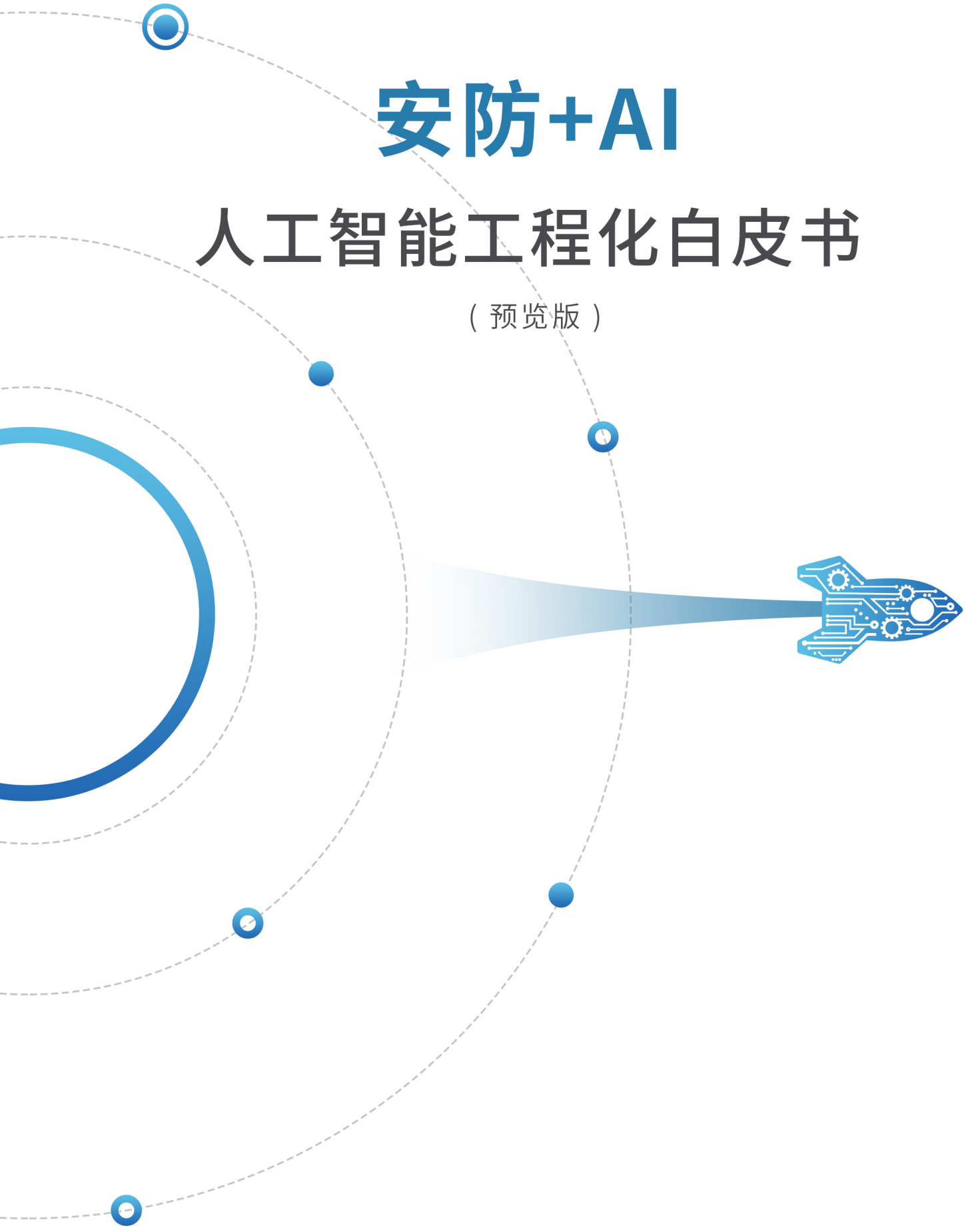
安防+AI

人工智能工程化白皮书

（预览版）



中国科学院自动化研究所 Institute of Automation, Chinese Academy of Sciences

uniview 宇视研究院

联合出品

CONTENTS

目录

前言 1

第一章 背景 3
1.1 从自动化迈向智能化时代 3
1.2 三个框架奠定产品化基础 4
1.3 各国政策规划和智慧安防 9
1.4 安防+AI的爆发 12

第二章 智慧安防生态 17
2.1 基础硬件 17
2.2 云平台 20
2.3 软件框架 20
2.4 基础算法 21
2.5 产品及行业应用 21

第三章 智慧安防典型应用 22
3.1 卡口场景:人脸身份确认应用 23
3.2 卡口场景:人脸身份验证应用 23
3.3 卡口场景:车辆识别应用 24
3.4 非卡口场景:视频结构化分析与快速检索应用 24
3.5 非卡口场景:行为分析辅助安防应用 24

第四章 智慧安防规模应用的八大限制性因素 24
4.1 成本高昂 25
4.2 算法场景限制高 26
4.3 布点困难 27
4.4 网络和安全要求更高 28
4.5 深度应用不足 30
4.6 系统性顶层设计 31
4.7 缺乏行业标准与评估体系 32
4.8 用户学习与组织保障成本更高 32

第五章 八大新趋势造就智慧安防新未来 33
5.1 工程的科学布点 33
5.2 产品的云端结合 33
5.3 AI分布式计算 35
5.4 数据的多维应用 36
5.5 数据和网络安全 36
5.6 下一代人机交互技术 39
5.7 系统设计及项目实践能力不断提升 39
5.8 非卡口存量视频逐步应用 40

参考文献 42
研究与撰写团队 43

前言

近年来，人工智能迎来了第三个发展高峰期。在计算、大数据、深度学习等技术的综合作用下，人工智能技术得以大幅度提升。在很多应用领域，人工智能被给予很大期望，最乐观的预期认为可以带来人类文明的第四次工业革命。过去几年里，中国公共安全视频建设经历了飞速发展的黄金时期，适逢人工智能技术取得突破性进展，以人脸识别为代表的人工智能（主要是机器视觉）在安防行业迅速落地，诞生了一系列初具成效的应用，也存在虚张声势的营销。

批评者指出，人工智能当前的主要矛盾，是业界的营销能力和 PPT 水准，远远领先于用户的真实需求和实战准备；人工智能序幕揭开，算法仍有很多发展空间，对于算法落地难、实战差，工程化是今后要解决的问题。实践者认为，任何一项技术，其生命力由商业化应用的程度决定，只有将技术转化为产品，形成解决方案，最终转化为用户的有效利用，才能形成技术和价值的良性循环。

在顶层设计方面，中国政府对人工智能发展战略的高度重视。自 2015 年 6 月以来，中国密集发布了 7 项关于人工智能的政策与规划，并倡导将人工智能技术应用于公共安全领域，进行技术创新、产品创新和应用创新。

在技术创新层面，传统的安防企业、新兴的 AI 初创企业，都开始积极从技术各个维度拥抱人工智能，在模式识别基础理论、图像处理、计算机视觉以及语音信息处理展开了集中研究与持续创新，探索模式识别机理以及有效计算方法，为解决应用实践问题提供了关键技术，具备了原创性技术的突破能力。

在产品应用层面，很多企业推出了系列化的前后端 AI 安防产品，理论上满足了许多典型场景下的实战应用需求。人工智能技术的不断进步，传统的被动防御安防系统将升级成为主动判断和预警的智慧安防系统；安防从单一的安全领域有望向多行业应用、提升生产效率、提高生活智能化程度方向发展，为更多的行业和人群提供可视化、智能化解决方案。

智慧安防的技术基础和产品化已趋成熟，因此在下一阶段的命题就是如何系统化规模部署。挑战与机遇并存，从技术手段的不断革新到产品形态的成熟落地，智慧安防仍然面临众多难题，诸如成本高昂、工程化布点困难、算法场景局限大、缺乏深度应用、缺乏系统性顶层设计、缺乏满足实战应用的行业标准与评估体系等。能够在多大程度上解决这些问题，关系着智慧安防产品和方案能否真正的落

地生根。

安防+AI 前景可期，久久为功。国内的学术界及实业界积极尝试将人工智能应用于安防领域，正视问题，研究方法，实践中总结改进，稳健推动安防行业的第三次升级。『安防+AI 人工智能工程化白皮书』集合了中科院自动化所、浙江宇视科技有限公司的技术专家及行业专家的研究成果、实践经验。本报告从当前人工智能技术与产业发展的背景、智慧安防生态圈、智慧安防典型应用、智慧安防规模化应用存在的问题，以及智慧安防未来趋势等五个维度，系统梳理总结了当前安防+AI 的发展现状，尤其重点分析指出了智慧安防领域存在的八大限制性因素，以及智慧安防的八大新的发展趋势，供学术界及实业界的学者、专家参考。

由于编写时间仓促，本报告存在一定的不足，欢迎业内各界人士批评指正；作为一个开放系统，也欢迎其他国内外的机构和企业加入汇聚自己的经验智慧。

中科院自动化所、宇视研究院报告团队

2018 年 11 月于乌镇

第一章 背景

1.1 从自动化迈向智能化时代

人工智能始于 20 世纪 50 年代，至今大致分为三个发展阶段：

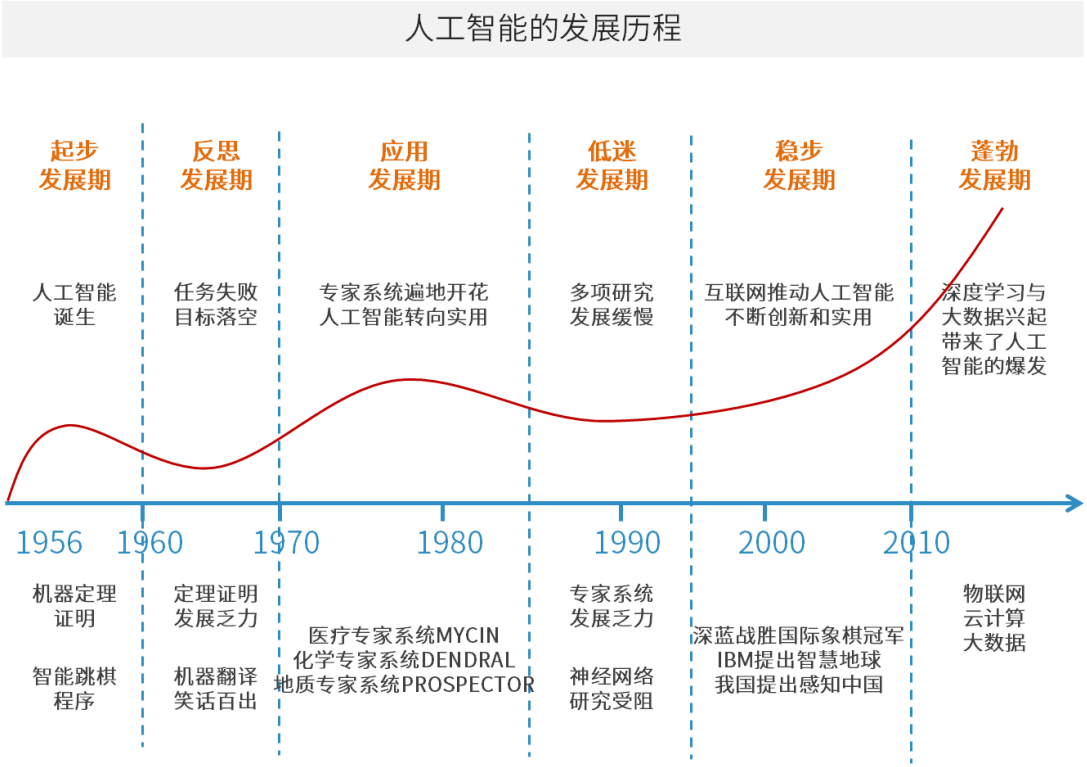
第一阶段（20 世纪 50 年代——80 年代）：形成了基本的人工智能，但还远远不及智能化水平。符号主义理论快速发展，一些基础的算法理论得到证明。计算机的出现，人工智能的实际应用具备了硬件条件；但是硬件设备的计算能力极为有限，难以处理复杂性更大的计算任务。

第二阶段（20 世纪 80 年代——90 年代末）：专家系统得到快速发展，数学模型有重大突破。计算机从完成单纯的数学和逻辑运算，演变为执行知识库的自动化工具。这一阶段的专家系统需要人们把知识总结后灌输给计算机，计算机只能按规则应用这些知识，无法从数据中自行获取知识。

第三阶段（21 世纪初——至今）：随着大数据的积聚、算法理论的革新、计算能力的提升，尤其是深度学习技术的发展，机器实现了分析数据，从而自动学习出知识能力。

从人工智能的发展历程来看，深度学习（深度神经网络）推动了本轮人工智能的发展，本质上是多层次的人工神经网络算法，即从结构上模拟人脑的运行机制，从最基本的单元上模拟了人类大脑的运行机制。当前基于深度学习的人工智能技术架构下图所示：

图 1[1]：人工智能发展历经 6 大时期，深度学习推动本轮发展

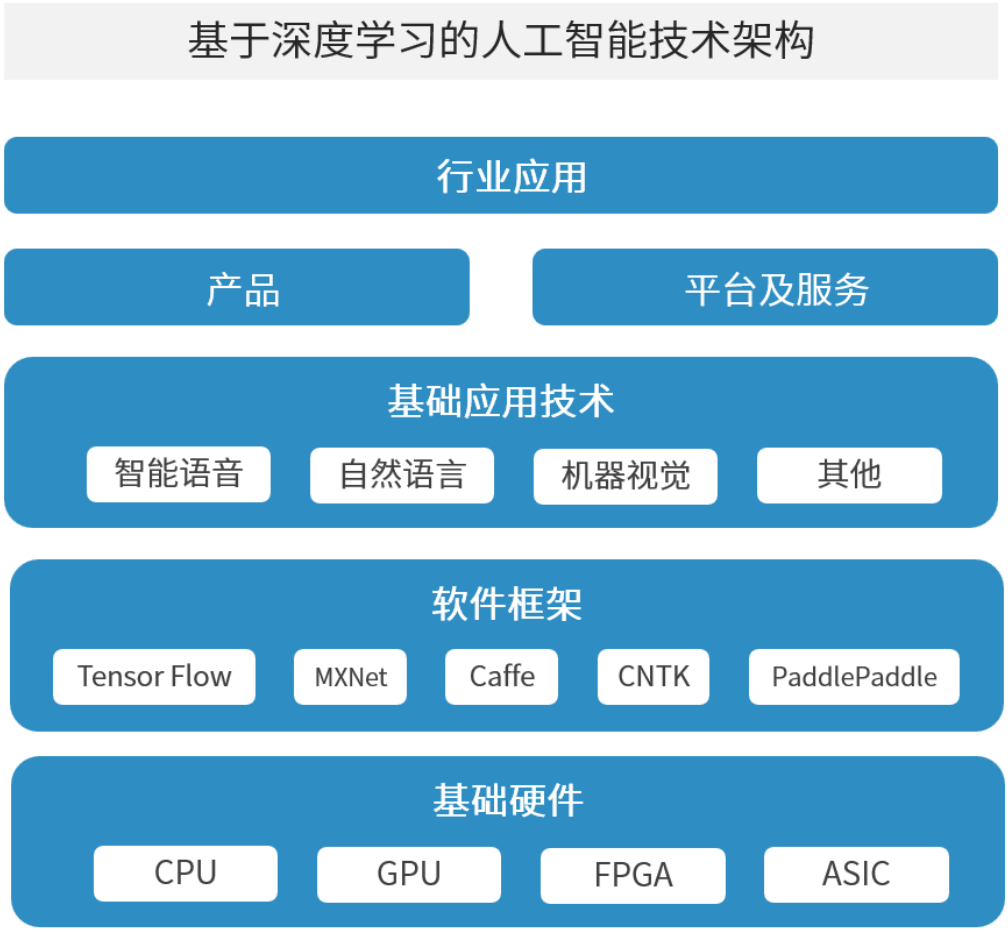


1.2 三个框架奠定产品化基础

从人工智能的技术架构来看，得益于基础硬件的强化与软件框架的优化，使这一轮人工智能的爆发式增长得以实现。而基础应用技术的进一步研发则使人工智能从抽象技术实现了向可及性产品与服务的转变。

[1]数据来源：《中国科学院第十九次院士大会报告》

图 2[2]：基于深度学习的人工智能技术架构得益于软硬件的优化

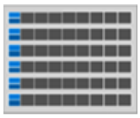
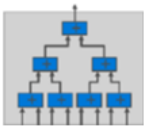
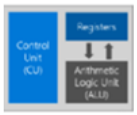
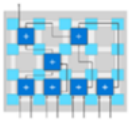


基础硬件层为算法提供了基础计算能力。涵盖 GPU、CPU、FPGA、ASIC。

[2] 数据来源：《人工智能发展白皮书技术架构篇》

图 3[3]:基础硬件提供基础算力，四大类硬件各有特点

四大类硬件特点比较

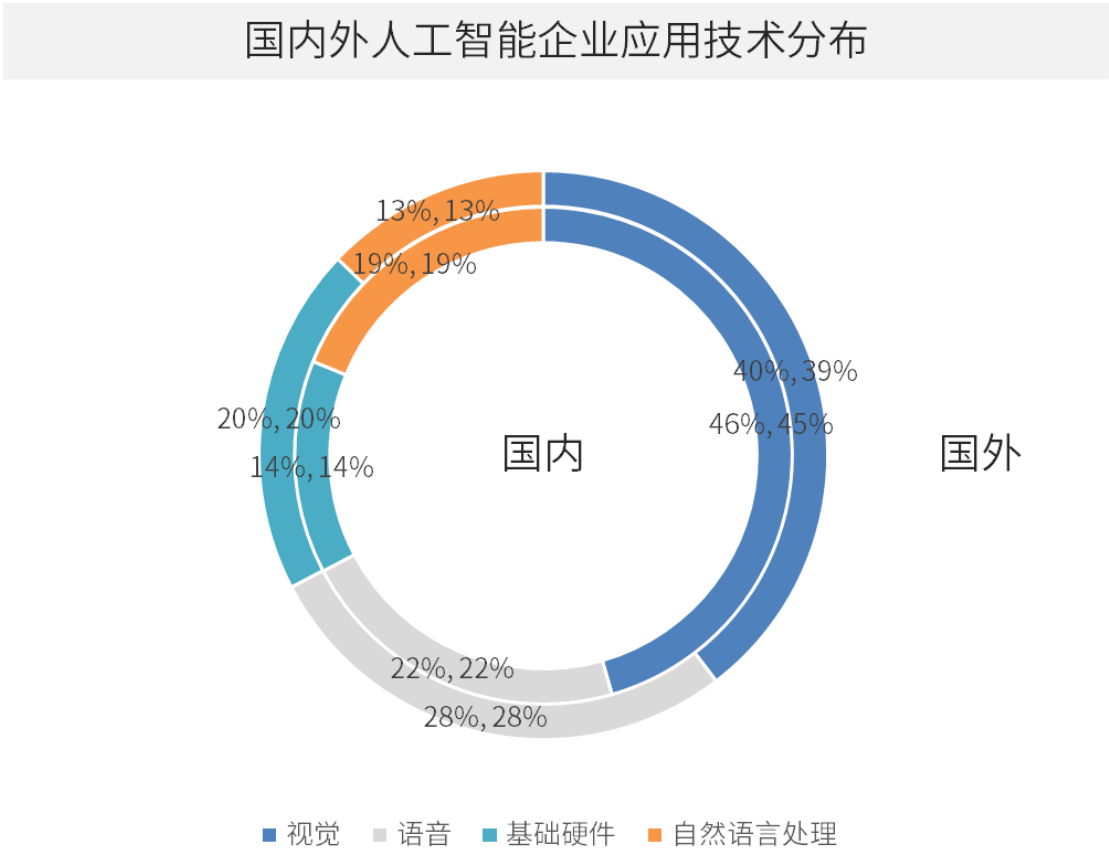
类别	GPU	ASIC	CPU	FPGA
特点	1、可多达上千个简单核心，上千个并行硬件线程； 2、并行运算能力，浮点运算能力强大； 3、最大化浮点运算数据吞吐量。 	1、需求确定后可进行专门优化设计； 2、优秀的功耗控制； 3、性能稳定，可靠性高； 	1、通用性强； 2、核心复杂程度高； 3、串行运算能力强，单线程性能优化； 4、晶体管空间用于复杂并行性指令（Complex ILP） 	1、电路级别的通用性； 2、可编程性； 3、适用于开发周期较短的IOT产品、传感器数据预处理工作以及小型开发试错升级迭代阶段； 

软件框架层实现算法的模块化封装，为应用开发提供集成软件工具包。该层涵盖范围包括针对算法实现开发的各类应用及算法工具包，为上层应用开发提供了算法调用接口，提升应用实现的效率。

算法框架是人工智能核心生态圈建立的关键环节，是决定人工智能技术、产业、应用的核心环节，是人工智能核心生态圈建立的基础和关键。

[3] 数据来源：微软 build、谷歌官网、天风证券研究所整理

图 4[4]：国内外人工智能企业应用技术分布，计算机视觉占比较高



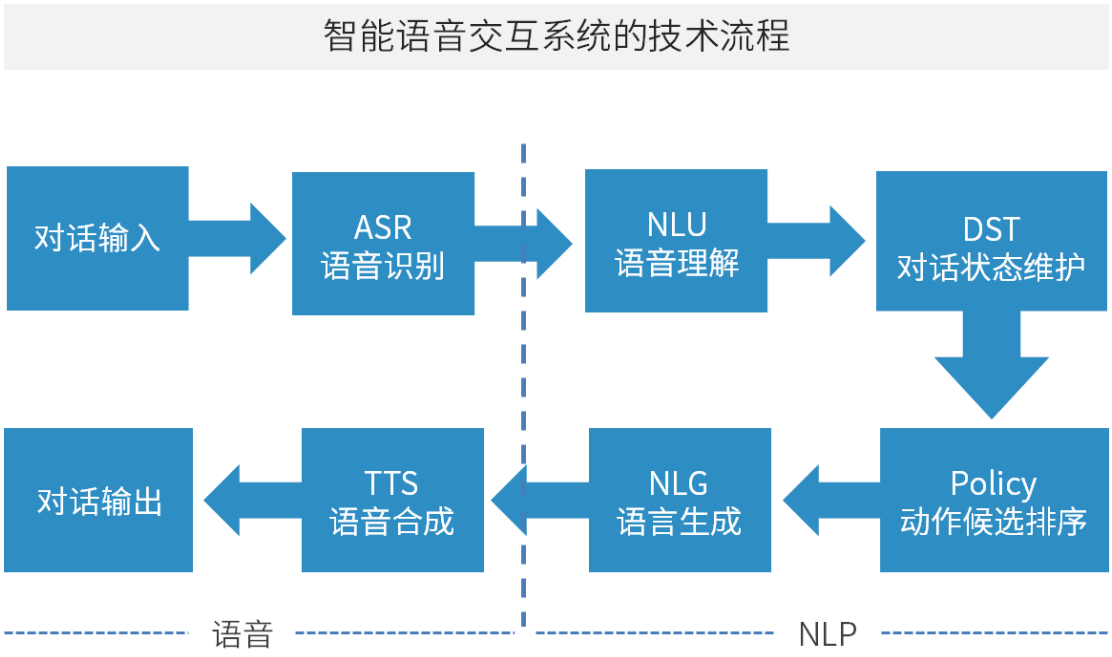
当前人工智能的商业化实现主要是基于计算机视觉、智能语音、自然语言处理等基础应用技术实现，并形成了相应的产品或服务。

目前国内外人工智能企业应用的技术主要是计算机视觉和智能语音语义两个方面。

自然语言是人与人沟通交流最主要的手段。智能语音语义的核心是研究人与计算机直接以自然语言的方式进行有效沟通的各种理论和方法。自然语言处理技术仅在特定领域取得了较好的应用，鲁棒性存在大量挑战，学术发展和产品应用上都有非常大的空间。

[4] 数据来源：《中国人工智能发展报告 2018》

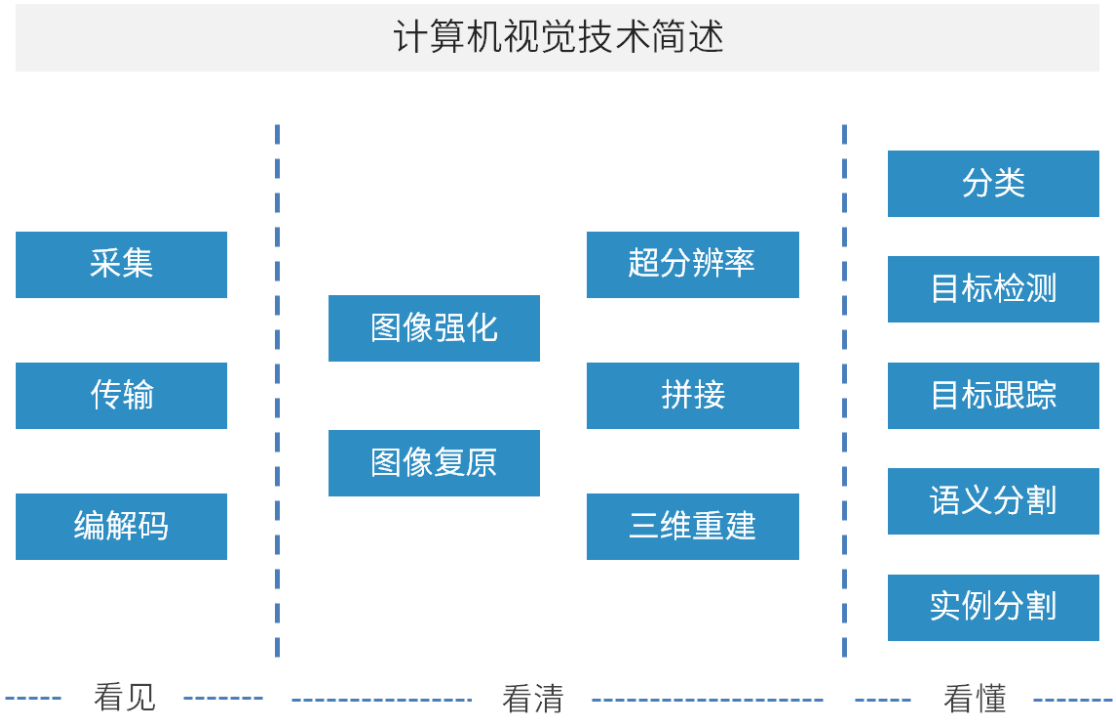
图 5[5]：智能语音交互系统技术流程，发展应用潜力大



计算机视觉的目的是建立能够从图像或者多维数据中获取信息的人工智能系统。得益于深度学习算法的成熟应用，侧重于感知智能的图像分类、目标检测等技术已经逐步实现商用价值。但现阶段的视觉技术往往仅能利于影像表层信息，缺乏对事物功能、因果、动机等深层信息的认知把握，在技术层面仍有很大的探索空间。

[5] 根据网上公开资料

图 6[6]：计算机视觉简述，逐步实现商用价值



1.3 各国政策规划和智慧安防

人工智能被认为是第四次工业革命的主要使能技术，获得了各行业的极大关注。为了抓住 AI 发展的战略机遇，越来越多的国家和组织已经相继制定国家层面的发展规划。

[6] 根据网上公开资料总结

图 7[7]:世界人工智能产业政策指导，各国紧抓 AI 发展

世界人工智能产业政策指导

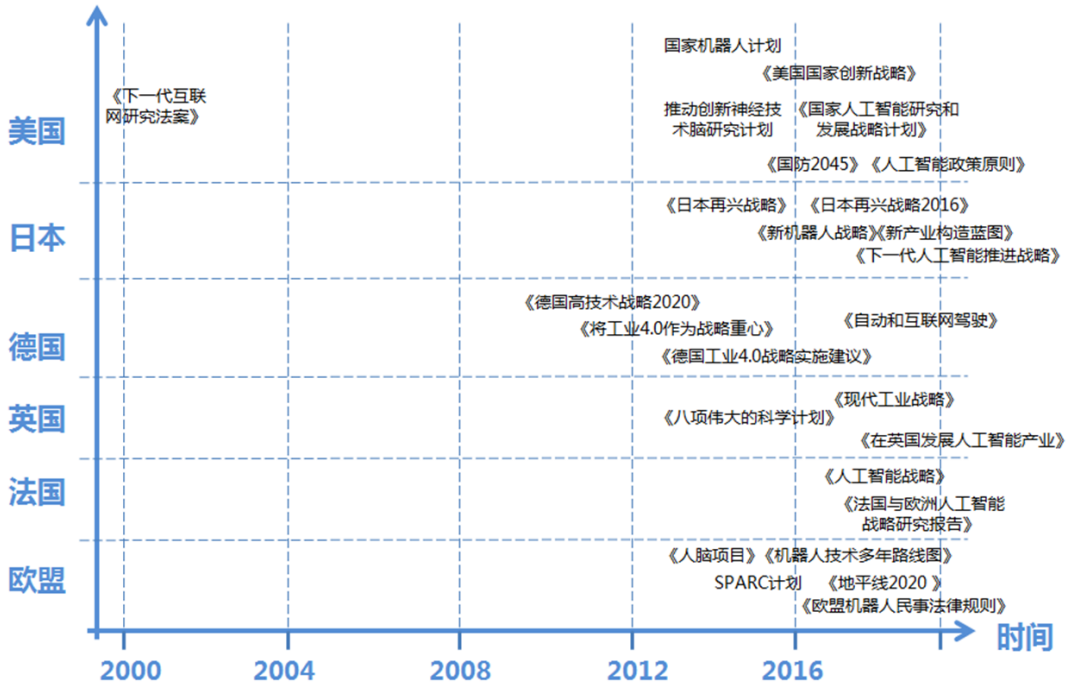


表 1[8]：各国制定人工智能政策研发战略

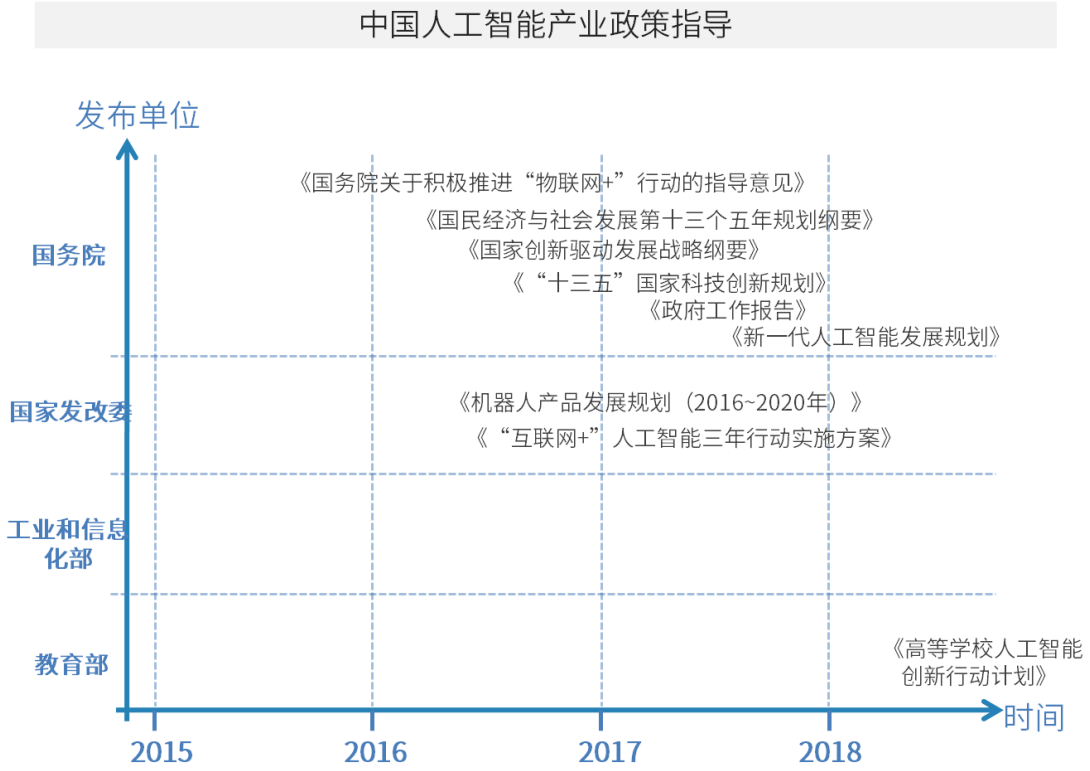
世界各国人工智能政策研发策略比较分析

	重点研发领域	重点应用领域
美	特朗普总统FY2019预算要求是美国历史上第一个指定人工智能和自主、无人系统作为行政研发重点的预算。特朗普政府的《让美国再次伟大的预算蓝图》中对国土安全、军事国防、医疗给予重点支持	国土安全领域：脸部识别，FLOOD APEX PROGRAM项目，可穿戴警报系统等(国土安全局已出台《人工智能白皮书》,《就有关新兴技术战略执行概要向总统的报告（拟）》）； 医疗影像(已出台《医疗影像研究和发展路线图》,有提到人工智能和医学影像的协调）； 国防军事（特别项目通告//2018海军研究办公室//基础研究机会：“促进海军领域的人工智能研究”）
欧盟	数据保护；网络安全；人工智能伦理；数字技术培训；电子政务	超级计算机；数据处理；金融经济；数字社会；教育
德	人机交互；网络物理系统；云计算；计算机识别；智能服务；数字网络；微电子；大数据；网络安全；高性能计算	智能交通（陆海空）健康护理；农业；生态经济；能源；数字社会
英	硬件CPU；身份识别	水下机器人；海域工程；农业；太空宇航；矿产采集
法	超级计算机	生态经济；性别平等（对女性的AI教育）；E-Government；医疗护理
日本	机器人、脑信息通信、声音识别、语言翻译、社会知识解析、创新型网络建设、大数据分析等	生产自动化、物联网 医疗健康及护理，空间移动（自动驾驶、无人配送等）
中	关键共性技术体系“1+N”计划: “1”是指新一代人工智能重大科技项目，聚焦基础理论和关键共性技术；“N”是人工智能的理论研究、技术突破和产品研发应用。 加强人工智能前沿领域交叉学科研究和自由探索的支持。	智能制造；智能农业；智能物流；智能金融；智能商务；智能家居；智慧教育；智能医疗；智能养老；行政管理；司法管理；城市管理；环境保护 在深海空间站健康保障等重大项目，以及智慧城市、智能农机装备等国家重点研发计划重点专项部署中，加强人工智能技术的应用示范

[7] 数据来源：《2018 世界人工智能产业发展蓝皮书》
[8] 信息来源：《中国人工智能发展报告 2018》

中国高度重视人工智能发展，2015 年后密集发布人工智能相关政策和规划。

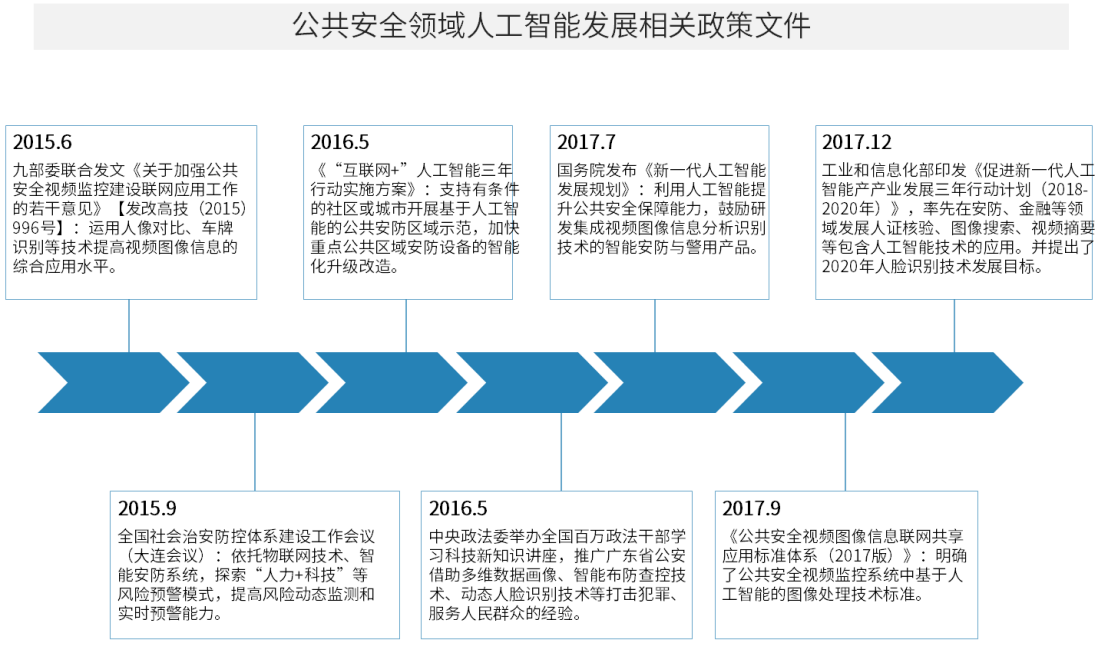
图 8[9]：中国高度重视人工智能发展，密集发布相关政策规划



在人工智能应用领域，我国智慧安防领域走在了世界的最前沿。在国内众多关于人工智能的政策、发文、规划中多次提到将人工智能技术应用于公共安全领域，进行技术创新、产品和应用创新，同时相关部门也提出并发布了在视频监控应用中基于人工智能的视频图像处理技术标准。

[9] 数据来源：《2018 世界人工智能产业发展蓝皮书》

图 9[10]：公共安全领域人工智能发展相关政策，中国走在世界前沿

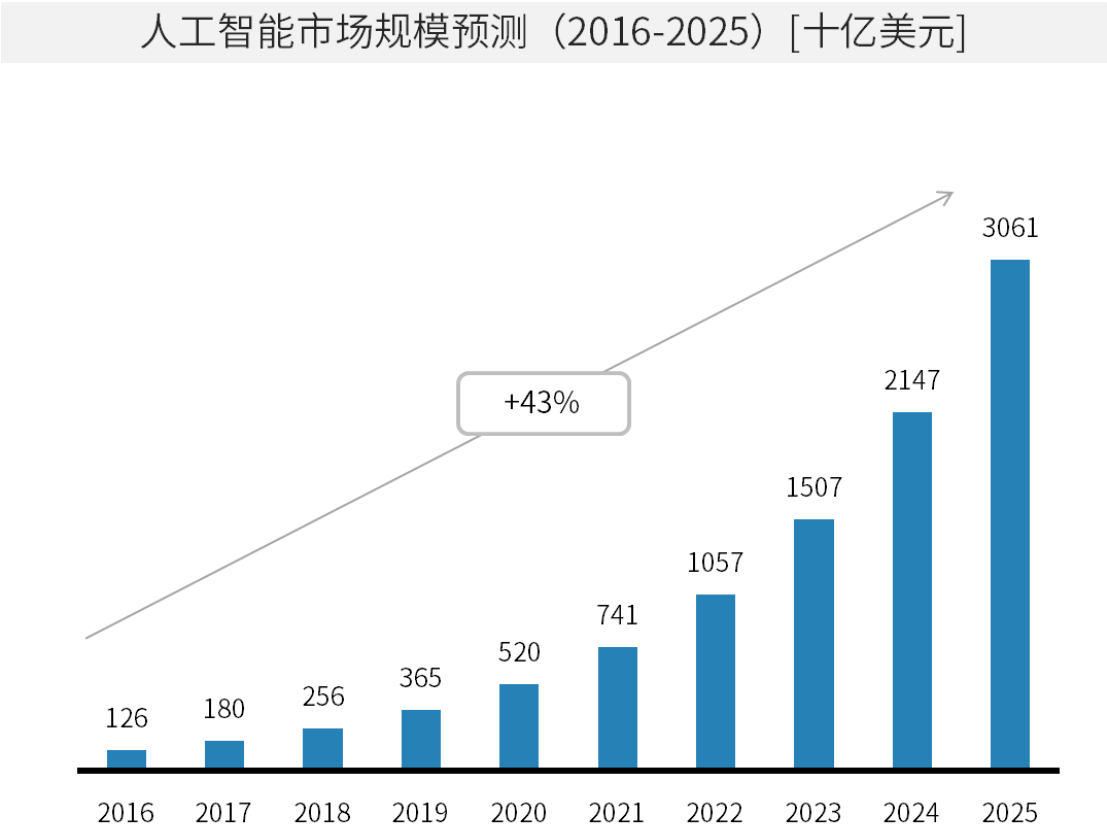


1.4 安防+AI 的爆发

全球 AI 相关产品业规模庞大。据中国人工智能学会和罗兰贝格咨询公司预测，2016 年至 2025 年，全球人工智能市场规模年均增速超过 40%，2025 年将达到 3 万亿美元。

10 数据来源：宇视根据公开信息整理

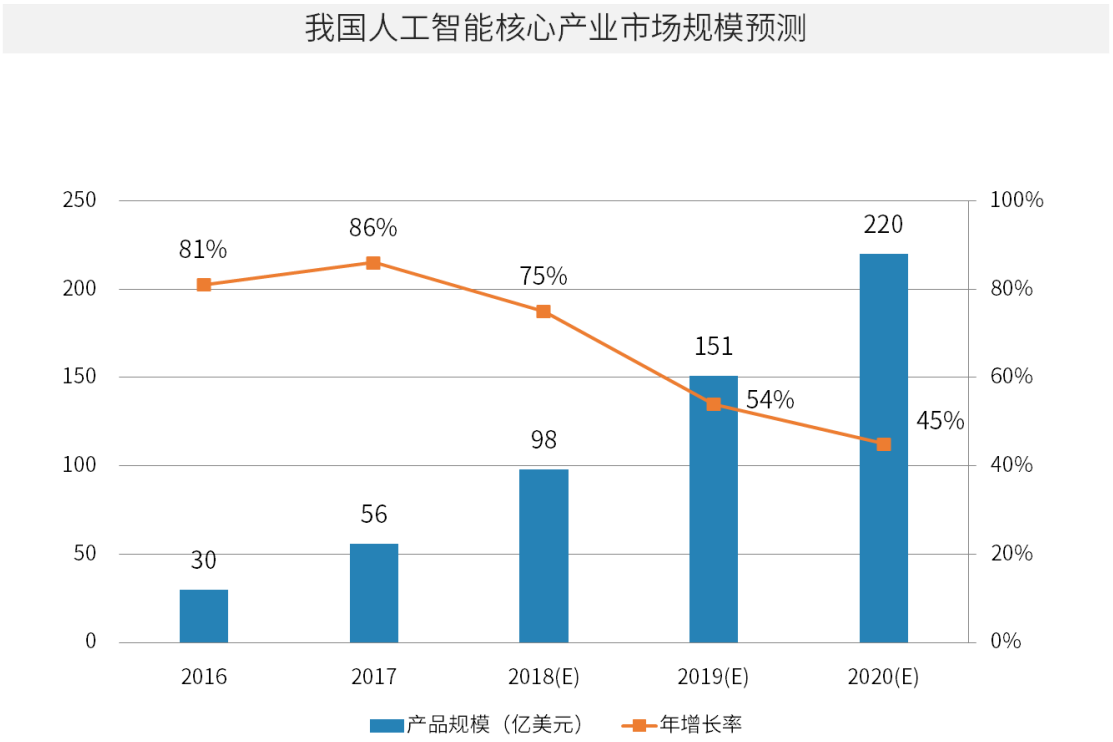
图 10[11]：全球人工智能市场规模预测增速快，全球 AI 相关产品业规模庞大



在这个技术大背景之下，我国人工智能产业初具优势。中国电子学会公开数据显示，2017 年，中国人工智能核心产业规模已达到 56 亿美元左右，预计 2020 年，中国人工智能核心产业规模将超过 220 亿美元，年均增速接近 65%。

11 数据来源：《中国人工智能创新应用皮书》

图 11[12]：中国人工智能市场规模预测，产业初具优势



按照中国信息通信研究院的统计结果，目前中国人工智能市场主要由五个领域构成，按照市场规模从高到低分别为：机器视觉占比 37%，语音识别占比 22%，自然语言处理占比 16%，基础算法及平台占比 14%，芯片占比 11%。其中，由于近几年中国互联网娱乐、广告传播和公共安全视频监控市场的高速发展，计算机视觉市场规模以 37%占比大幅领先。

12 数据来源：《新一代人工智能发展白皮书》

图 12[13]：2017 年人工智能市场结构，计算机视觉占主比大幅领先

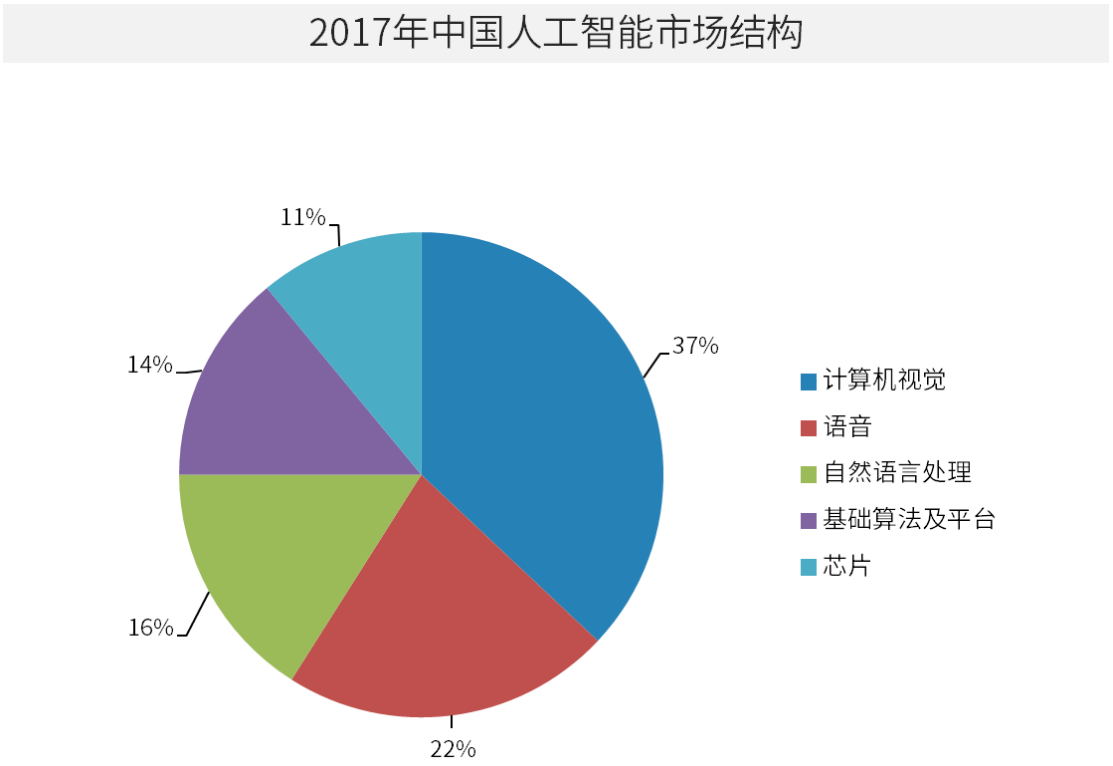
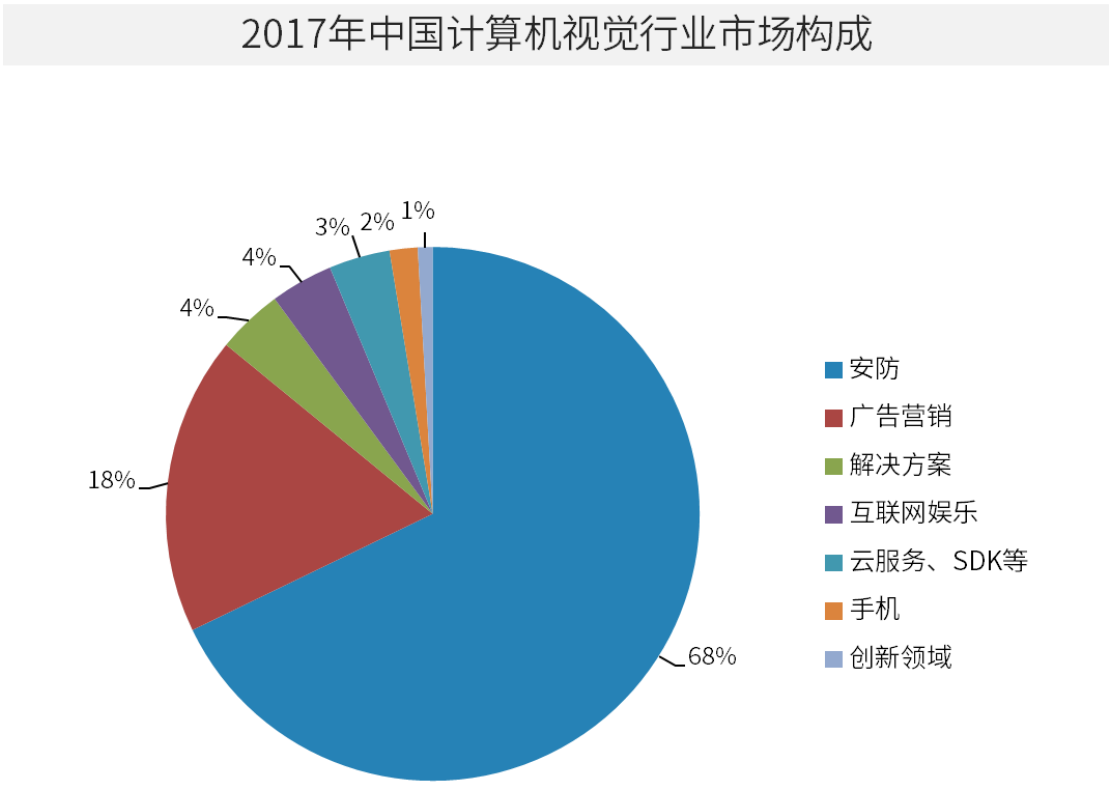


图 13[14]：2017 年中国计算机视觉行业市场构成，安防占据大部分

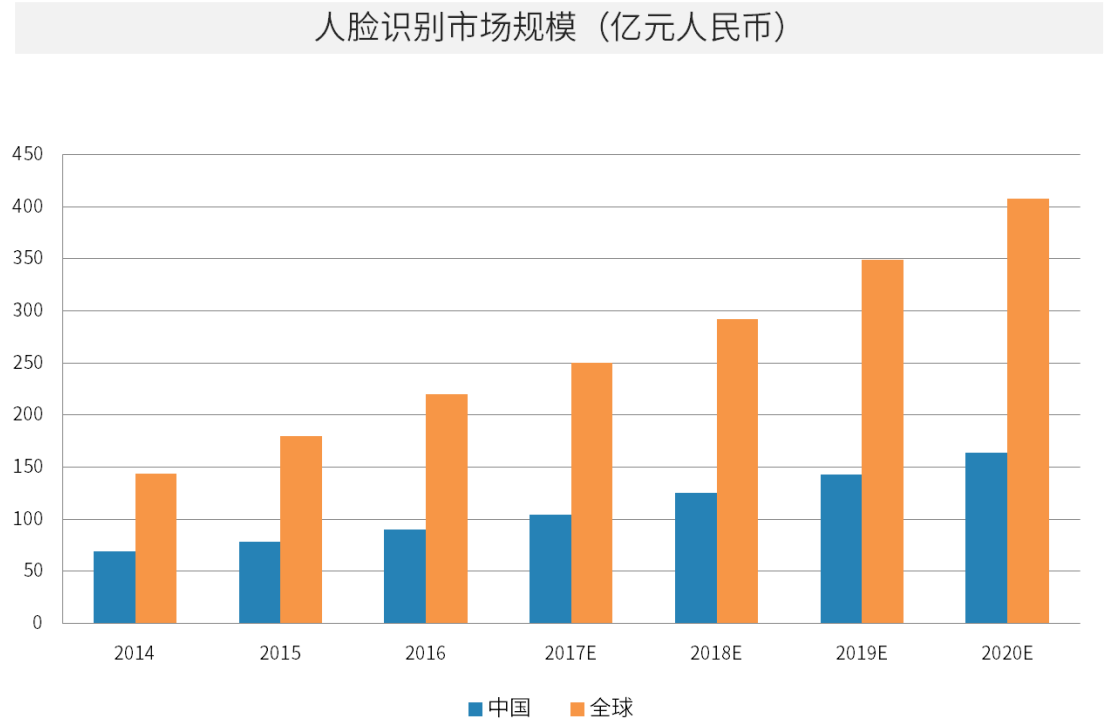


[13] 数据来源：《2018 人工智能应用安防行业研究分析报告》
[14] 数据来源：《2018 人工智能应用安防行业研究分析报告》

在机器视觉领域市场构成中，安防行业以 67.9%占据大部分份额，这得益于中国公共安全视频监控建设的庞大市场。随着高清视频、智能分析、云计算和大数据等相关技术的发展，安防系统正在从传统的被动防御升级成为主动判断和预警的智能防御。安防行业也从单一的安全领域向多元化行业应用方向发展，旨在提升生产效率、提高生活智能化程度，为更多的行业和人群提供可视化、智能化解决方案。随着智慧城市、智能建筑、智慧交通等智能化产业的带动，智慧安防也将保持高速增长。预计在 2020 年全球产业规模实现 106 亿美元，中国会达到 20 亿美元。

在安防行业，人工智能应用发展最快的是人脸识别，其市场规模如下图所示。

图 14[15]：人脸识别市场规模发展最快



15 数据来源：《2017 人工智能报告》

第二章 智慧安防生态

图 15[16]：智慧安防生态圈如下所示



2.1 基础硬件

这里的基础硬件特别强调芯片厂商，目前主要的 AI 核心芯片供应商如下表所示：

[16] 信息来源：宇视根据公开资料整理

表 2[17]：目前主要 AI 芯片厂商，但学术界对“AI 芯片”说法存疑

目前主要AI芯片厂商

名称		主要供应商	简介
CPU		intel	CPU是一台计算机的运算核心和控制核心，它的功能主要是解析计算机指令以及处理计算机软件中的数据。
GPU		NVIDIA	GPU又称视觉处理器，专门用作图像运算的微处理器。相比CPU更适合执行复杂的数学和几何运算，尤其是并行计算。
FPGA		intel XILINX	FPGA及现场可编程门阵列，用户可根据自身需求，用硬件描述语言对FPGA的硬件进行设计。
ASIC	VPU	intel	Intel收购的Movidius开发的Myriad系列VPU专门为计算机视觉进行优化，可以用于安防等计算机视觉用途。
	BPU	地平线 Horizon Robotics	BPU芯片是地平线机器人研发，该芯片未来会直接应用于自身的主要产品，包括，智能驾驶、智能生活、智能安防。
	BM1680	BITMAIN	2017年其最新发布的BM1680专用芯片适用于CNN/RNN等深度学习网络模型的预测和训练计算加速，最新推出的BM1680支持32位单精度浮点运算。
	Hi3559A	HISILICON	2017年海思发布Hi3559A，其整体AI算力基本可涵盖安防典型应用场景，此外还集成ISP、H.265等，为安防终端单芯片方案。

注释：对于“AI 芯片”这一称谓，学术界持严谨和否定的态度。中科院中国经济与社会安全研究中心主任王飞跃称没有这样的说法，“我不认为现在有所谓的人工智能芯片，当然这种宣传可以进行宣传。”德国马格德堡大学教授 Andreas Nuernberger 也同意这样的观点，不知道背后谁在推动，从而成为热词。

GPU 主要应用在数据中心，其特点是产品上市快，缺点是功耗高。安防应用中，GPU 芯片基本被英伟达垄断。

[17]信息来源：中信证券研究部整理

表 3[18]：人工智能应用，安防业内 GPU 芯片被英伟达垄断

人工智能应用		
Tesla	Tesla产品主要用于视频监控，作为PCI卡形式，安装在NVR或者视频服务器，可用于深度学习"训练"或者"推理"之用。 • V100 -高价格高性能，主要用于深度学习研发之用。 • P100 - 中等价格及性能，用于数据训练。 • P40 -中等性能及价位，用于数据训练及推断，使用在性能强劲的服务器上。 • P4 - 价位中低，主要用于"推理"（Inferencing）之用，在NVR服务器或者其他视频分析、深度学习应用中。	
Jetson	Jetson主要应用于前端摄像机，实现AI功能。 • TX1 -Maxwell architecture • TX2 -Pascal architecture	
GTX Quadro	• GTX - Graphics Cards • Quadro- Advanced Graphics Cards	
DGX	The DGX-1 用于复杂情况下大数据训练，深度学习。其性能等价于1台至强处理器配置了8个Tesla的V100模块。	

安防领头企业不乏基于 GPU 的视频监控产品，如下图所示：

表 4[19]：安防+AI 典型落地应用产品

安防+AI典型产品		
厂商	产品	图片
海康威视 HIKVISION	海康"深眸"摄像机，基于NVIDIA Jetson TX1的最新双目智能摄像机产品。该产品由双目摄像机（基于人眼工作原理）与高性能GPU模块组成，实现人员的多种智能分析功能。基于深度学习技术，支持人员行为，客流统计，人体属性，人脸识别等多种智能检测，适用于公共场所，银行，商场，景区等环境。	
uniview 宇视	宇视大容量分布式的云结构化智能分析服务器（代号"昆仑"），在4U的高度上支持了80颗NVIDIA Jetson TX1处理器，可以并发处理640张/秒的人脸识别、160路的人员计数、80路人车物的结构化分析，芯片和算法基于深度学习，准确性很高。	
alhua TECHNOLOGY	"Deep Sense睿智"系列视频结构化服务器，采用NVIDIA® Tesla® P4 GPUs作为核心处理负载，功耗低，性能强。服务器采用深度学习算法，最多可支持192路全清视频实时结构化分析，相较于市场上同类别的产品，视频处理能力将提高50倍以上。	

FPGA 在中心推理及数据中心也有较多应用，与 GPU 比，FPGA 的功耗优势明

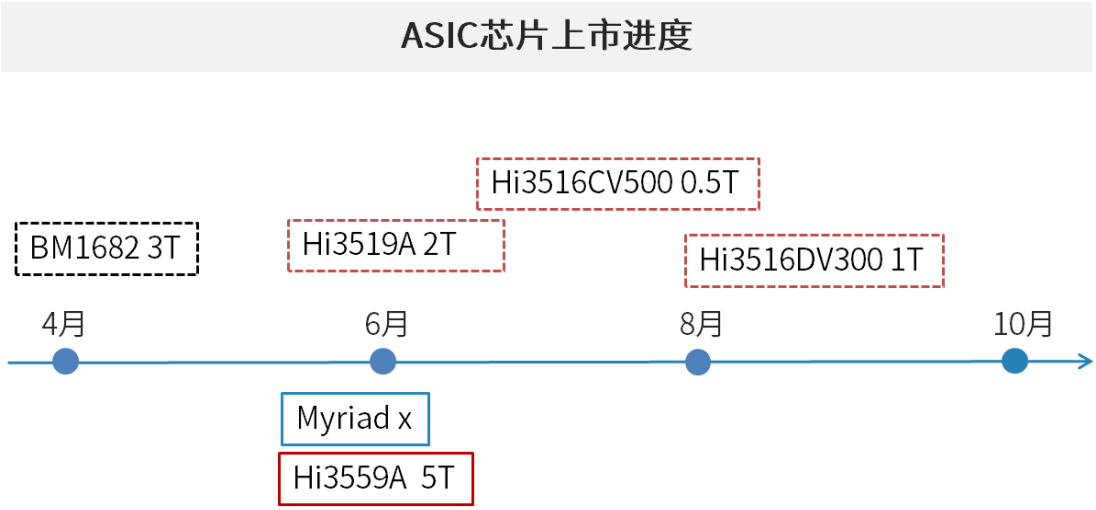
[18] 数据来源：《2018 人工智能应用安防行业研究分析报告》
[19] 数据来源：《2018 人工智能应用安防行业研究分析报告》

显。安防应用中，FPGA 主要厂家有 Xilinx、Intel（原 Altera）等。

ASIC 主要应用于端侧推理，由于端侧应用的多样性、复杂性以及对高性价比述求等原因，ASIC 厂家很多，例如：寒武纪、海思、地平线、比特大陆等，同时提供的方案也多。

2018 年安防市场 ASIC 竞争非常激烈，下图是根据网络数据整理的各 ASIC 芯片上市进度。其中，海思的布局非常密集。

图 16[20]：ASIC 芯片上市快，布局密集



2.2 云平台

近年来，具备云计算平台等技术资源的公司，如阿里云、华为云等云平台厂商，推出了针对智慧安防行业的智能视频云平台。除了传统的海康、大华、宇视、科大、天地伟业、东方网力等企业外，CV 厂商和云平台供应商也逐步开始提供云平台产品和行业应用。

2.3 软件框架

软件框架技术仍掌握在亚马逊、微软、谷歌、百度等科技巨头手中，是深度学习人工智能的核心。

算法框架是人工智能核心生态圈建立的关键环节。实现算法的模块化封装，

[20] 数据来源：宇视根据企业发布信息整理

为应用开发提供集成软件工具包，包括针对算法实现开发的各类应用及算法工具包，为上层应用开发提供了算法调用接口等服务。

2.4 基础算法

安防行业的算法企业总体来说可以分为两大类。第一大类是商汤、旷视、云从、依图、中科神探等 CV 企业；第二大类是海康、大华、宇视，也开始 AI 算法技术布局。随着各企业的投入进一步加大，视频识别算法准确率大幅度提升。例如人脸识别算法，在特定条件下，已经达到很高的水平。

此外，在图像分类、物体检测等方面，计算机的识别率都已经远远超越了人类平均水平。

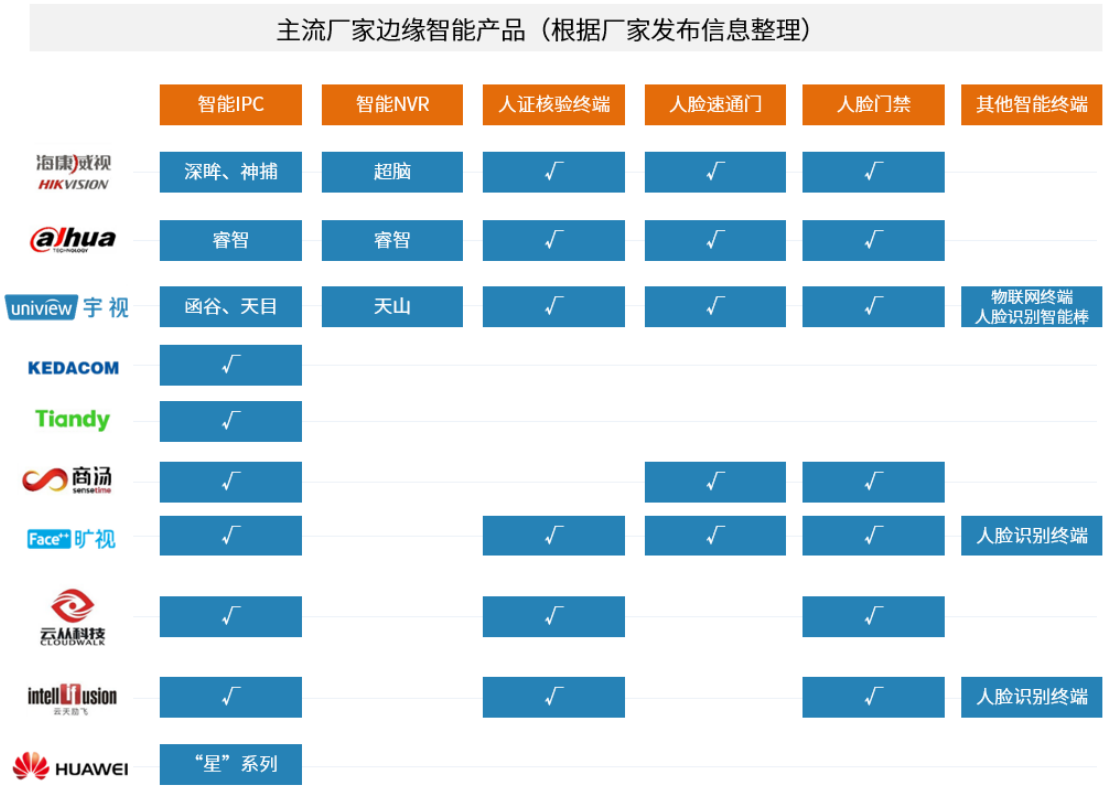
2.5 产品及行业应用

除了传统的海康、大华、宇视、科达、天地伟业、东方网力等安防厂商外，CV 厂商和云平台供应商也逐步开始提供产品和行业应用。

除了前文提到的云中心产品，各企业基本已经完成边缘智能产品序列化。

随着边缘和中心产品的丰富，用户开始对应用业务提出了更高的要求。从目前行业情况来看，无论是传统安防企业，还是 CV 和云平台企业，在业务应用上虽有部分提升，但仍以典型通用应用为主。

图17[21]：主流厂家边缘/中心智能产品丰富，用户更重视实际应用



第三章 智慧安防典型应用

随着 AI 在安防行业的渗透和深层次应用技术的研究开发，当前安防行业已经呈现“无 AI，不安防”的新趋势，各安防监控厂商全线产品 AI 化已经是当前不争的事实，同时也成为各厂商的新战略。随着 AI 在安防行业的深入落地，AI 在安防领域尤其是视频监控领域的产品形态及应用模式也开始趋于稳定，安防行业的 AI 技术主要集中在人脸识别、车辆识别、行人识别、行为识别、结构化分析、大规模视频检索等方向。

安防行业的 AI 应用场景分为卡口场景和非卡口场景，前者指光线、角度等条件可控的应用场景，以车辆卡口及人脸卡口为主；后者指普通治安监控视频场景。其中，卡口场景约占监控摄像机总量的 1%-3%，剩余的均为非卡口场景监控视频。

21 数据来源：宇视根据企业发布信息整理

3.1 卡口场景：人脸身份确认应用

人脸身份确认应用以公安行业人员布控为代表，在关键点位部署人脸抓拍摄像机，通过后端人脸识别服务器对抓拍到的人脸进行分析识别，同时与人脸黑名单库进行比对。

随着人员布控应用的增强，已经初显效果。例如近期的“张学友演唱会”：

2018 年 4 月 7 日，南昌站首个逃犯在现场落网；

2018 年 5 月 5 日，赣州站演唱会开场安检过程中，成功抓获一名网上逃犯；

2018 年 5 月 20 日，嘉兴站演唱会开场安检过程中，成功抓获一名逃犯；

2018 年 6 月 9 日，金华站演唱会，2 名逃犯落网；

2018 年 7 月 6 日，呼和浩特站演唱会，一名全国在逃人员落网；

2018 年 7 月 8 日，洛阳站演唱会，洛阳警方成功拿下“七杀”；

2018 年 9 月 21 日，遂宁站演唱会，共计抓捕 10 余名逃犯；

2018 年 9 月 28 日，石家庄站演唱会，现场三名逃犯落网；

2018 年 9 月 30 日，咸阳站演唱会，咸阳警方成功抓获 5 名逃犯。

人脸动态布控应用中主要利用人脸抓拍摄像机从高清视频画面中抓拍人脸照片，即时分析人脸特征，快速完成抓拍人脸与黑名单库人脸的比对并实现报警提示。报警后可结合人脸静态大库，将抓拍到的人脸在静态大库中进行人员身份信息查询，最终输出 TopN，经过人工研判后即可判定是否为在逃的违法犯罪分子，通过指挥调度实现对犯罪分子的“围追堵截”直至抓捕归案，类似的应用还有很多。

2017 年，沈阳地铁部署人脸识别系统，系统运行仅仅 27 个小时，就成功识别出 2 名被列为网上逃犯的犯罪嫌疑人；系统报警后还会对目标拍摄前后共计 10 秒钟的视频，以便留存证据。现场技术人员介绍，准确率超过 90%，偶尔会存在误报，试运行的 10 天内共计发生误报不超过 3 次。

2017 年在第 27 届青岛国际啤酒节期间，青岛开发区警方将“人脸识别”系统应用于啤酒节安保，并成功抓获网上逃犯 25 名，吸毒人员 19 名，当场还抓获了 5 名扒手，并且驱离扒窃前科人员 32 名。

另外，通过人脸识别系统的过人抓拍库，还可以查询人员行走轨迹，可以借助人脸识别系统寻找走失老人、儿童等，实现便民服务。

3.2 卡口场景：人脸身份验证应用

人脸身份验证应用逐渐普遍。常见的人脸白名单应用已经在很多行业落地，

比如人脸门禁、人脸速通门、人脸考勤、人员身份确认等，广泛应用于企业、各类园区等场景。除实现基础的人脸识别应用外，人脸门禁还可以防止通过照片、视频等人脸假冒行为，切实保障出入口人员安全管控及日常人员管理等。

3.3 卡口场景：车辆识别应用

车辆识别技术是公安实战中应用最成熟、效果最明显的技术之一。借助遍布全国各地交通要道的车辆卡口，车牌识别使得“以车找人”成为现实，成功协助警方破获各类案件。车辆识别技术已经从初级的基于车牌的车辆识别应用阶段，发展到车型识别、套牌车识别等精准的车辆识别应用阶段。

3.4 非卡口场景：视频结构化分析与快速检索应用

在视频结构化分析与快速检索应用中，视频结构化业务功能是对视频中的机动车、非机动车、行人等活动目标进行分类检测；同时提取目标小图和场景大图写入存储设备中，便于后续的快速查询及智能检索。通过视频结构化业务快速分析并提取出视频中感兴趣目标的特征属性信息，用户能够高效获取案事件相关线索，促进大安防时代视频数据从看清跨入到看懂的阶段。

3.5 非卡口场景：行为分析辅助安防应用

行为分析可辅助安防应用。通过行为分析系统对人员的异常行为进行分析处理，可应用于重点区域防范、重要物品监视、可疑危险物品遗留等行为的机器识别；也可对人员的异常行为进行报警，极大提升了视频监控的应用效率。

另外，还可以实现对群体的态势分析，如人群密度分析、人员聚集分析等，对重点区域或人员聚集较多的场所态势进行分析，防止人群事件发生，做到提前预警、及时处置。

第四章 智慧安防规模应用的八大限制性因素

虽然人工智能技术飞速发展，但在产品化和实践应用中，依然存在很多问题。

在过去几年，人工智能热度很高，但实际上只完成了“概念模型”的建立，尚未达到“有效利用”的理想效果。

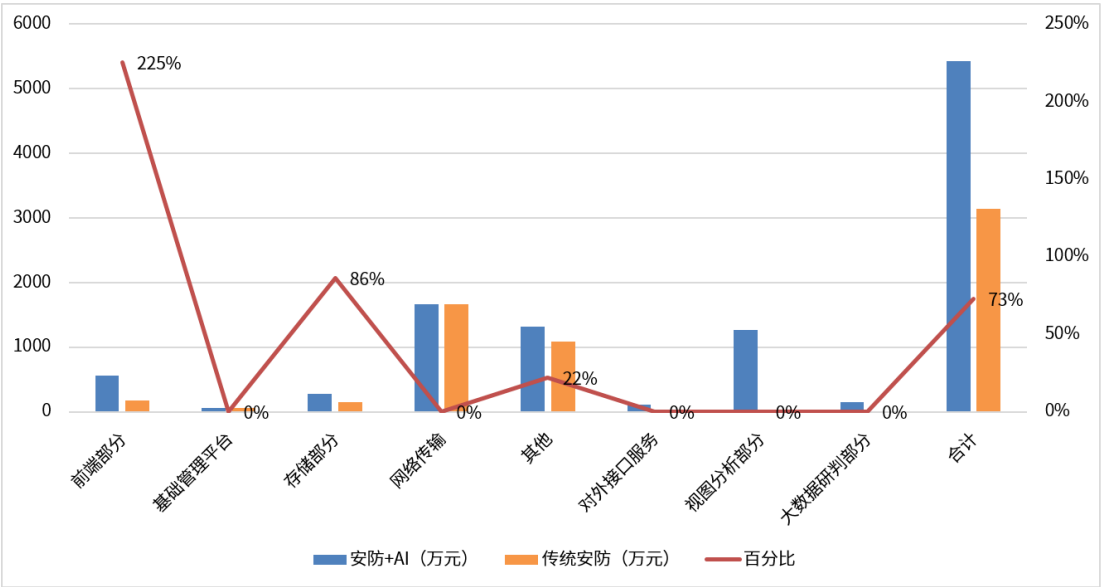
4.1 成本高昂

当前，影响“安防+AI”产品解决方案规模化应用的因素有很多，成本高昂是众多原因之一。从一个典型中大型城市级公共安全视频监控联网项目各部分成本占比情况可以清晰看出成本是“安防+AI”发展的重要瓶颈。

设备本身由于产品性能、算力性能等多方面要求造成布置成本较高；而科学化工勘布点需求带来的时间和人力成本、海量图片高并发网络带宽需求带来的设备和链路成本、多业务系统联网应用带来的沟通和研发成本、大数据研判分析应用带来的设备及研发成本以及不断增长的设备与集成施工和机房改造等因素则进一步叠高了“安防+AI”落地的成本。

通过统计典型案例的数据，以建设 1000 路规模的高清安防监控系统和 1000 路高清 AI 人脸识别系统为例，来对比分析“安防+AI”及“传统安防”的建设成本（注：各部分设备费用包含安装施工等人力成本）。

图 18[22]：安防+AI 与传统安防两周方案建设成本比对，安防+AI 优势显著



通过对比分析表，可以发现“传统安防”方案的建设比“安防+AI”方案的

22 数据来源：宇视根据公开招标信息整理

建设少了对外接口服务、视图分析部分及大数据研判部分，这一部分成本是建设“安防+AI”解决方案所必不可少的。通过对比其他项得知：

前端部分：“安防+AI”比“传统安防”要高出 225%，主要原因除了前端设备多出的算力之外，还来源于设备的工勘选点、设备安装调试的人力成本，这是传统安防监控点位所不需要的。

基础管理平台及网络传输部分：这两部分成本两种方案基本持平，对于整个基础平台部分来说，两种解决方案所需设备基本一致，而传输网络因为到每个点位均采用千兆网络带宽，故也是相同的成本。

存储部分：这一部分成本可以看出“安防+AI”方案要比“传统安防”方案高出 86%，主要原因是“传统安防”方案对存储设备的读写性能和可靠性没有“安防+AI”方案要求高。随之而来便是产品方案的选择不同，“传统安防”方案可采用传统 NVR 或者 IPSAN 磁盘阵列方案，而“安防+AI”方案则需要采用云存储方案，另外一方面原因是“安防+AI”方案多出了海量图片全周期的存储空间要求。

其他部分：“安防+AI”方案要比“传统安防”方案高出 22%，由于前面几大系统的整体高出，使得“安防+AI”方案系统集成、施工辅材、机房改造等设备及人力成本随之升高。

通过以上分析不难看出，在同等条件下，当前“安防+AI”解决方案的总体成本要比“传统安防”整体成本要高出 73 个百分点。高昂的成本在很大程度上限制了“安防+AI”解决方案的规模化落地。

4.2 算法场景限制高

人工智能算法的泛化能力是模式识别问题长期面临的一个问题，也是现阶段的主要瓶颈。

由于训练好的模型用在变化的场景中性能往往会明显下降，因此在实际使用中，必须对场景进行严格定义，或者从设计上将智能算法定位为对指标不敏感的辅助功能。在比较成熟的应用中，如智能交通中的过车及违章抓拍、机场车站的人证对比等，都需要具体的工程安装方案。这种做法在技术不够成熟的条件下有效实现了商业价值，但缺点同样明显：一方面，对已有设备的改造需要增加施工成本，影响人工智能算法对传统应用的渗透；另一方面，也限制了获取有效素材的效率，影响算法指标的进一步提升。

4.3 布点困难

人工智能往往有特定的场景要求，只有在特定场景下才能保持较好的识别率。

以人脸识别为例，公安部发布的《GB/T 35678-2017 公共安全 人脸识别应用图像技术要求》标准按照当前主流人脸识别水平规定了公共安全人脸识别应用中人脸图像的技术要求，详细如下：

1. 图像格式：人脸图片格式应为 BMP、JPEG、JPEG 2000 和 PNG 中的任一种。若图像为灰度图时，图像灰度级应为 256 级；

2. 遮挡：遮挡物应不遮挡眉毛、眼睛、嘴巴、鼻子及脸部轮廓等；

3. 两眼间距：两眼间距应大于等于 30 像素，宜大于等于 60 像素；

4. 姿态：人脸水平转动角应在±30°以内，俯仰角应在±20°以内，倾斜角应在±30°以内；

5. 脸部区域：人脸完整，轮廓和五官清晰，无浓妆，图像脸部区域应无编辑修改性处理，几何失真应小于等于 10%，运动模糊应小于等于 0.20，高斯模糊应小于等于 0.25。

进行人脸识别的摄像机，需要严格遵从公安部发出的政策标准，导致大幅度降低人脸识别的可应用空间，也大幅度提升了施工难度。

图 19：人脸识别摄像机使用场景模拟示意图

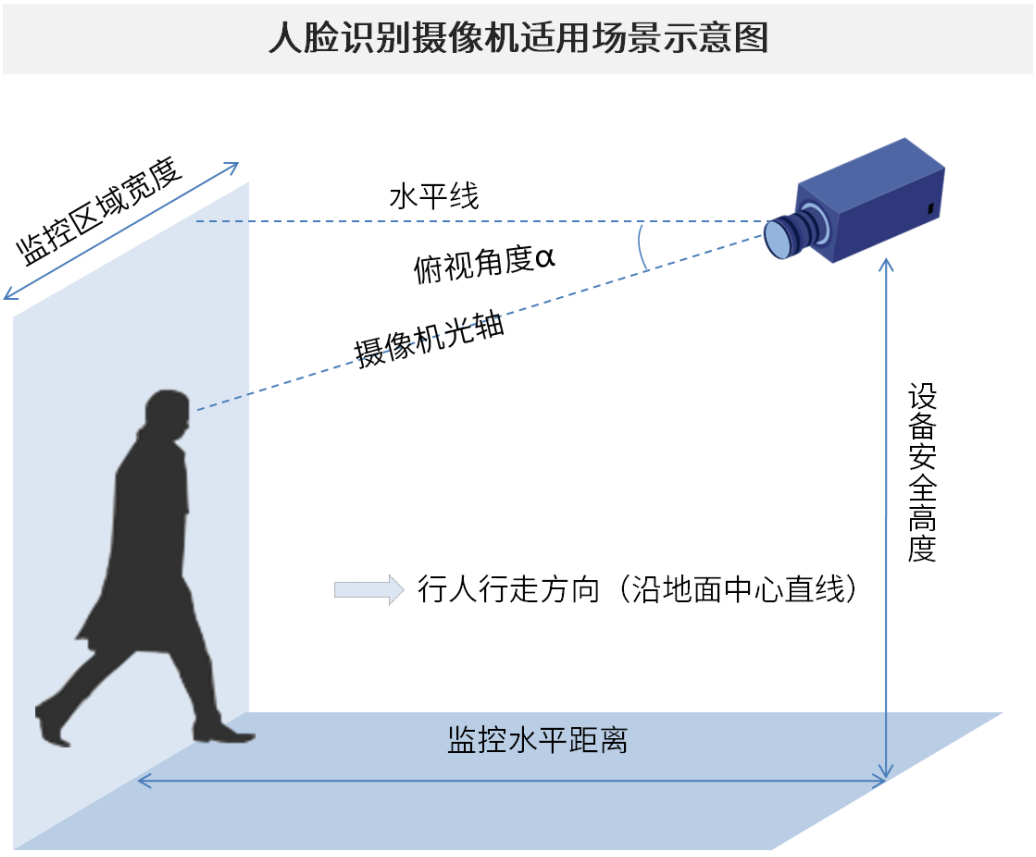


表 5：人脸识别摄像机使用场景数据范围

环境类型	推荐值	备注
安装高度	2.2-3 米	
水平监控距离	3-10 米	
俯仰角	15°以内	
左右偏转角	30°以内	
监控区域宽度	4.5 米以内	

4.4 网络和安全要求更高

近年来，人工智能技术的蓬勃发展赋予了安防监控系统更加多样化的业务功能，将安防监控行业的市场空间进一步拓宽，使安防监控系统在各行各业得到广泛部署。但从风险角度而言，在 AI 与安防融合发展的进程中，将大量非结构化视频转化为可快速检索的结构化数据，一旦网络被攻击，数据泄漏后的损失将更为恶化；另一方面人工智能将大量视频、图片集中到云中心，对网络带宽提出了更高要求。此类需求和风险可归类为以下 3 个方面：

问题 1：现阶段大量部署的端计算设备安全风险高：暴露设备数量太多、暴露端口太多、设备漏洞太多、固件更新不及时、通信协议安全性不高、数量过多无法管控。

图 20[23]：暴露的视频监控设备厂商分布情况

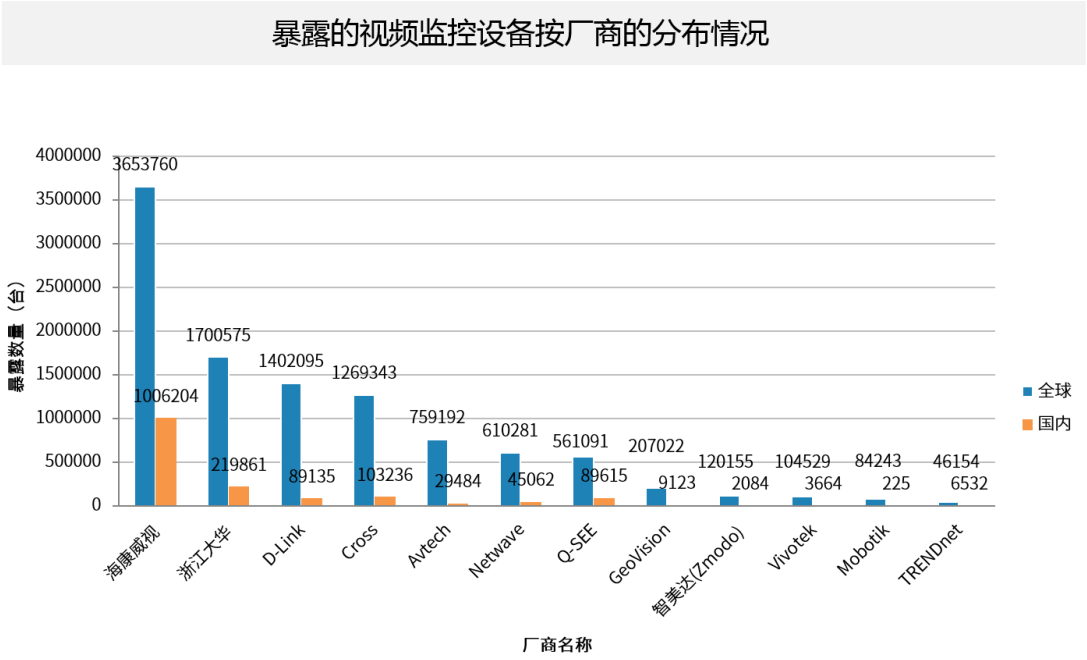
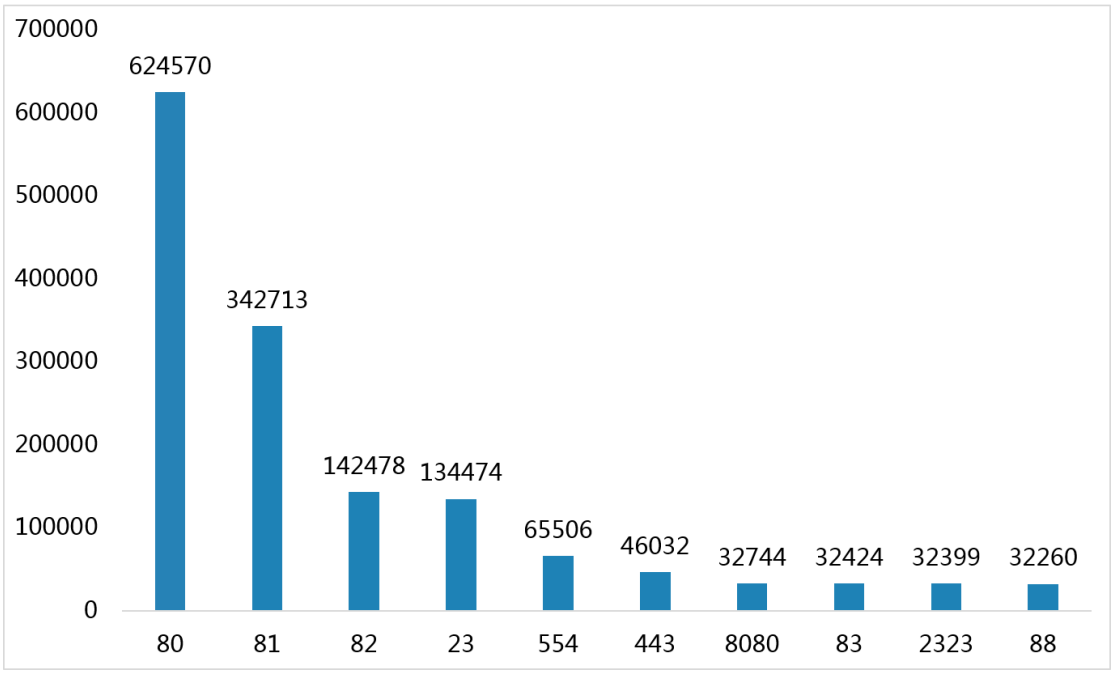


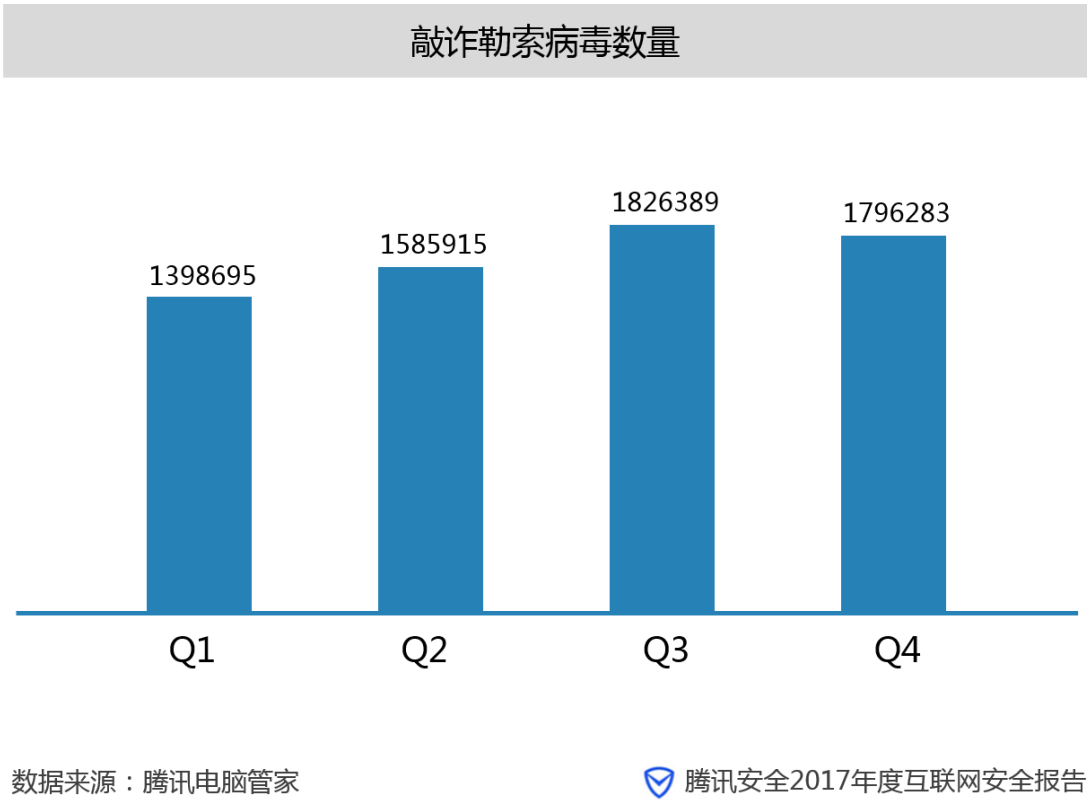
图 21[24]：暴露的视频监控设备端口分布情况



23 数据来源：绿盟科技《2017 物联网安全研究报告》
24 数据来源：绿盟科技《2017 物联网安全研究报告》

问题 2：监控等物联网设备已经成为新的攻击目标（僵尸网络与 DDOS、远程录拍、勒索病毒、挖矿木马、APT 攻击）。据腾讯安全报告：视频监控/物联网设备已经成为新的 DDoS 攻击目标，2017 上半年物联网攻击增加约 280%，2017 年新增勒索病毒样本 660 万个。

图 22[25]：2017 年全年敲诈勒索病毒数量情况



问题 3：人工智能的发展，数据被终端采集后传输汇集到集中式云计算中心，网络实时性和带宽都带来量级的要求，对云中心部署方案的带来了挑战，需要新的模式来适应 AIoT。

4.5 深度应用不足

视频监控系统产生的数据量庞大，而且日趋多元化，包含：非结构化数据、半结构化特征数据以及结构化数据。当前的人工智能视频大数据分析技术主要存在如下三个问题：

[25] 数据来源：《2017 年度互联网安全报告》

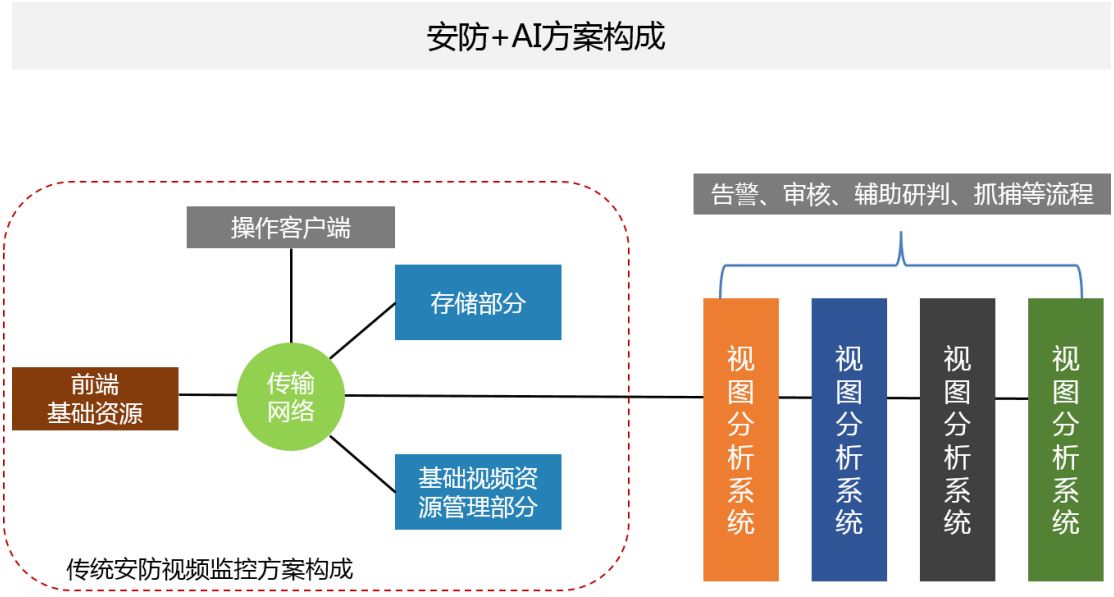
问题一：非卡口场景的视频分析算法在准确率、稳定性及计算成本等核心指标方面还有待于提高，导致非卡口场景的存量视频利用率极低，目前没有有效利用的非卡口监控视频约占监控视频总量的 97%左右；

问题二：当前的人脸识别技术、行人识别技术、行为分析等视频分析技术往往是接近于实验室场景下的初级应用、数据孤立下的单点识别应用，距离全天候场景下的精准锁定，最快时间、最小成本、跨摄像机下的识别搜索，还有很大的差距，真正解决客户实战问题的能力还有待于提高；

问题三：智能 AI 摄像机及视频结构化分析产品开始进入安防市场，产生了海量的结构化视频数据，但基于结构化视频数据的深度智能应用，如时空分析、模式挖掘、预测预警、技战法训练等尚在探索阶段，有可能形成新的数据浪费和低效投资。

4.6 系统性顶层设计

图 23：典型的安防+AI 解决方案构成示意图如下：



传统安防视频监控方案要落地能够满足客户的建联管用基本使用需求，大致由四部分组成，即上图红色虚线框所示：前端基础资源、传输网络、管理部分和存储部分。建成之后的安防视频监控系统用户只需要在操作客户端上即可完成视频解码上墙、实况录像调阅和资源管理等基本业务。

安防+AI 解决方案在传统安防的基础之上不仅对布点、网络、存储等提出新

的挑战，还在组成上多出了视图分析系统、大数据研判系统、视图资源归档、对外接口服务，以及最重要也是必不可少的告警、审核、辅助研判及抓捕一系列流程配合。安防+AI 方案融入了更多的系统集成的同时，不论是前期的科学选点，还是后期的研判抓捕，以及组织、流程保障等人的因素贯穿始终。

因此，安防+AI 解决方案需要进行前瞻性、系统性、科学的顶层设计，这是能否真正落地、取得丰富实战效果的前提。

4.7 缺乏行业标准与评估体系

当前情况下，安防+AI 算法、产品及解决方案以企业标准为主，应逐步建立面向实战应用的行业标准。鉴于人工智能技术飞速发展的现状，现阶段全面建立统一的行业标准有可能会伤害安防行业的健康发展，但安防+AI 算法、产品及解决方案的评估体系应尽快构建。

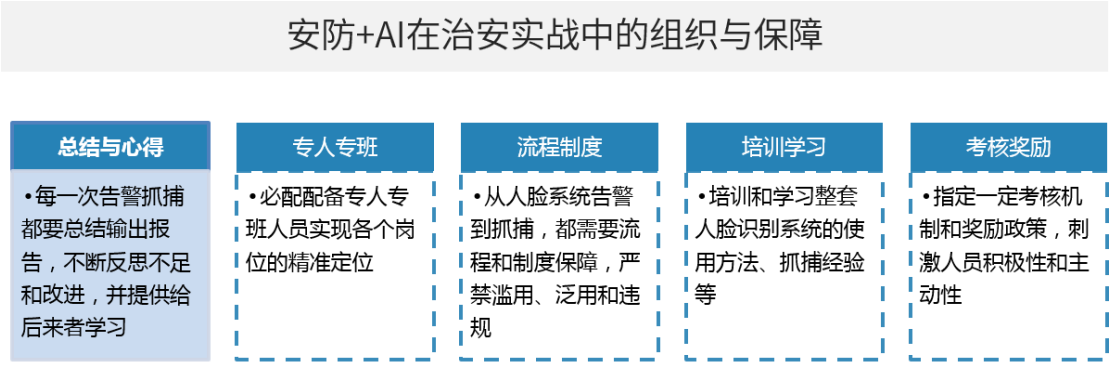
4.8 用户学习与组织保障成本更高

AI 产品方案在安防行业的落地，对用户来说：如何使用好这样一套系统，让系统发挥出它最大的功效是一个全新的挑战，这个挑战不仅源于对颠覆原有以往任何技术手段的不断学习和经验总结，更来自于用户自身的组织和制度如何保障系统的有效运转。

以人脸识别系统为例，对于公安用户来说，如何利用这套系统完成人员身份信息的核实，对相关嫌疑人产生准确的告警，并通过告警完成相应人员的抓捕归案是一整套流程的打通。对于部分公安用户，存在建设部门与使用部门相分离，各业务警种之间相分离，各部门上下层级间相分离，公安内部与外部资源相分离以及各单位资源间相分离等情况，形成了一定的壁垒。

如何使用好一套人脸识别系统，还来自于用户本身的不断学习和经验总结，一方面对于系统本身通过厂商的培训学习和对外的参观考察学习，另一方面对于系统使用本身，需要结合本地实际情况，不断总结符合本地实情的技战法并快速有效的复制传递。比如如何完成本地黑名单库的建立和更新，如何实现嫌疑人人脸目标的获取，如何通过多种技术手段实现告警嫌疑人的轨迹追踪，如何保时刻持抓捕人员的高机动性，在发生黑名单告警并确认后快速实施抓捕任务以及如何保障一线抓捕人员与指挥中心人员的信息及时交互等都是系统在使用过程中需要不断学习和总结的。

图 24：安防+AI 在治安实战中的组织与保障



如何能够提高相关人员的积极性和主动性，除了相应的考核机制之外，还可以建立一定的奖惩措施。

第五章 八大新趋势造就智慧安防新未来

5.1 工程的科学布点

人工智能的强场景化特点，决定了在智慧安防应用中，摄像机的使用位置、覆盖范围受到很大限制。相同数量的摄像机，在一个城市中的开放区域，安装于不同的位置，所能起到的作用显然是不同的。一个智慧安防系统如何在有限的摄像机资源覆盖情况下，达到最优的防范效果？这就对系统方案设计、布点设计提出了更高的要求。

一方面，用户和设计机构，根据各地的区域情况和历史经验，建立了一些基于经验的方法论，例如：关键点覆、关键区域覆盖、网格化覆盖、外环内网等。

另一方面，人工智能的技术将会被应用到系统设计阶段。AR/VR、信息融合、数据挖掘、知识图谱等技术，将为用户提供更精细更准确地系统科学布点的决策分析服务。

5.2 产品的云端结合

目前安防系统中，常见的中心计算架构问题已经日趋严重，主要体现为网络传输带宽问题、及时性问题得不到有效解决。

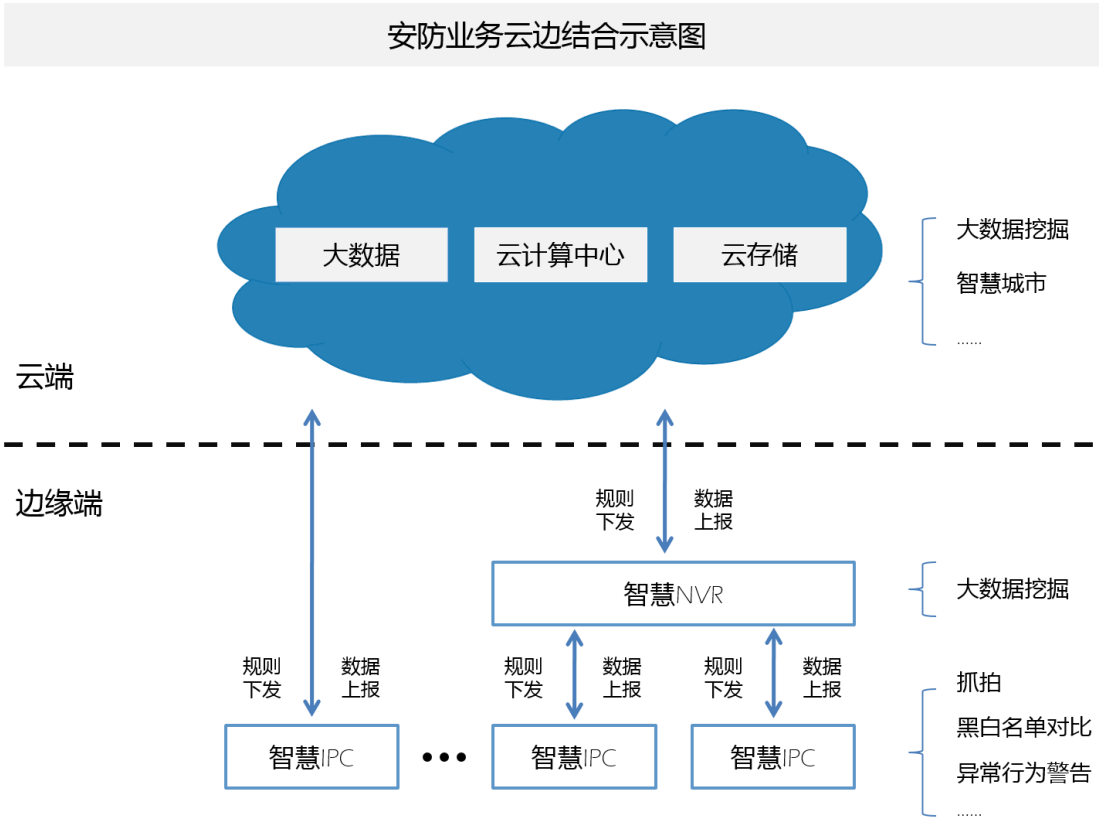
边缘计算的出现有效缓解了上述问题。云计算聚焦非实时、长周期数据以及

业务决策场景，而边缘计算在实时性、短周期数据以及本地决策等场景方面有不可替代的作用。这使得云端云端结合成为新趋势：一些需要集中式处理的计算继续交由大型云计算中心，如大数据挖掘、大规模学习；大量实时的需要交互的计算、分析在边缘节点完成。同时边缘计算也是云端所需高价值数据的采集终端，可以更好的支撑云端应用的大数据分析；而云端通过大数据分析得出的一些业务规则也可以下发到边缘端，优化边缘端的业务决策。云计算与边缘计算分工协作，来满足智能时代爆发式的计算需求。

云边结合的架构，解决了集中式云计算架构的几大问题：

1. 给到云端的数据都是边缘智能产品过滤之后的图片、结构化信息，相较于原始视频，带宽压力大大降低；
2. 汇聚到云端的数据量少，云端的计算和存储性能需求可大幅降低。IDC 数据统计显示，云计算和边缘计算结合，成本只有单独使用云计算的 39%；
3. 由于边缘计算距离用户更近，在边缘智能产品处实现了对数据的过滤和分析，海量的设备数据不需要上传云端，再反馈于终端执行，边缘智能产品可以实时分析并给出结果，本地业务快速响应。

图 25：安防业务云边结合示意图



5.3 AI 分布式计算

在智能应用场景中，存在空间和时间的不均衡性。空间不均衡性是指在不同场景不同地点，分析目标的密集度是不同的；时间不均衡性是指在同一个区域，不同时间的分析目标的密集度是不同的。例如在早晚高峰期间，地铁人流量要远高于平时，而同样在早晚高峰，各站的上下行客流量又要相差很大。

图26[26]：北京地铁客流量时间分布图

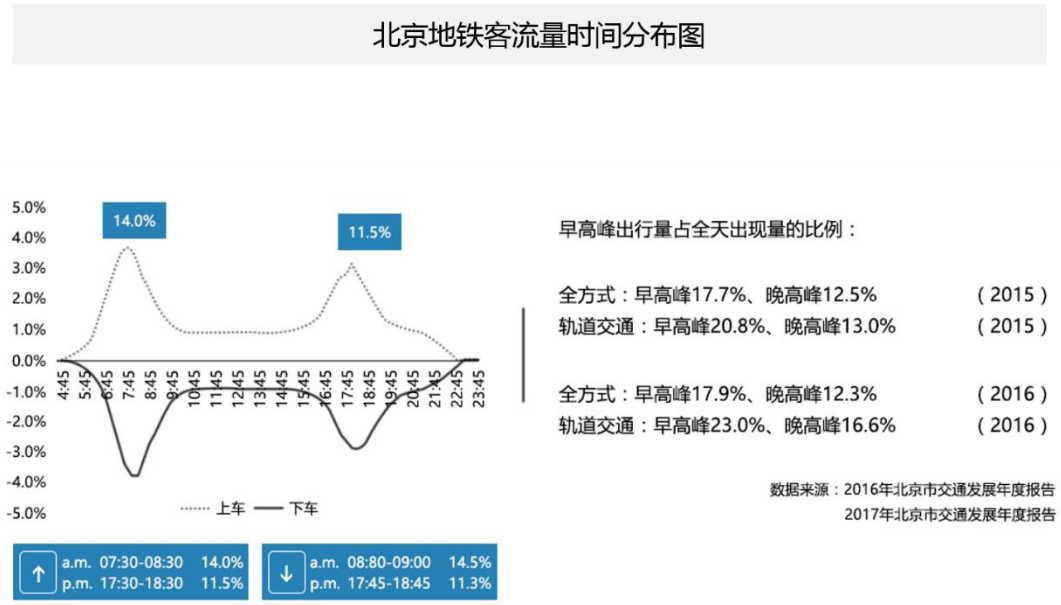


图 27[27]：北京地铁断面客流量分布图



这就导致在智能应用的项目设计阶段很难在数据完整性和成本之间平衡。如果按照高峰期流量模型设计计算性能需求量，则会导致数倍的性能浪费。而如果

26 数据来源：《北京轨道交通线网客流特征分析》
27 数据来源：《北京轨道交通线网客流特征分析》

按照均值流量模型设计计算性能需求量，则会导致在峰值时间段，出现大量的因性能不足导致的数据丢失甚至是系统出现异常宕机。因此，采用分布式计算架构将成为未来趋势。

通过对全网的中心计算设备和边缘计算设备进行统一的计算调度，可以有效地缓解问题，大幅度降低智能应用系统的整体建设成本。另一方面，算法的按需调度将成为可能。不同的算法成为一个可按需分配的资源池，不同的计算资源将根据不同的时间针对不同的分析对象分配算法能力，进一步提升资源利用率。

5.4 数据的多维应用

现今的智能监控系统已经开始融合人工智能分析技术和物联网技术，采集和提取更多有效的多维数据。人工智能技术能够对视频内容进行智能分析，将所有运动目标进行自动分离、自动分类，并自动提取目标多维度的结构化数据以及半结构化数据，如人脸特征、人体特征、车辆特征、异常行为、时空特征等及相应的、更为细化的属性特征。通过物联网技术可以采集相关的物联网信息，如利用RFID 技术、5.8G 射频技术等。

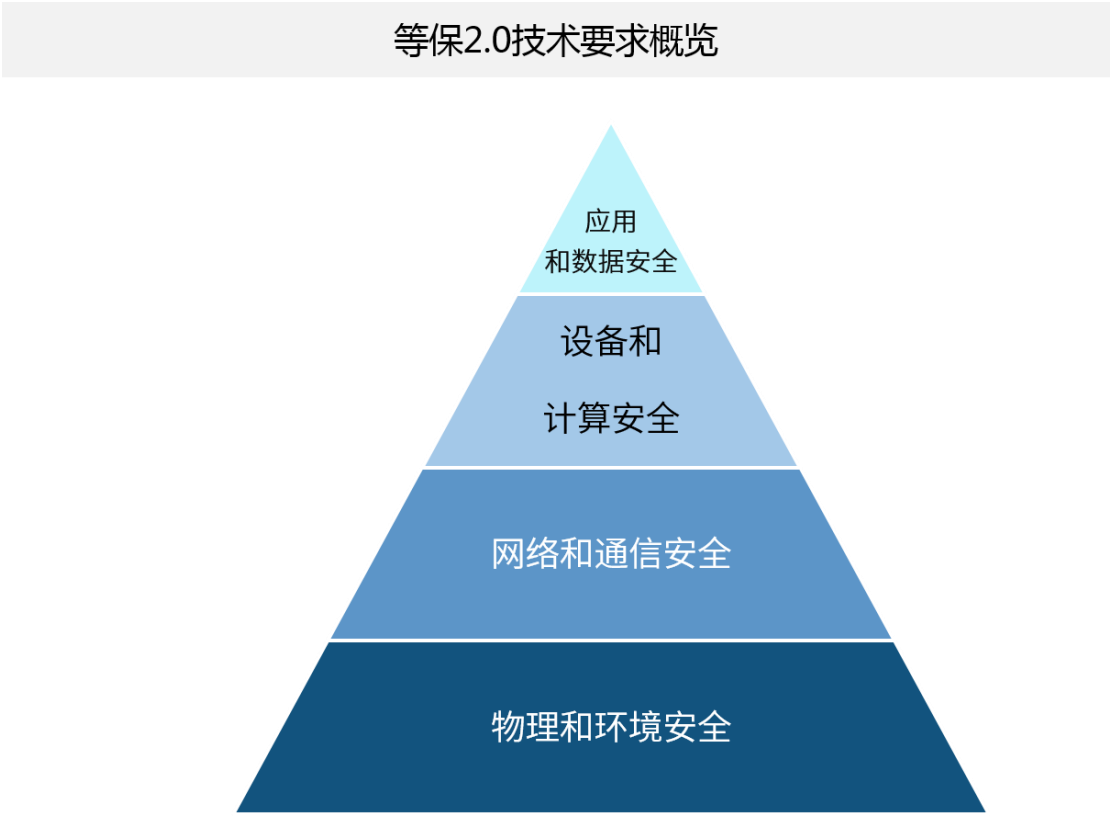
通过对历史数据的分析挖掘，可以挖掘事件的内在联系，识别出异常模式，从而提供实时报警服务；利用知识图谱技术，可以挖掘人和人、人和事、事件和事件之间的关联关系，并进行深度推理，进而为重大事件提供决策分析，提高预警的准确性和及时性。

5.5 数据和网络安全

国家对网络安全的重视，促进安防系统加大对安全解决方案的完善。《中华人民共和国网络安全法》和《网络安全等级保护条例》的发布，如何就安防系统进行安全的巩固和提升给出了系统的指导意见。

《网络安全等级保护条例》（征求意见稿）于 2018 年 6 月 27 日对外发布。被业界普遍称为“网络安全等级保护 2.0”。

图 28：网络安全等级保护 2.0



等保 2.0 的要求，将网络安全等级保护扩展到云计算、大数据、物联网、移动互联网以及公共新领域，并增加了风险、评估、安全监测、通报预警、考核评价、应急处置，还涉及对供应链的要求，可信可控态势感知等方面。

为了解决安防系统中的安全问题，适应新的等级保护条例要求，主要在以下机房采用新技术、新方案来解决安防系统中的安全问题。

表 6：等保 2.0 网络安全相关技术要求

等保2.0网络安全相关技术要求		
网络和通信安全	设备和计算安全	应用和数据安全
网络架构 通信传输 边界防护 访问控制 入侵防范 恶意代码防范 安全审计 集中管理	身份鉴别 访问控制 安全审计 入侵防范 恶意代码防范 资源控制	身份鉴别 访问控制 安全审计 软件 容错 资源控制 数据完整性 数据保密性 数据备份恢复 剩余信息保护 个人信息保护

数据的源端加密成为趋势。在数据的产生阶段，即摄像机音视频数据在源端实现数据的加密。

数据（尤其是视频、图片等关键数据）跟踪追溯技术。安全事件发生后泄露源头的追查和责任的判定是及时发现问题、查缺补漏的关键，同时，对安全管理制度的执行也会形成一定的威慑作用。

AI 应用于安全，实现安全可视化和态势感知。人工智能与网络安全深度融合，机器学习、深度学习等人工智能技术在网络安全领域落地应用，助力提升网络安全风险预测、攻击防御等全方位能力。用户行为分析成为“人工智能+网络安全”落地的重点方向。应用知识图谱技术，将用户各类行为进行归类、聚合，筛选出具有某一共性的关联图，对未发生的威胁进行感知和预测；提供更为智能化的决策模式，突破了传统安全技术的局限。

区块链技术的应用为网络安全带来新思路。数据防篡改与验证、多节点分布式冗余、共识机制共同保证区块链所构建数据库中数据的不可篡改；关键信息链上存储，将关键信息的哈希值存储在区块链上，通过区块链上数据的不可篡改确认关键信息的正确性。

5.6 下一代人机交互技术

随着智能技术在安防系统里的应用，产生的数据越来越多，随之而来问题：如何让使用者快速看懂数据，也就是数据可视化的问题。安防行业下一代的人机交互，展现上会朝着操作性和立体性更强的方面发展，交互上朝着互动感更强方面发展，应用上朝着功能业务深度结合的方面发展。

用户界面的操作性及立体性不断加强。普通摄像机反映的是“现实”，这种现实由于缺少附加性的信息，对安保人员的环境熟悉度要求非常高。通过 AR 技术辅助能使屏幕前的安保人员更加及时有效地处理视频画面捕捉到的异常、突发情况。

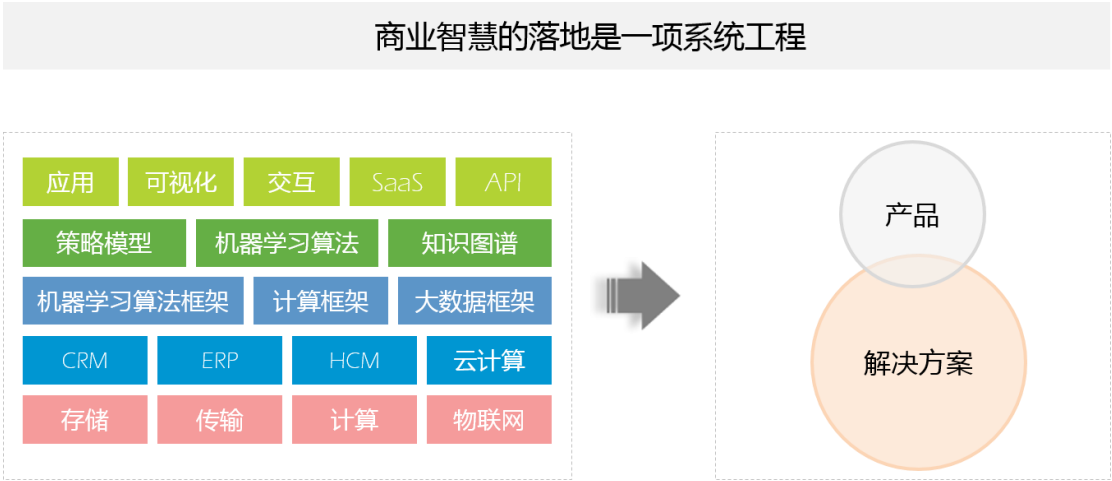
向着多通道互动及智能互动的方向进步。现阶段，主要通过键盘与鼠标来实现人机交互。在感压技术的基础上，技术人员开发出了触屏手机、触屏电脑，得到了初步应用，但由于其带来的交互体验提升有限，并未得到更广泛的应用。随着传感器和人工智能技术的发展，基于人感觉的开发效应通道，如视线跟踪系统、三维听觉定位器、分贝感应器、语音识别系统等利用人的听觉、视觉，进行人机交互成为可能。而这些产物应用安防领域后，可显著的提升安防效果。而且通道切换也不需要频繁的开展，促使人机交互效率的提升。

5.7 系统设计及项目实践能力不断提升

智能业务应用的落地需要建立在合理的成本控制、合格的施工质量、完善的数据整合和配套的管理机制之上。再由配套场景的算法、模型基于高效的计算框架将数据转化为可视化的用户业务，进一步驱动或辅助用户决策。因此，智能业务应用是一项系统工程，架构、算法、计算、数据、应用、工程、管理流程等缺一不可，需要不断加强系统性顶层设计的能力，提高项目实践能力。

由于智能业务的场景性限制，标准化产品背后依然需要集成商、ISV、解决方案/设备供应商为客户提供场景个性化服务。因此，在很长时间里，智慧安防应用仍将以部分标准化产品/解决方案、部分场景定制化产品/解决方案相结合的形式存在。

图 29：商业智慧的落地是系统工程，智慧安防应用与产品/解决方案结合存在



5.8 非卡口存量视频逐步应用

根据统计数据，中国一年有约 5000 万个摄像机需求，实际只有约 50 万个智能摄像机被有效应用，仅占 1%左右，而高达 99%的摄像机无法赋予“智能”属性。这意味着安防+AI 刚刚进入初级阶段。

非卡口场景下人工智能算法的泛化能力是在安防领域落地的主要瓶颈之一。与传统模式识别方法相比，在大数据的支撑下，深度学习算法的泛化能力和复杂场景的适应性有了明显的提升。例如，融合人脸识别、人体轮廓识别、步态识别等多模态生物特征识别技术可实现跨摄像机的人员追踪，在海量的普通非卡口视频中搜索出犯罪嫌疑人的逃跑轨迹，并在刑侦破案中发挥了积极作用。

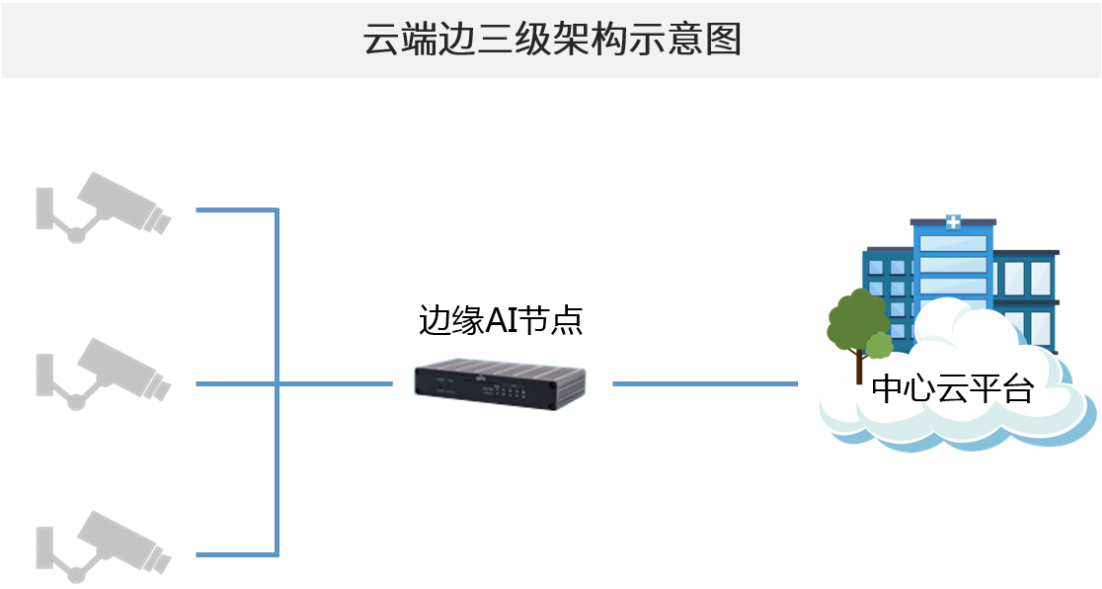
面对海量普通摄像机的存量市场，要实现智能化改造，有几种方案选择：

第一种方案，是将现有的普通高清摄像机替换成 AI 摄像机，这种方案成本高，会造成巨大的社会资源浪费，基本行不通。

第二种方案，普通摄像机将视频码流传输到中心云平台，在中心部署 AI 服务器，统一做 AI 分析。这是目前最常用的一种方案。这个方案带来的问题有两个：一是中心 AI 服务器的部署成本高；二是数据全部送到中心 AI 服务器进行分析，时延大，带宽占用大。

第三种方案，采用“云+边+端”架构，在前端网络中增加边缘设备，摄像机只要就近将视频码流传输到边缘设备，由这个边缘设备负责 AI 分析，将 AI 分析的结果传输到中心云平台，也可以和中心云平台的 AI 服务器一起完成复杂的 AI 功能。

图 30：云端边三级架构



在第三种方案中，边缘设备还可以同时具备超感传感器，实现电磁信号、RFID、PM2.5 等物联网数据的采集和传输，具备完整的 AIoT 能力。

图 31：边缘计算示意图，更快更便捷实现前端智能



综合来看，采用边缘 AI 设备的方案，能更方便、快捷的实现前端智能，实现对当前海量的普通监控摄像机的 AI 改造，更好的实现后端 AI 向前端 AI 的过渡。

参考文献

1. 《中国科学院第十九次院士大会报告》，谭铁牛，中国科学院第十九次院士大会，2018.5
2. 《人工智能发展白皮书技术架构篇》,中国信息通信研究院&中国人工智能产业发展联盟，2018中国人工智能峰会，2018.9
   http://www.catr.cn/xwdt/ynxw/201809/t20180907_184751.htm
3. 《中国人工智能发展报告2018》，清华大学中国科技政策研究中心，清华大学，2018.7
4. 《2018世界人工智能产业发展蓝皮书》，中国信通院&Gartner，2018年世界人工智能大会，2018.9
   http://www.catr.cn/xwdt/ynxw/201809/t20180918_185385.htm
5. 《中国人工智能创新应用白皮书》，中国人工智能学会&罗兰贝格，2017.11
   http://www.caai.cn/index.php?s=/home/article/detail/id/433.html
6. 《新一代人工智能发展白皮书》，中国电子学会&CIE智库，2018.3
   http://www.qianjia.com/html/2018-02/26_285790.html
7. 《2018人工智能应用安防行业研究分析报告》，安天下，2018.9
   https://mp.weixin.qq.com/s/3TKWsHPG7o5RR1hoCukU-w
8. 《2017人工智能报告》，36氪研究院，2017.7
   https://36kr.com/p/5084191.html
9. 《2017物联网安全研究报告》，中国电信安全帮&绿盟科技，2017.12
   http://www.nsfocus.com.cn/content/details_62_2646.html
10. 《2017年度互联网安全报告》，腾讯安全联合实验室，2018.1
    https://slab.qq.com/news/authority/1708.html
11. 《北京轨道交通线网客流特征分析》，北京城建，2015.3
    http://www.199it.com/archives/706261.html
12. 《中国网络安全产业白皮书（2018）》，中国信通院，2018国家网络安全宣传周，2018.9
    https://cloud.tencent.com/developer/article/1358278

研究与撰写团队

研究撰写团队	中科院自动化所	徐毅 袁飞 马博 李哲峰 李江 徐浩清 汤昊宬 张勇
	宇视研究院	汤利波 羊海龙 王连朝 成东峻 叶菲 兰进 吕学军 陈乾 吕政 叶康 童景妍 秦洁

注：排名不分先后

中国科学院自动化研究所
Institute of Automation, Chinese Academy of Sciences

中国科学院自动化研究所成立于1956年10月，是我国最早成立的国立自动化研究机构，现设12个科研开发部门，已形成立足智能技术，聚焦复杂信息的智能计算、复杂系统的智能控制、集成化智能系统三个重要方向，基础研究、应用开发与高技术产业化“三位一体”，相互支持、相互补充的格局。

近年来，自动化所共获得省部级以上奖励30余项；发表论文数量逐年增加，质量不断提高；专利申请和授权量连年攀升，获得国际同行的广泛关注和好评。

截至2017年底，自动化所共有在职职工896人，其中科技人员795人，科技支撑人员54人；有4个二级学科博士、硕士研究生培养点，并设有1个博士后流动站；共有在学研究生663人（其中博士407人，硕士256人），在站博士后59人。

中国科学院自动化研究所努力创建具有强大科技创新和可持续发展能力的国际知名的国家研究所，为中国科技事业的发展做出更大贡献！

http://www.ia.cas.cn/

uniview 宇视研究院

宇视科技（uniview）为全球公共安全和智能交通的解决方案提供商，以可视、智慧、物联产品技术为核心的引领者。2011年12月独立运营，2017年进入全球市场前6位（IHS数据），快速行进在通往全球视频监控领域领导者的路上。

宇视研发技术人员占公司总人数50%，每年将营收的15%投入研发，为可持续发展提供有力支撑。

宇视研究院位于杭州市滨江区，主要负责未来五年的战略预研，根据公司战略、技术趋势和市场需求，在关键领域进行快速积累和创新，强调对核心产品和解决方案提供关键技术支撑；跟踪和分析世界前沿新技术发展动态，承担突破性技术的预研，为公司进入新领域提供决策参考，为行业贡献建设性标准。

宇视研究院协同杭州、深圳、西安、济南、天津六大研究所，涵盖人工智能（机器视觉）、大数据、光机电、图像处理、云存储等前沿维度。

http://www.uniview.com/



宇视研究院

www.uniview.com



中科院
自动化研究所

www.ia.cas.cn

原创声明

本报告中所有的文字、数据均受到中国法律知识产权相关条例的版权保护。没有经过中科院自动化所和宇视研究院的许可，任何组织和个人，不得将本报告中的信息用于其他商业目的。

本报告中的资料和数据来源于国内外行业公开信息的收集和分析、项目实际调研总结，结合中科院自动化所和宇视研究院相关分析模型展开。