监测数据“虚胖”，这个组织暗中干着怎样的勾当？

不可忽视的数据安全风险

□据新华社报道

进入信息化时代，数据被广泛采集汇聚和深度挖掘利用，在促进科技进步、经济发展、社会服务的同时，安全风险也在不断凸显。

11 月 1 日，在反间谍法颁布实施 7 周年之际，国家安全机关公布了一起数据安全案例，披露了相关数据被境外别有用心的人窃取利用，抹黑我国际形象、危害我国家安全的过程。

今年 2 月，某国一家研究机构公开发表了一篇“科研文章”，诬称上海海岸线的垃圾密度是澳大利亚和美国的 10 倍，并抛出了所谓的“有力证据”。然而，事实证明，这家机构得出的结论完全站不住脚，其所引用的数据存在极大偏差。

这家研究机构宣称的“有力证据”从何而来？这背后藏着怎样的秘密？

这些数据的来源都指向境内的某海洋公益组织。时间回到 2019 年 6 月，国家安全机关接到群众举报，反映境内某海洋公益组织在我国境内设立海洋监测点，搜集海洋监测数据。该组织声称海洋监测数据均为国家有关部门搜集和使用，要求各监测点通过互联网每两个月向该组织上报数据。

但经国家安全机关核实发现，有关部门从未接收过该公益组织提供的数据信息。

问题出在何处？这一情况引起了国家安全机关的重视，随即展开调查。经查，这个海洋公益组织并不简单。

国家安全机关调查发现，该组织有着复杂的境外背景，自 2014 年以来，持续接受 20 多家境外机构资助。仅 2018 年至 2019 年一年多时间，就接受了两百多万元境外资金，其中仅一笔资金向有关部门备案。

其实，该组织是依据某境外研究机构制定的流程，在我国沿海地区设立海洋垃圾监测点，搜集垃圾种类、重量、分布密度等信息，形成并发布中国海洋垃圾地图和研究报告。据国家安全机关办案干警介绍，该海洋公益组织接受境外机构资助，采取不科学的方式监测，为其提供虚高的数据。

此外，该组织在各地监测点选择上也有“讲究”。他们要求监测点申报者提交备选监测点的详细经纬度、地理位置、地貌水文、现场照片等数据后，再行确定监测点，并派人前往监测点实地考察。

更为可疑的是，该组织会指定一些具体监测点，其中就包含一部分靠近军事目标的地点。比如在上海设立的一处监测点，其对面就是某军港。在这个地点已经被围栏拦住并且大门上锁的情况下，该组织仍会让人绕过滩涂抵达该地点开展监测活动。

国家安全机关介绍，截至今年被查处前，该组织在我国设立的监测点，已基本覆盖我国自南向北海岸线，辐射我国南海、东海、黄海、渤海区域。

这些数据将对我国造成多大危害？

国家安全机关干警介绍，该组织发布的垃圾监测报告中，将其结果与国家海洋公报中的相关数据进行比较，并发布与官方数据差异较大的海洋垃圾统计数据，故意抹黑炒作我环保问题，损害我国的国际形象。

另一方面，直接威胁我国军事安全。据介绍，该组织设立的 22 个涉军监测点，已对我海上军事安全构成现实威胁。其收集的经纬度、环境、地质、海洋流量等信息，极易被境外情报军事机构利用，对我造成潜在威胁。

目前，依据反间谍法及其实施细则，国家安全机关已责令该组织进行整改，关停 22 个涉军监测点，消除不良影响，并对该组织作出“没收违法所得”“警告”处罚。

国家安全机关干警表示，国家安全机关将坚决依法打击处置境外势力及其境内代理机构在海洋、环保等领域的渗透、窃密等活动，积极防范化解风险，切实维护国家安全。同时，提醒广大群众一经发现可疑且危害国家安全行为，要及时拨打国家安全机关举报受理电话 12339。

近年来，境外间谍情报机关等危害我国家安全的行为已经不再局限于传统安全，非传统安全领域形势越发严峻。我国各行业产业、重要企业的基础性数据，都是境外间谍情报机构觊觎的目标。

对此，社会各界和广大群众都要提高警惕，防止在不知不觉中被不法人员利用，对我国各领域国家安全造成重大危害。国家安全，与每个人息息相关，只有大家都积极行动起来，加强防范，才能筑起坚实有力的防线。

北京市出台强化节能实施方案

副中心行政办公区原则上停止外景照明

□据新华社报道

昨天，北京市发展改革委等 11 部门联合印发《北京市进一步强化节能实施方案》。方案提出，将发挥节能的“第一能源”作用，党政机关、国有企业、学校等事业单位要带头采取更严格、更精细化的节能管理措施，副中心行政办公区带头做好表率，各项措施率先达到行为规范要求，原则上停止外景照明。

方案提出，党政机关、国有企业、学校等事业单位要带头采取更严格、更精细化的节能管理措施，要优化办公区门厅、走廊、卫生间、电梯间等不同区域照明方案，充分利用自然光，加强感应控制，杜绝“白昼灯”，会议结束及下班时随手关灯，杜绝“长明灯”。同时，推动党政机关、事业单位能耗数据实时监测并接入北京市节能监测服务平台，率先推动副中心行政办公区各单位实现电耗实时监测并接入平台。

方案还提出，将对石化、水泥行业严控、压减年度能耗规模，加强重点数据中心的电耗监测，对能效水平较低和违规数据中心的整改，对虚拟货币“挖矿”活动排查清退。

方案还强调，要依法依规开展节能工作，确保市民生活用能，不得以强化节能名义影响企业正常生产经营用能。

北京市发改委有关负责人表示，将发挥党政机关和国有企事业单位表率作用，大力倡导全民行动，确保全年万元地区生产总值能耗持续下降，两年平均下降 5%左右，能源消费总量控制在 7250 万吨标准煤左右，为实现“十四五”时期绿色北京建设目标提供有力保障。

江苏警方侦破一起游戏外挂案

□据新华社报道

记者从江苏省靖江市公安局了解到，近日，在“净网 2021”专项行动中，当地警方通过 3 个月缜密侦查，侦破一起提供侵入、非法控制计算机信息系统程序、工具案，辗转 4 省，抓获制作、销售游戏外挂程序人员 5 名。

今年 7 月，靖江市公安局城西派出所接游戏玩家小袁报案称，他玩某手机游戏时发现有人使用并出售外挂。小袁告诉民警，出售外挂者声称，该外挂具有“透视”功能，可掌握对手的实时信息。小袁花费 240 元购买该外挂，确认是作弊软件后报警。

民警很快锁定向小袁出售外挂的嫌疑人陈某。9 月 6 日，侦查人员赶赴江苏常州将陈某抓获。据陈某交代，自己只是销售代理，平时通过 QQ 群发布广告，真正的开发者一般用支付宝收款，实名登记为卜某。

靖江市公安局随即成立由网安部门牵头的专案组。9 月 8 日，民警发现卜某在四川成都的行踪，赶赴当地排摸蹲守，10 日在一出租屋内将其抓获。9 月 26 日，侦查人员在成都另一地点抓获与卜某共同开发外挂的王某，10 月 15 日在湖北武汉抓获销售总代理董某，10 月 26 日在福建福州抓获一级销售代理兰某。

经审讯，卜某、王某等人对违法犯罪事实供认不讳。原来，刚满 19 岁的卜某是一名大学新生，他精通编程，看到手机游戏玩家众多，遂和同龄的王某商议，从 2019 年开始开发“透视”外挂，前后更新了 7 个版本。

他俩还发展董某为外挂销售总代理，将外挂通过 QQ 群、微信群以 80 元至 120 元包月的形式销售。兰某、陈某作为一级销售代理，再将外挂加价出售。

经统计，自 2019 年以来，该团伙已非法获利 70 余万元。目前，卜某等 5 人因涉嫌提供侵入、非法控制计算机信息系统程序、工具罪，被靖江市公安局依法采取刑事强制措施，案件在进一步侦办中。

警方提醒，制作游戏“外挂”是违法犯罪行为，广大网民应当增强守法意识，不要为违法犯罪推波助澜，共同营造公平、清朗的网络环境。

靠刷赞、泼污水挣零花钱

——揭秘娱乐圈兼职“水军”江湖

□据新华社“新华视点”报道

晚上 8 点，一条影视宣传任务在微信群内发布。姜瑞（化名）很快就在群内敲下回复，随后她登录自己的微博账号，将群内早已准备好的文案和图片发送出去，“xx 的演技真的好有感染力，情绪传达相当到位。”结尾附上作为宣传重点的话题词条。待群主审核完任务发送情况后，姜瑞便成功获得两元的收入。这就是姜瑞兼职工作的主要内容——当一名娱乐圈“水军”。

刷好评、写推广软文、泼污水……有的一个月能挣上千元。“新华视点”记者调查发现，游走在灰色地带的网络“水军”主要是一些兼职人员，他们在网上接单，兼职做“水军”挣零花钱。

几个月前，姜瑞经介绍加入一个兼职群。经过简单培训，她成了一名“水军”。姜瑞说，主要工作内容是在微博宣传明星动态、影视作品，由派单人发送任务，群内的兼职“水军”抢单，随后在微博内发送撰写好的宣传文案。“只要有社交账号就能挣这个钱。”

据业内人士介绍，网络“水军”既有机器账号，也有真人账号。机器账号俗称“僵尸号”，主页通常都是批量的广告宣传，容易造成“一眼假”。而真人账号则因更为个性化的表达，在网络炒作中更受青睐。

广州某营销公司工作人员秦小燕（化名）告诉记者，一些“水军”公司披着公关公司的“马甲”，实则是几个人的“小作坊”，大量收集真人账号。由于雇佣专职“水军”成本高，他们瞄准了兼职群体。

“点个赞、发条评论就能有几毛到几元的收入。这种时间灵活、工作量不大的‘兼职’，对想赚点零花钱的年轻人很有吸引力。”暨南大学新闻与传播学院教授张潇潇说。

广州市民刘方方（化名）说，不少朋友都加入了兼职“水军”群。“起初是某个人在微博上看到招募。为了挣钱，我们几个人都跟着她进群当了‘水军’。”

记者在 QQ 上输入“推广”“数据维护”等关键词进行搜索，发现存在大量提供“水军”购买服务的 QQ 群，覆盖各种社交平台。

此外，据一名“水军”招募者透露，拉人头还可以提成。这种招募方式使兼职“水军”社群病毒式膨胀。

广州市白云区检察院第一检察部检察官肖雅菁介绍，购买“水军”服务的过程一般来说需要多层级流转，每一层级的获利都是赚取差价。做推广的多数兼职人员，位于这个灰色产业链的最底层。

张潇潇认为，“水军”在网络世界控制热搜、流量，炮制虚假舆论，轻则影响公众的判断、选择，重则损害他人权利、影响社会公平，危害严重。大家对此要有清醒认识，坚决拒绝以这种不正当方式获得报酬。

此外，法律界人士提醒，兼职“水军”还可能潜藏着法律风险。

肖雅菁表示，兼职“水军”如果发表不当言论，侵犯他人人身、财产权利，可能违反治安管理处罚法，情节严重的甚至可能触犯刑法，涉嫌的罪名包括网络型寻衅滋事罪、诽谤罪、故意传播虚假信息罪、非法利用信息网络罪等。如果作为组织者，组织、招揽其他人员散布虚假信息，同样可能涉嫌上述犯罪，且在共同犯罪中如果起到主要作用，则要被作为主犯处理。

多年来，“水军”如同网络空间的牛皮癣，长期存在却又难以根治。

秦小燕说，“水军”在一定程度上给平台带来了流量。为了热度，平台在监管方面有时“睁一只眼闭一只眼”。同时，兼职“水军”背后代表的是真人账号，相比机器账号而言，在监测层面具有一定难度，出现平台“不愿管”“不好管”的局面。

张潇潇认为，加强行业监管是斩断“水军”产业链的关键。在技术层面上，平台应当加强对异常转发、评论等网络活动的识别与监管。肖雅菁建议，加大对互联网公司的行政监管，落实互联网用户实名制。

受访专家表示，当前“水军”产业已经形成了完整的灰色乃至黑色产业链，但由于各个链条之间的联系并不紧密，在信息网络上将任务化整为零进行发布，由网络兼职人员去“认领”，这种跨地域性和分散性增加了打击难度。

肖雅菁表示，网民在网络中的身份虚拟性和主题的不确定性，也为“水军”提供了保护的外衣，导致发生网络“水军”案件时，监管部门确定行为主体具有一定的难度和不可控性。

“网络‘水军’活动的开展都是依靠网络平台进行，因此其发布信息和资金交易留下的都是电子证据。收集电子证据需要有很强的专业知识和技能，目前侦查机关或者相关监管部门与网络企业的信息共享机制有待健全，很难保证及时、高效、规范进行电子取证，影响了对‘水军’的查处。”肖雅菁说。

受访专家建议，进一步完善相关法律法规，提升相关部门对网络平台的监管能力，加大对“水军”的打击力度。对于涉嫌犯罪的网络“水军”，必须深挖产业链，斩断利益链条。“同时，还要加大网络权益的民法保障力度，对网络侵权行为，要加大赔偿处罚力度。”肖雅菁说。