也会捎带『暗祸』公共场所『明牌』

近期，境外一家购物中心的户外大型数字广告牌突然异常，连续数小时循环播放某已故知名政治活动家被篡改的、带有戏谑性和讽刺性的图片，引发业界对公共场所数字显示屏等公共数字设备潜在风险的重视。公共场所数字显示屏作为现代城市信息传播的重要载体，承担着信息发布、公益宣传、环境营造等多重功能，广泛应用于交通枢纽、商业中心、公共服务场所等人群密集区域。然而，随着互联网化、智能化程度不断提升，公共场所数字显示屏在带来便利的同时，也暴露出不容忽视的安全隐患。

公共场所数字显示屏的潜在隐患

形同虚设的“数字篱笆”。个别公共场所的数字显示屏在系统管理上存在一定薄弱环节，设备接入权限设置较为宽松，后台管理系统缺乏有效身份认证和访问控制机制，个别设备甚至长期使用默认账户和初始密码。加之设备与系统的更新维护不及时，导致系统漏洞未能得到及时修复，为不法分子提供了可乘之机。一旦攻击者通过远程或物理方式突破防线，便可随意更改显示内容，造成信息误导甚至公众恐慌。

层层传导的“链式风险”。公共场所数字显示屏通常依托自主建设的信息发布平台进行管理，若核心管理服务器存在安全隐患，一旦被攻破，可能引发“牵一发而动全身”的连锁反应，导致多个终端同步播放异常内容。此外，部分系统在数据传输过程中未采取加密措施，信息在传输链路中易被截获或篡改，进一步增加了安全风险，可能使得单点故障逐步演变为区域性、规模性安全事件。

监管缺位的“责任真空”。由于公共场所数字显示屏涉及建设、运营、内容发布等多个主体，管理职责分散，如存在日常巡检机制不健全、应急响应流程不明确等连锁问题，可能导致在异常事件发生时难以快速定位责任、及时处置。这种管理上的碎片化，为安全风险的滋生提供了土壤。

筑牢数字防护的“铜墙铁壁”

内容审核环节要“严把关”。应建立完善的内容发布审核机制，对拟投放信息进行政治性、合法性、社会影响性评估，杜绝发布含有虚假、误导、煽动性内容。可探索引入人工智能内容识别技术，提升审核效率与准确性。对于重大公共活动期间或重点区域的显示屏，应实施提级审核制度，确保信息内容安全可控。

系统管理环节要“扎篱笆”。加强对信息发布系统的安全防护，严格落实账户权限分级管理，定期更换密码，关闭非必要端口和服务。对系统进行常态化漏洞扫描与安全加固，及时消除已知风险。鼓励采用国产化软硬件产品，提升系统自主可控水平。

运行监测环节要“全天候”。建立公共场所数字显示屏运行状态的实时监测平台，对设备在线状态、内容播放记录、操作日志等进行集中管理，实现异常操作自动预警。明确管理责任主体，落实日常巡检制度，定期开展安全自查。制定完善应急预案，组织开展常态化应急演练，确保在发生入侵或内容异常时能够第一时间发现、报告、处置。

维护公共信息安全，确保城市窗口清朗人人有责。如发现公共场所数字显示屏播放内容异常、系统疑似被控等情况，可通过12339国家安全机关举报受理电话、网络举报受理平台（www.12339.gov.cn）、国家安全部微信公众号举报受理渠道或者直接向当地国家安全机关进行举报。

别让“隔空投送”变成“隔空投险”

不少用户的手机上都曾收到“XX想给你隔空投送一张照片”的请求提示，“隔空投送”作为日常分享文件、图片的快捷功能，为我们数据传输提供便利的同时，也可能被不法分子和别有用心之人盯上，给个人信息和国家安全带来风险隐患。

功能便捷 暗藏风险

“隔空投送”是基于蓝牙发现与Wi-Fi直连技术，实现设备间快速传输照片、视频等数据的系统功能。不法分子可能将设备设为“所有人可接收”模式，向周边用户肆意发送接收请求，用户一旦误点“接收”，不仅会收到不良信息，还将导致个人隐私数据泄露风险。攻击者还可能利用传输协议的漏洞远程操控用户设备，悄无声息地开启摄像头，若该漏洞被境外反华敌对势力利用并实施窃密，将直接威胁国家安全。

被用于制造恐慌

公开案例显示，有不法分子在公共场所使用“隔空投送”功能向人群随机投送低俗不良信息，造成公众恐慌，涉事人员均已被依法处置。

被用作传谣源头

公开案例显示，境内人员杨某某在留学期间被境外反华敌对势力拉拢，参与非法游行活动。在非法活动内部群聊中，杨某某提议利用Wi-Fi热点和“隔空投送”功能散布不良言论，意图扩大不良影响，后杨某某被依法处理。

被当成窃密通道

公开案例显示，多个境外反华敌对势力以免费提供设备、共享信息为诱饵，招募境内人员非法采集敏感数据，而具有隐蔽性的“隔空投送”，正是这类窃密行为的“帮凶”。

维护国家安全 筑牢信息防线

筑牢国家安全防线，需从规范信息功能的使用、警惕泄密风险做起。

严控接收权限

严禁通过互联网、无线网络等非涉密渠道传输处理涉密信息，建议将个人电子设备的接收范围设置为“仅联系人”或直接关闭相关功能。

拒收陌生投送

对来源不明的投送请求，尤其是包含“内部文件”等诱导性标题的，应一律拒绝，以防恶意程序植入或信息泄露。

及时更新系统

建议从官方应用商店等渠道安装软件，定期更新手机系统，修补安全漏洞，加强设备防护，降低被技术攻击的风险。

广大人民群众如发现利用“隔空投送”等功能进行窃密或传播敏感内容的行为，可通过12339国家安全机关举报受理电话、网络举报受理平台、国家安全部微信公众号举报受理渠道或者直接向当地国家安全机关进行举报。

（均转自国家安全部微信公号）

“老地图”引发新问题

涉密地图涵盖敏感地理数据、军事设施分布、关键基础设施坐标等重要信息，一旦泄露可能危害国家安全。近期，国家安全机关查获多起违规使用涉密地图的典型案件。

“老地图”失泄密敲响警钟

国家安全机关工作发现，王某在某二手交易平台上公开售卖标注有“秘密”“机密”字样的上世纪六七十年代测绘部门印制地图。经相关部门鉴定，这些“老地图”未履行解密程序，不得向社会公开，更不能进行售卖，王某被依法追究责任。

某科研院所研究员李某长期从事地质勘探工作，掌握了许多涉密地图资源，他错误地认为“老地图”不再涉密，遂利用职务之便私自将大量涉密“老地图”储存在个人电脑和移动硬盘中，甚至几年内多次通过网络进行传输，造成严重失泄密隐患，李某被依法追究责任。

涉密地图使用管理需牢记三大准则

依规申请，保持警惕。法人或其他组织因合法目的需要使用属于国家秘密的涉密基础测绘成果时，应当向有关主管部门提出申请。审批通过后，由测绘成果保管单位提供。对网络上、市面中流通的所谓“内部地图”“已销密地图”应保持高度警惕，购买、索要、接受有可能构成违法。

合规使用，严禁扩散。涉密地图的使用必须严格控制在获批的特定目的、范围和人员之内。严禁任何未经批准的复制、扫描、非涉密信息系统传输涉密地图的行为；严禁将涉密地图用于公开发表、展览、教学等场景。

保管严密，责任到人。涉密地图须指定专人负责，建立台账，动态掌握载体动向。存储必须使用符合国家保密标准的密码柜或保密室，确保物理隔离。最终销毁必须按照规定程序，严禁作为普通废品处置或私自留存。

国家安全机关提示

那些看似陈旧的地图无声地承载着过往的记忆与家国的烙印。它们不仅是纸张上的线条与标注，更可能是一段秘密信息的留存。广大人民群众应保持清醒的认识：维护国家安全无小事，亦无“过期”之说。在日常生活中，若接触到来源不明、标注可疑的地图，或发现有违规售卖、传递涉密地图等可疑线索，请通过12339国家安全机关举报受理电话、网络举报受理平台、国家安全部微信公众号举报受理渠道或者直接向当地国家安全机关进行举报。

责任编辑/王睿卿 E-mail:fzbfyzk@126.com