公安机关新质战斗力作出了战略部署，这是公安机关落实习近平总书记“加快发展新质生产力，扎实推进高质量发展”重要指示的重大行动。

（一）深化对提升公安机关新质战斗力的系统性规律性认识

公安机关新质战斗力的基本内涵，是以创新为主导、先进技术和大数据为支撑、警务机制改革为途径、高警务效能和高质量为目标，摆脱传统警务模式和战斗力提升路径，形成符合新发展理念以及新时期新征程要求的新型警务运行模式和优质先进战斗力质态。

生产力的传统三要素是劳动者、劳动资料、劳动对象。新时期先进生产力的三要素，劳动者是专业力量专业能力、劳动资料是AI（人工智能）和大数据、劳动对象是大数据。“AI+”时代已经来临，AI是新时期科学技术的代表，是第一生产力。准确把握新时期生产力三要素的发展，以及生产力与生产关系的辩证关系，掌握其内在规律和本质特点，深化对提升公安机关新质战斗力的系统性规律性认识，是形成公安机关新质战斗力的关键。

（二）准确把握公安机关新质战斗力的基本内涵和发展方向

作者：中国警察协会学术委员会委员，公安部十一局原副局长

鉴于 AI 和大数据是新时期生产力的关键要素，及其对社会变革的巨大推动作用，本文提出按照“人工智能技术 + 大数据 + 专业力量专业能力 + 新型警务机制”四位一体、四轮驱动，构建和提升公安机关新质战斗力。人工智能技术 + 大数据 + 专业力量专业能力属于生产力范畴，新型警务机制属于生产关系范畴。构建公安机关新质战斗力，具体包括以下七个方面：一是建立公安机关各警种实战能力图谱，完善支撑公安实战的技术体系，为提升公安机关新质战斗力把握方向、奠定基础；二是以“人工智能技术 + 大数据”为支撑，实现公安业务和能力的提档升级；三是打造新一代“情指行”指挥作战平台，建设一批警察实战训练基地，为构建公安机关新质战斗力提供重要保障；四是建立公安机关新型实战化人才教育训练体系，为公安机关新质战斗力提供人才保障；五是打造“攻防兼备”的高素质公安专业队伍，强化专业力量建设和专业能力提升；六是开展新型公安理论（网络空间地理学）研究，以理论和技术创新支撑公安机关新质战斗力的提升；七是开展“现代警务机制建设”，打造警力调配科学、部门设置合理、作战机制顺畅的新型警务运行模式。

以公安机关新质战斗力为引领，深入研究“AI+”时代的新型数字警务生态建设的方法和途径，大力提升公安业务水平和实战能力，打造攻防兼备的高素质过硬公安铁军，实现公安工作现代化。

二、“AI+”时代已经来临，“AI+”时代社会公共安全和数字警务建设面临的重大风险与挑战

（一）世界已从“互联网 +”时代跨入“AI+”时代，为社会发展进步和变革提供全面支撑

当今世界已从“互联网 +”时代跨入“AI+”时代，AI 技术属于颠覆性技术，正逐步渗透到各行各业和各个领域，成为新一代技术革命和社会变革的核心推动力。一是 AI 技术的突破和快速发展，大大降低了全社会应用门槛，成为了通用技术的核心和数字化智慧化的基石。二是 AI 技术已从重点领域应用发展到全社会大规模广泛应用，催生新业态新生态的涌现，有力支撑各行各业发展进步。三是国家陆续出台《新一代人工智能发展规划》《生成式人工智能服务管理暂行办法》等法律政策，为支持和规范 AI 技术发展应用提供了坚强保障。四是算法、算力协调演进和开源生态的迅速发展，以及国家 AI 发展战略布局和资本大规模涌入，促进“AI+”的范式革命，使 AI 成为了核心推动力和生产力底座。五是国家加快建设信息基础设施、融合基础设施和创新基础设施建设，为 AI 广泛应用提供了有力支撑。

（二）AI 是一把双刃剑，“AI+”时代社会公共安全和数字警务建设面临许多重大风险与挑战

“AI+”时代的社会公共安全和数字警务建设，面临着许多重大风险和挑战：一是网络攻击能力迅速上升。攻击者利用 AI 技术研发网络攻击武器和机器人，7×24 小时不间断攻击，攻击能力、水平和速度显著提升，传统网络安全防御手段和措施难以有效应对。二是违法犯罪活动升级。犯罪团伙和不法分子利用 AI 技术研发超强网络攻击木马病毒等，并借助 AI 技术实施网络攻击入侵、潜伏控制、窃密，利用 AI 进行深度伪造、换脸等，实施诈骗、钓鱼等犯罪活动，给打击违法犯罪带来新挑战。三是大模型自

身存在算法和漏洞隐患。攻击者利用模型自身漏洞实施攻击与欺骗，诱导大模型发送错误决策和判断。同时，攻击者可对大模型的训练数据植入恶意代码，即数据投毒，破坏大模型的决策逻辑。四是数据存在遭破坏和滥用风险。AI 依赖海量数据进行训练，但数据存在泄露、破坏、篡改等风险，导致大模型失效。五是数字化安全风险与 AI 化风险叠加。国家加快推进数字化建设，数字基础设施建设正在走向 AI 化，数字化安全风险与 AI 化风险叠加，给社会安全防范带来更大挑战。六是大模型生成内容存在合规风险。大模型存在时间绕过、地点绕过等风险，利用越狱字符串可突破安全检测，输出违规违法内容。七是低空经济快速发展，社会公共安全和数字警务建设在飞行安全、数据安全、基础设施安全、应急响应等方面面临许多重大风险挑战。

三、准确把握数字警务的本质和内涵，结合“AI+”时代社会公共安全和数字警务建设面临的风险挑战，以公安机关新质战斗力引领“AI+”时代的新型数字警务生态建设

（一）数字化生态建设是国家重大战略行动，在数字化生态建设中同步加强数字化生态安全建设

2021 年以来，国家出台一系列数字化建设的政策文件，包括《国务院关于印发“十四五”数字经济发展规划的通知》《国务院关于加强数字政府建设的指导意见》《数字中国建设整体布局规划》。我国加快推进数字经济、数字政府、数字中国建设，企业开展数字化转型，本质是打造数字化生态，建设数字化智慧化社会。国家从信息化建设发展到数字化建设，数字化生态建设是数字化的最高形态。数字化生态由以下四方面构成：一是数字化生态由基础要素（网络、系统、平台、大模型、智能体、数据、技术等）支撑，二是数据流打通相关领域和行业，三是数据资源得到充分有效利用，四是“AI+ 大数据”全面赋能数字化建设和生产活动，五是同步加强数字化生态安全建设。

数字化生态建设是一个复杂的系统工程，与自然生态建设类似，具有“脆弱性、风险性、长期性和复杂性”等四个特性，建设难，破坏容易。数字化建设面临的最大威胁是网络攻击，为使我国全面建成科学、健康、高质量的数字化生态，保障国家安全和经济社会高质量发展，加快实现中国式现代化，必须大力加强数字生态安全保护。以 AI 和大数据等核心技术为支撑，加强基础要素安全、数据流通安全和数据应用安全，全面构建制度、管理和技术相衔接的数字化生态综合防护体系。

（二）数字警务生态建设是国家数字化生态建设的重要方面，建设新型数字警务生态是“AI+”时代数字警务建设的必由之路和必然选择

公安机关已从“传统警务”跨入“数字警务”时代。新型数字警务生态的基本含义是：以大数据为驱动力，以人工智能等现代技术为支撑和赋能，通过改革创新，对传统警务模式实施数字化、智慧化改造和提档升级，建设数字警员和数字警队，形成数字化智慧化警务生态，全面提升单警作战能力、多警种联合作战能力和公安机关综合实战能力。

新型数字警务生态建设的主要目标是，通过数字基础设施支撑、数据驱动、技术赋能和改革创新，全面推进警务运行和履行职

责的数字化转型、网络集约建设和互联互通，构建数字化智慧化警务新生态，实施多警种合作作战、跨部门协同联动和“挂图作战”，实现侦查办案快速化、社会治理精准化和便民服务高效化，加快实现公安工作现代化。

（三）新型数字警务生态建设的建设思路和主要措施

新型数字警务生态建设的建设思路和主要措施如图 1 所示。

1．加强组织领导和指导

开展新型数字警务生态建设是一个复杂的系统工程，应全面加强新型数字警务生态建设的组织领导、顶层设计和督办落实，组织制定数字警务建设战略规划和年度计划，科学确定数字警务建设的目标和主要措施。成立专家组，科学指导新型数字警务生态建设。

2．开展战略规划和战术设计

新型数字警务生态建设需要采用工程的思维、方法和路线制定战略规划，包括数字警务建设指导思想、建设原则、建设目标、主要任务、时间表、路线图、组织领导、考核评价等内容。在战术上需要设计具体措施，加强改革创新，落实战略规划，主要包括：能力图谱构建—基础设施支撑—大数据驱动—警务场景刻画—AI 赋能—打造数字警员警队—“挂图作战”—治理体系—理论技术创新—基地建设—“三化六防”—数字警务生态安全—评价和改进等内容。

3．构建公安机关业务能力图谱

各警种、各部门应按照新型数字警务生态建设要求，设计并建立业务能力图谱，为建设新型数字警务生态把握方向、奠定基础。一是情报获取能力，包括情报侦察、情报分析、情报挖掘、情报使用等；二是刑事执法能力，包括线索获取、勘查取证、精准打击等；三是行政执法能力，包括行政处罚、监督管理等；四是治安管控能力，包括风险监测、预知预判、预警预防、风险防控等；五是应急处突能力，包括指挥调度、突发事件应对、快速处置、警力调度、社会动员等；六是科技支撑能力，包括理论创新、技术攻关、科技赋能等；七是队伍建设能力，包括人才培养、专业训练、实战能力提升等；八是综合保障能力，包括实训基地、武器装备、法律政策、标准规范、经费、机构编制、国

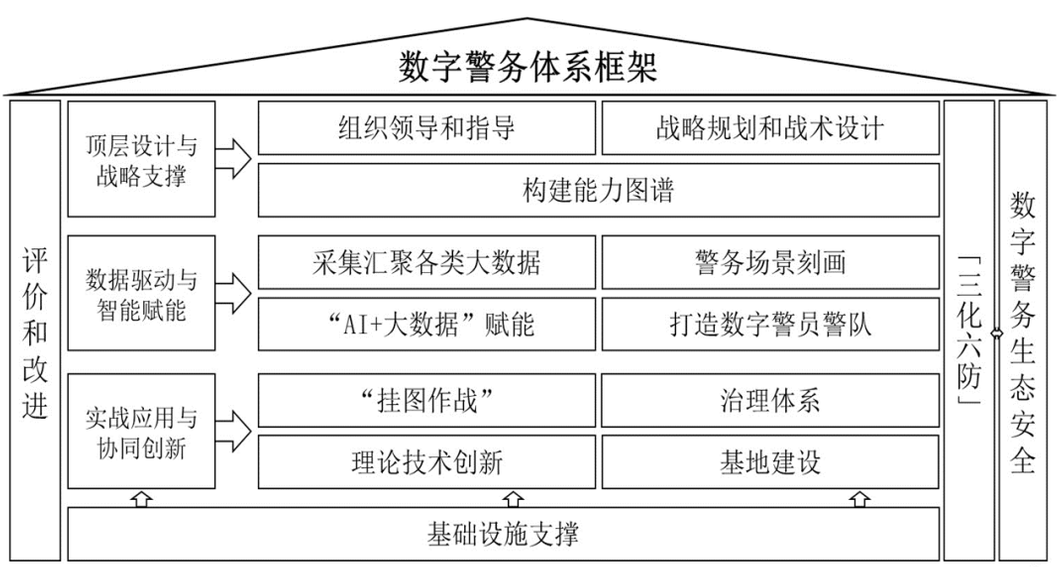

图 1 新型数字警务生态建设框架

际合作等。

4．建设完善数字警务基础设施

充分利用卫星互联网、算力网络等国家数字化基础设施，研发新一代公安网络、业务系统、云平台、大数据中心、算力中心等基础设施，建设完善数字警务底座和基础数据库、业务数据库，指挥作战平台、态势感知平台等设施，为数字警务建设提供支撑和保障。

5．采集汇聚各类大数据

实施新型警务的数据驱动和智慧化应用。利用互联网、视频监控、交通管理、物联网、无人机等多种渠道和方式，采集汇聚各类大数据；打破警种壁垒和数据孤岛，按照有关标准，汇聚公安内部数据；打破行业壁垒，建立跨部门数据共享机制，汇聚社会大数据；建设数据链、新型数据湖、警务云，汇聚各警种、各部门、各渠道大数据，实现大数据的采集、汇集存储。

6．深入刻画数字警务场景

公安机关各警种、各部门都应研究数字警务场景，经侦、治安、刑侦、反恐、环食药、网安、禁毒、交通、铁警、空警等警种，深入刻画情报获取、犯罪预防、犯罪线索挖掘、侦查办案、监督管理、行政执法等具体业务场景；情指中心、办公厅（局）、科信、人训等有关部门，也需要深入刻画具体业务场景，为“AI+ 大数据”的算法设计、建模和 AI 应用把握方向。

7．利用“AI+ 大数据”全面赋能警务活动

利用 AI 技术升级改造数字警务基础设施，研发数字机器人；利用大数据驱动警务活动，开发数字警务大模型、智能体；开展数据建模，依托海量数据、专业数据、历史数据和大模型进行数据挖掘，对案事件和犯罪嫌疑人进行“画像”，或形成有价值的情报，为“情报主导警务”赋予新的内涵，为开展违法犯罪的预知预判、预警预防、案件侦办、社会公共安全治理、公众服务等警务活动提供强大动力，有力提升警务效率和能力。

这里以一个网络攻击检测大模型（天查机器人）和网络攻击检测 AI 团队（AI 智能体）研发部署为例，给出利用 AI 和大数据技术研发专业数字机器人及数字作战团队的方法流程。

研发设计网络攻击检测大模型（天查机器人），用于网络攻击渗透测试。研发设计网络攻击检测大模型的方法和流程，如图 2 所示。

第一步，数据准备。为完成网络攻击检测专门任务，采集汇聚所需要的数据，例如漏洞详情数据、攻击报文数据、告警分析数据、推理通用数据、公开渠道搜集的数据，利用自动化手段将原始数据转变成标准数据，达到高质量大模型的数据集规模要求；第二步，数据语料蒸馏审核和标注。选择优秀模型（如 OpenAI）蒸馏数据，通过聚类算法，对数据进行分组，筛选数据并标记，解决数据多样性和重复筛选问题；第三步，为大模型配置硬件设施。选择配置多组服务器，形成大模型集群架构；第四

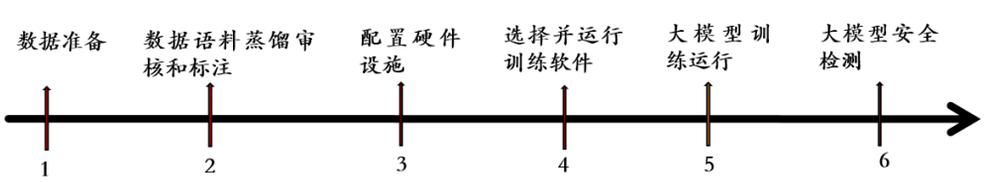

图 2 网络攻击检测大模型（天查机器人）的方法和流程

步，选择并运行训练软件。可选择开源软件 LLaMA-Factory，准备好基础模型和标注好的数据，启动微调 / 训练程序；第五步，大模型训练运行。按照预训练模型 BERT（Bidirectional Encoder Representations form Transformers，一种自然语言处理领域的预训练模型），开展大模型训练运行；第六步，经过预训练，获得大模型的 gguf 文件，即设计制造出网络攻击检测大模型。第七步，大模型安全检测。按《生成式人工智能服务安全基本要求》，利用大模型对网络攻击检测大模型进行安全检测，以模测模，确保其语料安全、算法安全和应用安全，检测合格后即可投入使用。利用天查机器人，可以实施网络攻击检测活动。

研发设计网络攻击检测 AI 团队（AI 智能体），用于多角色联合开展网络攻击渗透测试。

网络攻击渗透测试主要包括通用漏洞验证分析和验证、逻辑漏洞生成与验证、资产暴露面检查、系统上线漏洞检测、重大活动网络安保检测、事件应急检测等活动，这些业务活动通常需要渗透策划师、信息探测师、渗透工程师、情报分析师、脚本编辑师等多人完成。在研发设计网络攻击检测大模型（天查机器人）基础上，利用 AI 和大数据技术，升级制造出第二代天查机器人，研发设计网络攻击检测 AI 智能体（AI 渗透策划师、信息探测师、渗透工程师、情报分析师、脚本编辑师），如图 3 所示，替代人，建立网络攻击渗透测试 AI 团队，开展网络攻击检测活动。

图 3 中的 AI 红客团队通过群体智能的方式，完成自动化攻击渗透测试任务。智能体使用 Function calling 和 MCP 技术与通用大模型配合，调用不同功能模块。借助天查大模型的分析与规划能力，提升在信息探测、攻击面分析、漏洞分析验证和利用、高价值数据分析和文件处理等方面的智慧化自动化能力。

8．打造数字警员和数字警队

利用“AI+ 大数据”技术研发警务活动支撑平台、单警装备，对全警开展数字化培训和技术训练，使每位干警都能掌握数字化平台和数字化装备的使用、数字化工作流程，打造数字警员；培养一批 AI 数据分析师，培养干警利用数字化警务平台密切协同、联合作战，打造数字警队，提升单兵和警队的

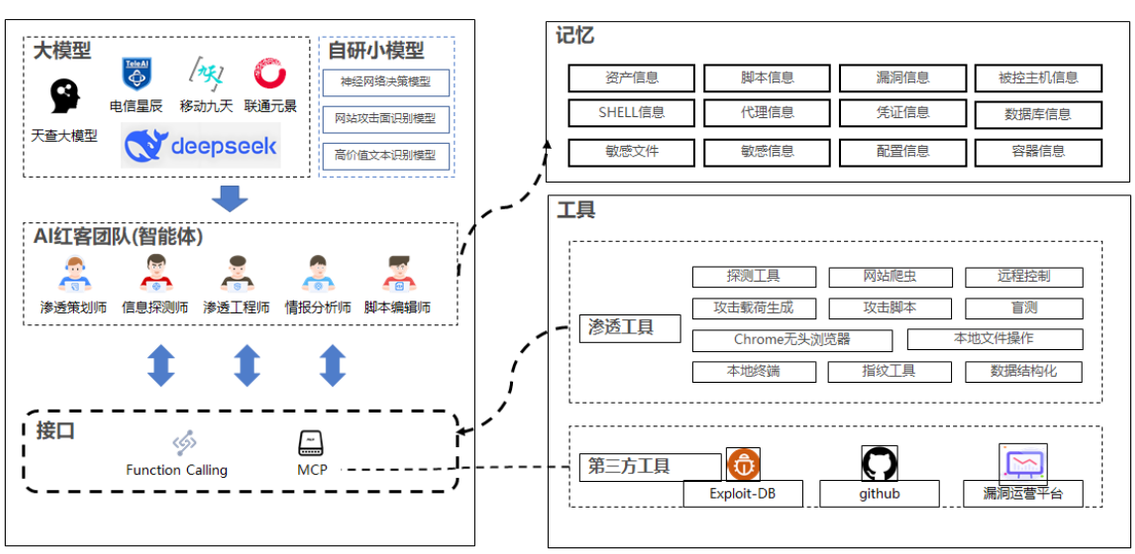

图 3 网络攻击检测 AI 智能体

接处警能力、侦查办案能力和快速处突能力。

9．实施“挂图作战”

从提升指挥作战能力出发，按照“实战化、体系化、科学化”三化要求，以大数据为支撑，利用 AI 开发平台“智慧大脑”，利用“AI+ 大数据”技术，打造新一代“情指行”综合指挥作战平台，建立全业务全链条图谱，将人、地、事、物、网、空域、组织等全要素上图，实现警务活动可视化、警力调度可视化、警务环境可视化，实施“挂图作战”，有效提升快速响应和指挥作战能力。

10．构建数字警务治理体系

数字警务治理体系包括数字化组织、数字化管理和数字化治理。在数字警务建设中，建立数字化治理机制，统筹协同队伍、技术、数据和流程，优化组织结构和职能，提升警务效率和警务能力；创新管理模式和工作方式，充分调动广大干警的创造力和主动性，建立“群防群治”新业态；培育数字警务文化，将数字警务建设转化为全警的自觉行动。

11．理论技术创新

理论、技术与实战紧密结合、三位一体，是建设新型数字警务生态的新引擎。公安机关战斗在现实空间和网络空间，按照“理论支撑技术、技术支撑实战”的理念，研究《网络空间地理学》，利用地理学的理论、方法论和成果，深入研究网络空间与现实空间的内在关系和作用机制，掌握规律特点，发展公安新理论。在理论指导下，突破网络空间智能认知技术、资产测绘技术、画像与定位技术、可视化表达技术、地理图谱构建技术、行为认知和智能挖掘技术等一批核心技术，为各警种的警务活动提供理论指导、技术支持和实战支撑。

12．建设一批新型警察实战实训基地

按照“教战训结合”原则，公安机关与公安院校、地方高等院校、重要企业、研究机构联合建设一批实战实训基地，将现有警察培训基地打造成新型警察实战训练基地，开展新型实战训练。同时，利用基地集中开展技术攻关，采用 AI、大数据、可信计算、密码、数字孪生、量子等技术，结合国家数字化生态建设、低空经济、无人无线领域、智慧化建设、大模型研发应用、无人机系统、机器人等新业态新生态，研究警用新技术、新产品和新装备。

13．落实“三化六防”要求

在新型数字警务生态建设中，工作上落实“实战化、体系化、科学化”要求，措施上落实“动态防控、主动防控、纵深防控、精准防控、整体防控、联防联控”的“六防”要求， 建立新时期社会治安综合防控体系和网络社会综合防控体系。

14．同步加强数字警务生态安全

以 AI 技术为核心，密码技术为基石，量子、大数据、区块链、可信计算、数字孪生等技术为支撑，全面构建制度、管理和技术相衔接的数字警务综合防护体系：加强公安网络、大系统、大平台等数字警务基础要素安全；对数据进行分类分级管理和保护，加强从数据采集、汇集、存储、应用、提供、流通、销毁全生命周期全过程的安全管控，保护数字警务生态安全，提升技术防护能力。

15．科学评价和持续优化改进

建立数字警务评价体系，制定评价方案，确定评价目的、流程、方法、要求，收集评价信息，遴选评价专家，开展综合分析和评价，形成评价结果。对数字警务建设中的问题和不足，应经过科学论证后加以改进，持续进行优化和迭代，最终实现新型数字警务生态建设目标。

责任编辑　马煜童