守护口岸上的国家安全

国门枢纽，八方交汇。口岸是国家对外开放的门户，是对外交往和经贸合作的桥梁。在全球化纵深发展的今天，这些承载着人员互通、物流交汇、信息交融的通道枢纽，也面临着新挑战，需要你我共同守护。

一次快门定格的安全危机

作为陆海空多维交汇的枢纽，口岸承载着国门边防、军事保障、能源运输等多重安全职能。但个别人员不了解相关规定，违规记录口岸内的边防布局、军民两用设施参数等敏感情况，对国家安全造成潜在隐患。某公司宣传部门员工在未履行审批报备程序的情况下，私自携带无人机进入某口岸限定区域拟实施航拍作业，意图拍摄一段航拍视频用作宣传素材，被有关部门依法及时制止。执法人员当即对其开展法律科普并进行批评教育。国家安全机关提示，口岸限定区域涉及国家安全事项，不得随意拍摄。

一颗水果带来的安全风险

生物安全是国家总体安全的重要组成部分和重要保障。口岸查验是防范外来物种入侵的第一道防线，一只异宠、一片贝壳、一粒种子的非法入境，都可能对我国物种资源、生态系统、农业生产乃至人民群众生命财产安全造成风险隐患。某旅客违规夹带一批未经申报的水果入境，被有关执法部门截获。经检测，该批水果中存在桔小实蝇幼虫。该虫又被称为“水果杀手”，繁殖能力极强，一经扩散可能造成大量作物减产。《生物安全法》规定，境外组织或者个人通过运输、邮寄、携带危险生物因子入境或者以其他方式危害我国生物安全的，依法追究法律责任，并可以采取其他必要措施。国家安全机关提示，入境人员应主动配合执法部门开展检疫查验，严禁私自携带寄递生鲜果蔬、活体宠物、境外土壤等相关检疫物品入境。

一纸文件引发的安全隐患

我国法律对国家秘密载体出境事项有着严格的管理规定。私自携带涉密文件出境，将带来失泄密风险隐患。某涉密单位工作人员高某拟赴境外执行公务，违规携带1份秘密级文件出境，被有关执法部门截获。经查，高某确因境外业务需要携带该文件出境，但未按规定办理涉密载体出境许可手续。事件发生后，高某所在单位给予其行政记过处分。《保守国家秘密法》规定，寄递、托运国家秘密载体出境，或者未经有关主管部门批准，携带、传递国家秘密载体出境的，根据情节轻重，依法给予处分；有违法所得的，没收违法所得。

国家安全机关提示，涉密单位人员要增强保密意识，严守保密法律法规，未经批准严禁携带国家秘密载体出境。维护国家安全是每个公民的责任与义务，口岸上的安全没有“旁观者”，我们都是防线上的“守护者”。公民如发现违规拍摄敏感设施、携带可疑物品和其他危害国家安全等行为，可通过12339国家安全机关举报受理电话或网络举报平台举报。

不可随意、不可轻信、不可大意！

近年来，境外间谍情报机关对我实施网络攻击窃密愈演愈烈，各种手段层出不穷，对我国家安全构成威胁，需引起警惕。

随意存密引“毒患”

某国家级重点实验室工作人员王某，为了盲目追求工作的方便快捷，故意绕开审批监管手续，在其个人联网计算机内违规存储了1000余份涉密文件和敏感资料。某天王某收到一封主题为“会议通知”的电子邮件，邀其参加所属研究领域一场学术会议。王某未作甄别就直接下载并阅读了该邮件附件，导致计算机被境外间谍情报机关植入特种木马程序，并被秘密控制长达三个月。王某个人计算机内违规存储的文件资料全部被窃取，造成重大失泄密事件。

轻信“官邮”陷圈套

一天，某机关单位办公邮箱收到一封标题为“××规划〔20××〕××号（以此为准）”的钓鱼邮件。工作人员小张误以为是官方邮件，未严格遵守工作规定，在来源不明的情况下随意打开并点击了邮件内的“官方链接”。该页面立即跳转到某钓鱼网站，随即该单位办公邮箱的密码和邮件内容被境外间谍情报机关获取，造成该单位相关敏感数据泄露。

大意疏防“门洞”开

境外间谍情报机关试图利用境内个别OA系统漏洞，对我党政机关、科研院所、重点企业和关键基础设施实施网络攻击。国家安全机关工作掌握，某科研单位使用的OA系统由于长期未进行漏洞修补和杀毒软件更新，导致服务器被境外黑客攻击并植入木马病毒，最终造成该单位重要数据被窃取倒卖。

国家安全机关提示

莫让国家秘密“裸奔”。《中华人民共和国保守国家秘密法》规定：任何组织和个人不得使用非涉密信息系统、非涉密信息设备存储或者处理国家秘密。广大公民尤其是涉密单位工作人员，务必严守保密纪律，切勿使用非涉密信息系统、非涉密信息设备处理、存储任何涉及国家秘密或敏感信息的数据，不给境外间谍情报机关可乘之机。

莫让指尖的贸然一动成为泄密的导火索。机关、团体、企业事业组织和其他社会组织应当落实反间谍安全防范主体责任，开展反间谍安全防范教育、培训，提高本单位人员的安全防范意识和应对能力。对来源不明的邮件、链接等，广大公民尤其是党政机关、涉密单位工作人员，要提高安全防范意识，核实其来源，判断是否可靠，不可轻易点击陌生邮件、链接和下载未知软件等，以防境外间谍情报机关借此植入木马病毒，导致敏感信息被窃取。

莫让网络威胁乘虚而入。关键信息基础设施运营者应采取反间谍技术安全防范措施，防范、制止境外网络攻击、网络入侵、网络窃密等间谍行为，保障网络和信息核心技术、关键基础设施和重要领域信息系统及数据的安全。安全防护软件是计算机信息设备的重要防线，它能够实时监测并拦截病毒、木马等恶意程序，防止其窃取信息，并通过监控网络流量，识别并阻止可疑传输，对异常操作行为进行预警，有效预防网络窃密。一旦安全软件未及时更新，计算机将面临安全风险，成为攻击者窃密的渠道。

从源头管控涉密文件才安全

涉密文件任何环节疏忽大意都容易产生失泄密问题，必须坚持全周期管理理念，从源头治理形成全过程闭环控制。相较于涉密文件的收发、传递、使用、保存、销毁等环节，源头制作上的安全管控更容易被忽视，出现失泄密隐患。

设备混用引危机。文件制作过程中可能使用到的打印机、复印机、扫描仪，通常情况均带有存储固件或模块，在使用过程中，会保存处理过的信息。一旦在涉密和非涉密计算机之间共用，就相当于破坏了涉密计算机的物理隔离，会将处理过的涉密信息“摆渡”至非涉密计算机上，造成失泄密隐患。

硒鼓留存有风险。硒鼓是打印机的核心部件之一，用于接收激光扫描组块发射的激光图像数据，通过静电高压的配合，将需制作的图文资料转移到纸上，实现打印输出。硒鼓内置的芯片可被改造用于存储打印过的信息，未妥善处置管理，可能会造成失泄密。

随意外印犯大忌。相关法律规定，除在机关、单位内部印制涉密文件外，还可以选择保密行政管理部门审查批准的定点单位印制。但实际操作过程中，极个别单位和人员，心存侥幸、贪图方便，将涉密文件、敏感资料就近送往自以为熟悉不会出问题的文印店印制，甚至在印制过程中未予以全程监督、及时清理文件资料，造成失泄密事件。

管理不严有隐患。个别机关、单位工作人员由于缺乏保密知识和敌情意识，存在随意摆放涉密文件、没有及时登记销毁印制废页、无关人员在场时依然印制涉密文件或文件制作期间擅自离开等情况，造成失泄密隐患。

国家安全机关提示

制作场所要安全。涉密文件制作场所要符合保密要求，一般来讲应在单位内部具有安全保密措施的环境内开展涉密文件制作，如确需外送，应选择有国家秘密载体印制资质单位，与其签订保密协议并监督执行。

制作设备要留意。涉密打印机、复印机、扫描仪等涉密文件制作可能用到的信息设备在投入使用前，应进行必要的保密技术检测。

制作人员需可靠。涉密文件的制作人员应为涉密人员，符合涉密人员基本条件并通过保密检查、签订保密承诺书，明确保密责任，接受单位保密部门监督。

制作流程需严密。涉密文件制作应当使用涉密计算机和涉密设备，禁止使用非涉密计算机和设备起草、制作涉密电子文档，禁止使用低密级的涉密计算机和设备起草、制作高密级电子文档，并严格按照批准的数量制作，对制作产生的废稿、废页应当及时登记销毁。国家安全一切为了人民，一切依靠人民。广大单位及相关人员在日常制作涉密文件时，要严守安全底线，强化保密意识，提升保密素质，时刻绷紧安全弦。

（均转自国家安全部微信公号）

责任编辑/王睿卿 E-mail:fzbfyzk@126.com