警院聚焦

基于手机电子围栏的“图码联侦“应用

我们常规的天网工程一般是由前端的互联感应设备加中间的传输网络再加后台的数据系统组成。人工智能算法引入城市安防系统建设大概起步于五六年前，泸州市在当时就非常大胆地引入这类应用系统并取得了良好的效果，后来逐步推广到全省公安系统。目前人脸识别这类人工智能技术在全国范围内已经是非常普遍的公安日常技术侦查手段，但在现在社会矛盾日益激化的背景下，仅仅依靠这些单一的人工智能技术进行侦查存在一定的不足。

因此我们今天给同学们介绍的“基于手机电子围栏的‘图码联侦’应用”就是基于大数据算法和多维数据融合的一种新兴技术。它将多类数据融合并进行综合分析以改变公安侦查工作。

“图码联侦”中的“图”指的是设备图像数据，包括人脸识别、车辆特征等在内的视频图像数据；“码”指的是国际移动用户识别码，也叫手机串码或IMSI码，每一张电话卡与每一个国际移动用户识别码一一对应，相当于手机号码的身份证号码，与手机号码具有唯一对应关系。IMSI码基于用户身份识别认证，公安部门可以通过它实现对某一用户的查找、跟踪。国家近几年在全面推进手机号卡的实名认证，这将会为公安侦查工作带来极大的便利。手机号卡需要搭配相应的互联感知设备以采集对应的数据，这就是手机电子围栏设备，也称电子侦码设备。这是一种用于技侦的特种基站设备，并且由于公安系统使用的侦码设备级别高于运营商基站，我们可以优先捕获信号，获得所需信息而不会影响手机正常通信。这就是具体的手机串码采集流程。

多维数据融合就是将我们日常搜集到的许许多多可能无用的信息进行数据整合，以提高数据的价值。如通过一辆车的车牌号，采集到它的车主个人信息、手机IMSI码，就可以完善这位车主的行踪等信息，与数据库相对比，得出我们所需要的结论。但在现实案例中，人口数据的新鲜度无法得到保证、城镇地区人口基数调查难、重点地区重点人员管控困难等问题还长期存在。此时，电子围栏技术就可以起到相当重要的作用。在一些人脸识别、图像采集技术无法发挥作用的场合，电子围栏技术的引用可以极大地拓宽数据的采集途径、挖掘隐性的互联感知数据间的相关关系、提高数据采集的数量质量、协助公安机关加强对一些地区的治安管控、从最大程度上消除天气等自然条件对数据采集的影响、提高实战应用效果。

一般而言，常在人员密集且相对固定的区域如学校、政府机关所在地及人员密集且流动大的区域如车站、海关设置侦码设备，通过电子围栏实施人员布控。现有实践经验使得公安机关在人口密集区域更倾向于使用功率较小、覆盖范围较小的侦码设备，以求获得更高的数据精度，而在高速路口、国道省道等目标移动速度快的区域使用大功率、大覆盖面的侦码设备。

如今国内外政治环境变化，国家安全、政治稳定、社会治安等问题也日益突出。针对犯罪手段、形式不断翻新、犯罪嫌疑人基本都持有通讯工具，现行系统在轨迹数据方面不够丰富，重点人员管控，态势感知方面存在滞后性等情况，电子围栏技术的应用弥补了原有的天网系统和图像大数据算法在目前侦查工作中的不足，有助于加强对重点人员的管控、维护社会治安，提高了公安机关图上寻踪、轨迹融合的侦查能力。“图码联侦”的应用必将拥有广阔前景。（谢晓颖根据海康威视姜友维讲座内容整理）

2021年警务科技活动周

传承与创新

本报讯（通讯员 冯潇）5月24至28日，学校2021年警务科技活动周如期举办。

本次警务科技活动周以“传承与创新：新时期公安科技工作发展”为主题，由学校主办，杭州海康威视数字技术股份有限公司、中电天奥、中国网安协办，在5天的时间里对多维感知系统、AR高空鹰眼、智慧家居等多项设备进行应用演示和现场互动，并举办3场学术讲座。

在24日举行的启动仪式上，唐雪莲主任对协办此次活动的3家公司表示感谢并要求学校师生，要通过警务科技活动周增强科技创新意识，提升科技创新能力，培养科技创新人才。

新时代智慧警务中的大数据与人工智能

如今，我们处于一个以海量信息和数据挖掘为特征的大数据时代。在新一轮信息技术快速发展及广泛应用的背景下，越来越多的物体随着“物联网、云计算、大数据、人工智能”等技术的出现拥有了“智慧”与“价值”。如何在“科技兴警”这一号召下实现大数据与人工智能技术在公安领域的应用成为了中电天奥的重点研究对象。

“大数据与人工智能技术”的建设自然离不开“数据挖掘分析”与“算法模型”。通过互联网开放数据、真实案件数据和常识以掌握全量数据概况，再综合分析提取出公安所需的社会关系特征、行为特征、个人特征，从而形成特征宽表，结合算法构建相应模型，筛选人群与结果运算，最后通过业务回流、数据回流，形成可迭代的模式。这就是“大数据与人工智能技术”在公安领域的一整套技术操作流程，而像这样的技术操作与智慧公安所叠加产生的“化学反应”已经围绕在我们身边。

大数据在智慧公安中的应用广泛，小到安检异物自动检测、火情检测、车辆行人重识别，大到人群聚集点人流量预测及风险评估、步态识别、物体检测与跟踪、异常行为自动检测，大数据构建出了跨媒体的数据汇聚融合平台，实现对非结构化数据（包括视频数据、文本数据、音频数据、遥感数据等）的结构化处理，为公安机关打造出了一个“看得见、搜得出、找得到”的融合多源多媒体数据综合服务平台，大量应用于公安侦查、预防、指挥三大场景。

在过去，第一代指挥中心依托110报警服务台，采取“单一接警、逐级指挥”的指挥调度模式，第二代依托信息化系统应用，通过警用电子地图，精准调派警情周边和就近警力的处警处置。而如今，运用大数据、人工智能等技术支撑的第三代110指挥中心则以实战问题为导向，通过可视化综合警情处置，可视化重大事件指挥决策，智能信息处置、情报一体化、管控一张网、警务督导等，重构具有先进性、科学性和实用性的新一代智慧公安，以实现情报指挥一体化的目标。

公安信息化走向数字化、网络化、智能化已是大势所趋。而大数据与人工智能技术也将进一步推动和强化公安各领域可视化、结构化、多元化、数据化、动态化，在“盘活”公安底层数据资源的同时，赋能公安防控、打击、管理等业务工作，有效提升警务工作能力。（谢佳成、闫旭根据中电天奥周笛讲座内容整理）

以网络攻防为桥梁织牢大数据安全网

大数据，是近年来信息化时代的显著表现之一。我国公安部门的大数据技术是比较成熟的，在全球都算是首屈一指。比如，公安局可以通过大数据获取犯罪集团或嫌疑人的位置信息，甚至进一步了解到犯罪集团内部的相关信息，包括财务信息、流水信息。

但是，如果犯罪嫌疑人或犯罪集团在境外，并且他们使用的互联网服务的运营商是国外的，那使用国内的大数据就无法准确获取这个组织相关的内部信息。此外，对于诈骗集团涉及到的多方支付、具体金额、具体细节、受害人等相关信息则更是难以得知了。

为了解决这个问题，有人提出建议，在网络上“翻墙”进行数据搜集。但是，两年前江苏警方经过实践却收获寥寥。

另一方面，在大数据的背景下有一些漏洞值得注意——有操作系统漏洞，比如ms17-010；有网络协议漏洞，比如DDOS攻击、ARP攻击等；有应用程序漏洞，比如文件上传漏洞获取系统控制权、xss攻击获取登陆凭证、钓鱼链接利用受害者凭证执行预期外的结果、SQL注入获取数据等。而黑客集团就会利用这些漏洞，攻击数据网，夺取大数据系统中的重要资料，进而可能会使国家遭受重大的损失。

这时，网络攻防就应时而生了。

网络攻防中的一项重要内容是渗透测试，它是通过模拟黑客对目标系统发起授权攻击的一种能够发现目标系统漏洞并予以破坏的测试技术。听起来有点类似黑客入侵，它在本质上确实是黑客技术，能通过在信息系统中的攻防对抗，实现获取系统相关权限的目标。但是，它还兼重防御，能为后期系统防护提供修复目标和思路，提高大数据系统防护水平。

当然，渗透测试必须是在公安部门授权的情况下才能正常开展。因为，在非授权的情况下，攻击者可能会造成个人信息、数据泄露等情况，对社会造成一定危害。

总而言之，在正常情况下，网络安全中的攻与防，犹如一杆尖锐的“矛”与一块坚固的“盾”，只有掌握了黑客攻击技术与防御应对的方法，“矛”“盾”结合，才能织牢大数据安全网，促进大数据健康发展。

科技发展日新月异，犯罪手段也日益高科技化，为了保障公安对犯罪行为的打击力度，更好维护社会稳定，大数据技术是公安部门必须利用的技术手段。所以，当下，我们要普及网络安全技术，完善授权情况下的渗透测试，力争补足共享信息系统的漏洞！（闫旭根据中电网安刘文胜讲座内容整理）

（本版指导老师 宋杰）