【名家专栏】中共的网谍活动与生物识别监控

中共将网络间谍战略整合至农业物联网，想通过数字手段重塑地缘政治影响力。(shutterstock)

更新 2024-12-14 6:42 AM 人气 148

标签：中共，数字战略，智慧农业，战略风险，物联网，生物识别监控，网络间谍

【大纪元2024年12月13日讯】（英文大纪元专栏作家Carlo J.V. Caro撰文／原泉编译）中共将网络间谍战略整合至农业物联网，并向全球输出生物识别监控系统，这已经超出了追求技术进步的范畴，更是蓄意通过数字手段重塑地缘政治影响力。

通过农业物联网标准化进行网络间谍活动

中共在农业物联网（IoT）中的渗透是其全球科技战略中一个关键但尚未充分探讨的领域。通过华为、阿里云等关键企业，北京已将物联网技术嵌入拉丁美洲、非洲和亚洲的农业系统。这些举措通常被视为发展伙伴关系，旨在改善粮食生产与供应链韧性，同时能够收集具有深远战略和地缘政治影响的大量农业和环境数据。

农业物联网系统通过收集实时、高分辨率的数据，彻底改变农业生产方式，这些数据涉及土壤湿度、养分水平、天气条件、害虫侵扰、灌溉模式、作物生长速度和物流动态等变量。

像华为和阿里巴巴等中国公司正走在这一技术进步的前沿，他们设计了支持精准农业的平台，通过整合先进的传感器、云计算和人工智能来优化农场管理。

在肯尼亚，华为积极与当地合作伙伴、肯尼亚农业与畜牧研究组织合作，实施提高农业生产力的可持续性的智能农业解决方案。部署监测关键农业参数的物联网传感器，并将这些数据传输到云平台，利用人工智能算法提供可操作的建议，农民们因此提高了作物产量。这些举措不仅提高了当地的农业生产力，还增强了中共在该地区农业领域的影响力。

同样，在2020年，马来西亚政府与阿里云建立了战略合作伙伴关系，推进其智能农业议程，体现了利用数字技术促进农业转型的承诺。例如，2019年，马来西亚农业科技公司Regaltech与阿里云合作，为榴莲种植园开发了一个智能农业平台。该平台利用阿里云的ET农业大脑（一个分析大量农业数据的人工智能平台）、物联网设备和无人机监测作物健康状况，优化资源使用，实现农业流程自动化。这些系统在提高产量品质的一致性方面显示出可喜的成果，同时由于自动化而降低了劳动力成本。

这种数据整合的战略意义深远。在阿根廷——中国大豆的主要供应国——物联网系统提供了大豆和玉米等重要农产品生产的详细信息。2022年，阿根廷向中国出口了480万吨大豆，主要用于中国迅速发展的畜牧业的动物饲料。通过分析作物产量、气候条件和供应链动态的纵向数据，中国实体可以预测农业产出，识别干旱或虫害爆发的脆弱性，并精准制定进口策略。获取这些信息不仅为经济决策提供了依据，还使北京在与关键合作伙伴的贸易谈判中有了筹码。

这种数据的地缘政治效用非常显著。举例来说，在撒哈拉沙漠以南的非洲，物联网系统可监控因干旱而导致的主要作物产量下降，从而使中国在市场动荡发生之前确保进口。2022年，中国农业机械市场价值超过240亿美元，其中大量出口到非洲国家的产品采用了由中国云基础设施支持的物联网“智慧农业”解决方案。这些系统虽然被标榜为促进发展工具，但却建立了依赖关系，增强了中共的影响力。数据获取通常受到不透明协议的约束，使得北京方面能够对采用这些技术的国家保持战略影响力，尤其是在涉及气候冲击或粮食危机的情况下。

此外，农业物联网数据可以被武器化，以操纵贸易动态。一个相关的例子是哈萨克斯坦，中共对该国农业基础设施的投资已整合了物联网系统，用于监测小麦和大豆等关键作物。有了精确的产量数据，北京能够预测短缺或过剩，商谈有利于自己的贸易条款，并相应地调整进口策略。历史上的类似事件，比如，中共在外交关系紧张后于2020年对澳大利亚的大麦和葡萄酒征收关税，都突显了中共利用贸易关系实现地缘政治目标的意愿。虽然这些行为不涉及物联网，但它们突显了中共利用经济依赖关系作为影响力工具的模式。

中巴经济走廊框架下的巴基斯坦是另一个具有启发性的例子。巴基斯坦引进了中国先进的灌溉系统和基于物联网的作物管理技术，以实现农业现代化。尽管数据共享协议尚不明确，但物联网系统的整合使中共能了解小麦和棉花的生产态势，从而能够根据更广泛的地缘政治目标，提前调整进口，或提出符合其政策的建议。

同样，在老挝和柬埔寨，中国物联网技术嵌入他国的农业系统，引发了对数据主权的担忧。这些系统能让北京发现粮食安全的薄弱环节，从而影响国内政策，并加强这些国家经济对中国基础设施的依赖。

中共通过《中国标准2035》等倡议推动全球物联网标准化，这对其在技术和数据治理方面的雄心至关重要。通过将专有的物联网协议嵌入国际框架，北京确保其技术对全球物联网网络中不可或缺。华为和中兴通讯在出口物联网解决方案方面走在前列，特别是在拉丁美洲，华为的智能农业平台已在当地获得青睐。整合中国开发的加密技术可确保与中国国内平台的兼容性，巩固了中共对这些生态系统的控制，并加强了其收集和处理战略数据的能力。

这种影响力延伸到对信息流动的控制。根据中共的《数据安全法》，企业必须在特定条件下与国家相关部门共享数据，这提高了中共从依赖中国技术的地区获取敏感信息的可能性。将物联网农业数据与贸易及基础设施的洞察力互相参照，可以获得有关伙伴国家的全方位、多层次情报。虽然还没有出现确凿的证据证明存在系统性的物联网数据滥用行为，但这种能力与中共以数据驱动扩张全球影响力的战略相一致。

与农业物联网相关的网络安全风险同样值得关注。2021年，全球最大肉食品加工商巴西JBS公司遭到网络攻击，导致全球肉类供应链中断数周，突显了数字化农业系统固有的脆弱性。如果中国公司建立的物联网也受到类似的攻击，恢复工作可能会因为中共对关键数据的潜在控制而

受到阻碍，从而使缓解措施和政策反应变得复杂，这种情况凸显了物联网技术的双重用途性质，既是发展工具，也是战略杠杆。

尽管农业物联网在中共数字战略中的重要性与日俱增，但这一主题仍然未得到充分探讨。分析师和政策制定者通常关注电信和人工智能等领域，却忽略了与粮食安全、气候脆弱性和地缘政治稳定之间的交叉关系。例如，美国农业部2021年关于农业创新的报告，未能解决外国控制的物联网系统带来的战略风险。与此同时，华为继续扩大在拉丁美洲的业务，将物联网技术嵌入到这个在全球农业出口中发挥关键作用的地区。

先进的生物识别监控和行为数据开发

除了在农业领域的网络间谍活动外，中共在生物识别监控和行为数据开发方面的能力也大幅提升，这是中共全球数字战略的关键轴心，将技术创新与广泛的地缘政治野心交织在一起。中国视频监控巨头海康威视（Hikvision）和大华科技（Dahua）等政府支持的企业，以及商汤科技（SenseTime）和旷视科技（Megvii）等人工智能先驱，已经率先开发了远超传统人脸识别的技术。步态识别、声纹识别和情感检测系统等创新技术，实现了前所未有的行为监控，提供了细致入微的洞察力，将监控能力提升到了新高度。

截至2023年，中国企业已经向非洲、南亚、拉丁美洲和东欧的八十多个国家出口了生物识别监控系统。例如，肯尼亚的“平安城市”计划，将大约1,800台海康威视摄像头，整合到内罗毕的中央警察监控网络中，凸显了中共的深度参与。同样，在巴基斯坦拉合尔市（Lahore），在中巴经济走廊的框架下，华为的监控基础设施将生物识别数据与城市管理系统相结合。除了硬件安装，中国企业还将专有软件生态系统和先进的机器学习算法嵌入到这些项目中，巩固了对数据管道的控制，并促进了对中共管理平台的依赖。

这些系统的影响远远超出了表面监控的范围。据报导，在津巴布韦，配备了人工智能分析系统的中共监控摄像头已被用于识别政治异见人士。在塞尔维亚，中企开发的平安城市系统因使用面部识别技术追踪反政府抗议者而引发争议。安装这类监控系统通常伴随着不透明的许可协议、债务融资和广泛的服务合同，这造成了长期的技术和财务依赖。

中共的生物识别监测技术已经达到了以前被认为是理论上精度的水平。例如，步态识别领域的全球引领者、人工智能企业银河水滴（Watrix）声称，其系统可以在超过50米的距离内以96%的准确率识别个体，即使在拥挤的环境中或面部模糊的情况下也是如此。此类技术已在新疆等

敏感地区部署，当局用它们监控维吾尔族群体，并标记“异常行为”。同时，在上海，医院采用步态识别系统限制未经授权的人员来访，突显出该技术在安全和民用领域的多功能性。

情感识别是中国人工智能的另一个前沿领域，进一步丰富了中共的监控手段。通过分析微表情、声调变化和生理信号，这些系统可以推断情感状态，其应用范围涵盖从教育到执法等多个领域。例如，在杭州的智慧学校倡议中，据说摄像头会监控学生的情绪，以优化课堂管理——这一做法引发了关于隐私和心理健康的伦理担忧。

在新疆，类似的系统被用于评估被拘留者在审讯过程中的压力水平。这些工具服务于中共广泛的“维稳”战略，将监控嵌入日常生活，以确保对社会的控制。

在中国国内，生物识别监控支撑着中共的社会信用体系，该体系将大数据分析与行为监测相结合，规范个人和企业的行为。在深圳等城市，面部识别摄像头能够识别乱穿马路的行人，并公开展示他们的图像，以羞辱违规者。有些系统更进一步，给违规者发送短信，并将处罚与其社交账户挂钩。尽管中共社会信用体系的更广泛的应用（比如限制受教育或享受医疗服务）仍有争议，但其有文件证明的影响包括旅行限制。到2018年，数百万社会信用评分低的公民被禁止购买机票和高铁车票，显示该体系是如何通过限制出行来强制遵守规定的。

在国际上，中共监控技术的出口带来了深远的风险，尤其是在监管框架薄弱的国家。实际上，这些国家进口的不仅是硬件，还有助长威权主义做法的治理模式。在乌干达，华为价值1.26亿美元的闭路电视系统，表面上是为预防坎帕拉的犯罪而设计的，但却因为被用于监控反对派人士而受到批评。在埃塞俄比亚，与中企修建的非洲联盟总部等基础设施有关的数据泄露，加剧了滥用数据的指控。这些例子说明了（引入这些系统带来的）技术依赖和政治胁迫的双重脆弱性。

将中国标准融入新兴市场的治理基础设施，代表着中共深度固化其战略影响力。这些监控系统通常伴随着不透明的协议、专属协定和维护要求，将采用者与中国企业捆绑在一起，将监控嵌入到公共管理的运作结构中。除了操作功能外，这类出口还使侵入性做法正常化，破坏了民主规范，助长了恐惧气氛。对于缺乏严格保障措施的国家而言，这种对公民自由的侵蚀不仅会压制反对声音，还削弱了主权，创造出一种更贴近专制原则而非民主理想的治理模式。

战略整合和全球影响

中共将网络间谍战略整合至农业物联网，并向全球输出先进的生物识别监控系统，这已经超出了追求技术进步的范畴，更是蓄意通过数字手段重塑地缘政治影响力。通过将技术嵌入新兴经济体的关键基础设施，中共获得了无与伦比的获取海量数据集的机会，这些数据集既服务于经济目标，也服务于政治目标。

一个新出现的情况是，这些数据可能会互相结合，在政治动荡期间影响粮食援助决策。农业物联网系统可以识别面临饥荒风险的地区，而生物特征数据个人资料可以对当地人口进行评估，以衡量反抗或顺从的程度。通过根据行为趋势调整援助分配，中共可以选择性地实现或破坏地区稳定，以进一步推进其战略目标，加深对其技术和经济基础设施的依赖。

通过专有标准和人工智能驱动带来的洞察力，中共植入了全球依赖关系，这不仅降低了合作国家的自主权，还增强了中共塑造国际规范的能力。在这个由依赖数字关系定义地缘政治力量的新时代，这种数据驱动方法巩固了中共的影响力。

（文章源自RealClearWire）

作者简介：

卡洛·J· V·卡罗（Carlo J.V. Caro）在哥伦比亚大学获得硕士学位，是一名政治和军事分析师。

原文：China’s Digital Strategy: Cyber-Espionage and Biometric Surveillance in Global Technological Expansion刊登于英文《大纪元时报》。

本文仅代表作者观点，并不一定反映《大纪元时报》立场。

责任编辑：高静#

相关专题：名家专栏

自定义设置