军界瞭望

注意！这会泄密的

俄乌冲突“风行”开源情报

开源情报(OSINT)是指通过公开可用的数据和信息获取的情报,不仅可通过搜索引擎获得,还包括报纸、图书、杂志、图片、政府公开信息、互联网等许多其他来源。尽管开源情报问世于上世纪,但真正大规模应用却是在当前的俄乌冲突中。在高技术加持下,开源情报的数量和作用直线上升,正成为关乎战局走向的重要利器,同时也提醒每一个受冲突影响的人,也许你简单地跟谁“问个好”,都可能造成致命的泄密!

◀ 乌军人滥用的一款手机App,曾导致严重泄密

■ 开源情报的军事价值越来越高

轻取“满满干货”

相当长时间里,外界研究俄乌冲突时,普遍把关注度集中到某种武器的效能上,如“武器化”改造的民用无人机、星链通信网或低轨侦察卫星,但从俄乌前线反馈看,双方士兵最热衷用触手可及的智能手机、迅速更新的大数据软件、社交平台话题群等民用技术与特定的军事技术交互,组网交流开源情报,协调作战行动,效率远超传统封闭的军事情报指挥网络。

先看俄方,2023年4月初,美国空军情报102团一等兵特谢拉出于炫耀,在名为“恶棍活动中心”的社交群里发布了数十张关于北约援乌机密文件的翻拍照,尽管美方在3天后将其抓捕归案,消除影响,但泄密效应已然覆水难收,这些出自美国中央情报局、国防情报局、国家地理空间情报局等敏感机构的情报摘要或简报迅速被俄总参情报总局(格鲁乌)以及民间思想库所运用,逆向查明俄军导弹袭击乌克兰电力设施后的效果、北约最近两个月援乌装备到位情况、乌军“春季攻势”准备情况等,可谓“干货满满”。更重要的是,俄政府从这些开源情报中掌握了美方擅自向乌克兰移交韩国制造的炮弹,从而破坏首尔在俄乌冲突中不向乌提供武器援助的政治承诺,为俄外交工作提供了“证据实锤”。更有甚者,2022年11月11日、11月25日、12月20日,名为“顿涅茨克小丑”的俄黑客组织,利用乌军人在社交平台上的“口无遮拦”,获得权限多次入侵美国为乌国防部研制的“三角洲”部队指挥系统,下载北约向乌军提供的大量情报数据,后来乌国防部也承认黑客在“三角洲”系统肆虐了整整13分钟,窃取了从当年4月27日到11月6日的大量情报,其中有相当部分涉及北约和乌克兰在俄境内秘密活动内容,对俄罗斯打击国内的“第五纵队”帮助甚大。

乌方也不遑多让,开战之初,一度对全局失控的乌政府放权给“特殊技能人才”(含预备役军人),将操作简便、可重复并可随时投用的信息技术组合起来,弥补乌方军政高层的指挥空白。像DiYa、电报、Viber等应用程序将智能手机变成数据收集工具,乌克兰平民可向聊天机器人(一种通过文字或语音与人类交流的计算机程序)发送照片、视频或短消息,提供俄军行动信息。乌克兰数字转型部称,俄乌冲突爆发后短短一个月,就有26万人通过DiYa报告俄军行动情况。2022年3月的基辅会战中,乌军士兵使用轻松可得的技术组网,传送重要情报和命令的效率竟超过其野战指挥系统。尝到甜头后,乌方上至将领,下至操作无人机的普通士兵,都倚靠这种互联系统收集、分析城市街区或者战场上的各种数据,并将这些数据形成实际可用的成果。如今,在北约盟国和国外开源情报公司的帮助下,乌军利用国家和私人技术组建数据收集、通信、数据分析和行动等4个方面的指挥系统,而这些系统全都建立在开源情报的基础之上。

用好“巨型数据包”

早在无人侦察机广泛参战前,乌军士兵就利用商业组网卫星等传感器及其提供的开源情报,来掌握俄军动向。这些传感器收集空中、太空和网络空间的广谱信息,从而形成清晰的战场全景态势。例如,西方主要商业卫星服务商向乌方大量提供开源的地理空间情报,可直观反映俄军部署情况。ICEYE、Usra Space、MDA等公司则借助自己拥有的合成孔径雷达卫星(SAR),定向搜集某一战线的俄军目标图像,帮助乌军决策层排列打击对象的优先次序。2022年2月,乌军就通过卫星照片发现基辅北方开来的俄军长达60公里的装甲车队,随后断然炸毁伊尔片水库,接着组织多轮伏击,迟滞了俄军进攻。乌方还把电话、社交网络变成公开的情报设备,用来收集识别俄军及其技术装备的元数据。乌军曾经利用从社交媒体电报的通话内容中获得的原始数据,定位并打击了马克耶夫卡一带的俄方瓦格纳军事集团。

当2022年底无人机装备量急速上升后,乌军一线部队已普及了民用无人机侦察手段,常态化监视并勘察己方阵地数公里范围内的情况。迄今,乌军光损失的民用无人机就超过数以万架,但补充却源源不断。英国皇家联合服务研究所估计,乌军几乎做到连排级分队都装备了无人机,虽然这些平台型号五花八门,分布极为广泛,但它们收集的视频、照片等素材汇总成“巨型数据包”,供开源情报分析师“沙里淘金”。要知道,美国提供的高速低轨卫星通信网,将传感器与战场上任何一点上的处理器连为一体,使那些稍纵即逝的目标也容易被乌军捕捉并打击。此外,乌方移动通信和互联网运营商仍然通过固定信号塔、蜂窝和无线通信基站以及临时接入点提供分散式通信网络服务。这样即使遭受俄军猛烈炮击,也可以保障通信稳定可靠,这一点比单一系统运转重要得多。

再看俄军,经过几轮挫折后,也急起直追,学习和掌握众多开源信息使用手段后,在私营公司支持下利用人工智能算法和数字战场指挥系统,将零散数据整合成统一的战场作战图,里面汇聚了所有主要战区的敌军情况。俄方社交媒体上的聊天机器人能将成千上万人发送的信息汇总成完整的战术侦察数据库,这包括原始地理数据、用户元数据、图片或者文字、接触时间和地点等等,以确定所报情况的真实性,并确定优先顺序。到最后,一条普通的微博信息,就有可能为俄军实时提供对手的移动情况。据称,俄罗斯一家私营公司开发的人工智能软件能与军方的卫星成像照片连接起来,对图像进行连续分析,再结合公开的乌克兰地理空间数据,从而让俄军获取乌军作战及北约军援活动的实时情报。

此外,俄乌军方都利用Primer自然语言处理算法等工具,在实时或者录下的对方电台节目内容基础上挖掘出简短的情报报告。这一工具可以获取情报信号,在录音基础上生成完整的对话记录。此外,接口可以生成数据包和文字报告,指出部队位置、人数、装备、活动情况和未来企图等情况。

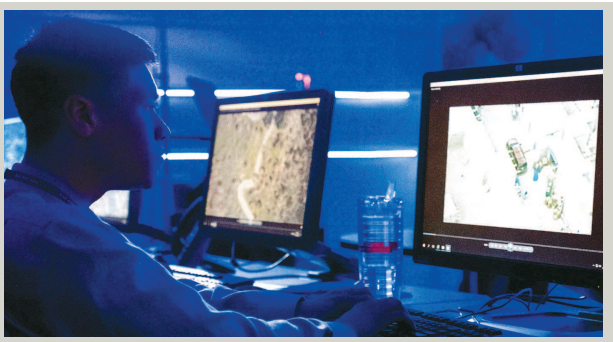
发现即打击

据俄乌双方各自发布的战报,开源情报在歼灭敌方有生力量方面发挥了不可估量的作用。乌军总参谋部在电报账户上透露,借助开源情报支持,2022年11月,乌军消灭了1500多个敌对目标,其“三角洲”指挥系统利用人工智能获取的数据,将其融入地理空间照片、视频、地图和情报报告中,大大提升旅营级单位的情报共享能力,并减轻了横向通信的负担。乌克兰从事开源情报业务的国际公司莫法尔,在开战后持续对电报社交媒体上发布的海量冲突图片进行了分析,把图片与谷歌地图、谷歌街景上的图片整合,用于识别俄军特定目标的身份和位置,并标注在地图上。这项工作最突出的战果,莫过于2023年莫法尔只花了两个半小时,就查出俄军皮亚特纳什卡旅的位置,随后乌军用美制M142火箭炮袭击了该旅基地。此后,莫法尔公司运用相似的套路将这种“发现即打击”的作战循环重复了多次。有趣的是,俄军也在效仿类似做法,抓住乌克兰基层军人“随手拍”“大嘴巴”所暴露的蛛丝马迹,成功打击了乌军在扎波罗热、巴赫穆特、马林卡等地的屯兵点和物资堆积场,造成对手重大损失。

事实上,随着人们对社交媒体平台的依赖,运用开源情报进行侦察定位的军事活动会越来越常见,重要性显而易见。曾任英国国防情报部门领导人的约翰·霍肯霍尔将军指出,目前部队指挥员对开源情报和秘密情报的使用比重已从过去的“二八开”反转为“八二开”,“俄乌冲突所刺激的开源情报技术创新运动已超出战术范畴”。事实上,北约已于2022年夏天投资10亿欧元,成立名为“面向北大西洋的国防创新加速器”的投资基金,专注于开源情报搜集运用以及与军事指挥的深度融合,毕竟没有人想再重演俄乌冲突所暴露的弊端。 常立军 梁梵

▶ 被开源情报定位的俄军瓦格纳集团营地

▶ 俄军导弹打击后的乌克兰军情总局的卫星图像



■ 开源的视频或图像数据成为各国军界的『情报富矿』

军情揭秘