

国安部：党政军核心部位成窃密重点，安全防线如何筑牢？

近年来，随着信息技术深度渗透国家治理与军事运作，党政军核心部位的安全防护面临前所未有的挑战。国家安全机关多次通报，境外情报机构将我国党政军关键部门列为窃密重点目标，手段从传统间谍活动演变为网络攻击、社交工程、内部人员策反等复合型渗透。这些核心区域一旦失守，可能直接威胁国家主权、安全与发展利益。面对这一现实，如何识别风险、防范漏洞、构建纵深防御体系，已成为各单位必须直面的课题。

核心部位为何成为窃密主攻方向？

党政军核心部位掌握着国家重大决策信息、战略部署数据和敏感通信资源，其价值远超一般行政或商业机密。例如，国防动员计划、重大基础设施布局、高层人事调整等信息，一旦泄露，可能被敌对势力用于精准打击或舆论操控。更值得关注的是，这类机构往往存在“信息孤岛”现象——各部门系统独立运行，数据共享机制不健全，反而为跨系统渗透提供了可乘之机。此外，部分岗位人员长期接触高密级信息，若缺乏持续性保密教育，极易成为外部势力拉拢的目标。

常见窃密手法与隐蔽特征

当前窃密行为已高度技术化与伪装化。最典型的包括：利用伪造的公务邮件诱导内部人员点击恶意链接；通过社交媒体建立信任关系后实施心理诱导；在办公设备中植入微型无线传输装置，实现远程数据外泄。值得注意的是，许多攻击并非来自外部黑客，而是源于内部人员的疏忽或主动违规。比如，使用个人手机拍摄涉密文件、在非加密网络上传递敏感资料、随意连接公共充电设备等，都可能造成信息泄露。这些行为往往发生在日常操作中，难以被常规审计发现。

防范措施需从制度到习惯全面升级

防范窃密不能仅依赖技术防火墙，更需构建“人防+技防+制防”三位一体的管理体系。首先，应严格执行分级分类管理制度，明确每份文件的访问权限与流转路径，杜绝越权操作。其次，定期开展实战化保密演练，模拟钓鱼邮件、社交诱骗等场景，提升全员风险意识。再次，强化终端安全管理，禁止非授权设备接入内网，对移动存储介质实行实名登记与加密管控。最后，建立内部监督与举报机制，鼓励员工主动报告可疑行为，形成“人人有责、人人尽责”的安全文化。

安全误区与真实应对建议

不少人误以为只要不主动“泄密”就等于安全，这种认知存在严重偏差。事实上，一个看似无害的操作——如在微信群转发一张带水印的会议照片——也可能构成信息泄露链条。另一个常见误区是过度依赖技术防护，忽视人员管理。再先进的加密系统，若被内部人员滥用或遗忘密码，同样形同虚设。因此，真正的安全在于细节把控：每次登录前确认身份、每次外发前核对接收方、每次设备交接时进行清查。这些习惯虽小，却是抵御风险的第一道屏障。

> 常见问题

> 问：普通工作人员是否也属于窃密目标？

> 答：是的。即使非核心岗位，只要接触过敏感信息片段，仍可能被用于拼凑关键情报。

>

> 问：使用加密软件就能确保安全吗？

> 答：加密只是手段之一，若密钥管理不当或设备被物理劫持，仍可能失效。

>

> 问：内部人员违规是否一定构成犯罪？

> 答：根据情节轻重，可能涉及行政处分、纪律处理甚至刑事责任，具体依《保守国家秘密法》判定。