

近年来，境外间谍情报机关对我开展渗透窃密活动愈发活跃，他们将我公职人员作为重点围猎的目标，精心布局，因人下套。个别公职人员因立场信念缺失、纪律观念弱化、规矩意识松懈等原因，引发失泄密恶果，既折损个人前程，更对国家安全和利益造成危害。

密防弛懈 亲属勾连的泄密暗流

张某大学毕业入职某基层单位，凭工作实绩 28 岁晋升部门副职，是当时最年轻的中层干部。仕途顺遂中，张某保密意识渐趋松弛，工作与保密纪律双重失守。某次会议领取 3 份涉密文件后，张某未依规送回单位妥善保管，竟将密件带回家中。回家后，张某在与亲属李某交谈时，擅自披露文件内容并允许其浏览，李某趁机偷拍并将密件信息传输至境外，造成恶劣影响。经查，李某受境外间谍情报机关指使，长期蛰伏伺机窃取我涉密文件，最终李某以为境外非法提供国家秘密罪被依法追究刑事责任；张某受党纪处分、被调离岗位。

赌债噬志 利益驱动的窃密交易

某市直机关干部侯某，在某届足球世界杯期间，以消遣心态涉足网络博彩，但贪念作祟，由小额投注滑向巨资豪赌，最终债台高筑，积蓄尽失。为填补赌债窟窿，竟将黑手伸向工作接触的涉密文件，主动联络境外间谍情报机关，利用职务便利多次偷拍涉密资料并传至境外，非法牟利 7 万余元。最终，侯某以为境外非法提供国家秘密罪被依法追究刑事责任。

色诱钳制 胁迫下的叛国迷途

某省直机关工作人员李某，因

工作需要，赴境外参加短期培训。其间，李某禁不住境外间谍情报机关人员的美色诱惑，陷入其精心设计的“温柔陷阱”。

事后，境外间谍情报机关以李某私密照片为要挟，胁迫其加入境外间谍组织，李某迫于无奈履行了参谍手续。回国后，李某抱有侥幸心理，并未向组织汇报自己被胁迫参加境外间谍组织的事情，更是在后续工作中多次将工作文件转交给境外间谍情报机关。最终，李某以间谍罪被判处有期徒刑 5 年，剥夺政治权利 3 年。

国家安全机关提示

从上述案件不难看出，失泄密事件往往藏匿于工作生活的细枝末节，如果理想信念不够坚定、纪律规矩意识不强，很可能被干扰、受影响、遭裹挟，最终陷入境外间谍情报机关设计的犯罪深渊。广大公民特别是公职人员要心有所畏、行有所止，始终绷紧保密之弦，用实际行动守护国家安全。

亲情有度。广大公民特别是公职人员要严守保密纪律规矩，非涉密场所不谈论涉密事项，遵循“亲属不透露，亲友不接触”的铁则，警惕“亲情牌”背后的境外渗透，同时强化家庭保密教育提醒，督促家人自觉树立保密观念、遵守保密要求，敏感事项不打听、不议论、不外传。

癖习无染。广大公民特别是公职人员应培养健康良好的兴趣爱好，牢固树立正确的金钱观和价值观，始终保持清醒头脑，自觉抵御不良诱惑，坚决摒弃“以密谋财”的错

严防间谍渗透 重点群体更要

误观念，深刻认识到任何对涉密信息的牟利企图，都将付出沉重代价，既断送个人前程，更损害国家利益。

回头是岸。如一时行差踏错，应及时悬崖勒马。如发现自己在境外遭遇拉拢策反、胁迫诱骗，应保持冷静，在确保自身安全的前提下及时举报反映，积极寻求派驻单位或驻外机构的保护和帮助。根据《中华人民共和国反间谍法》第五十五条规定，在境外受胁迫或者受诱骗参加间谍组织、敌对组织，从事危害中华人民共和国国家安全的活动，及时向中华人民共和国驻外机构如实说明情况，或者入境后直接或者通过所在单位及时向国家安全机关如实说明情况，并有悔改表现的，可以不予追究。

广大公民应增强国家安全意识，如发现可疑线索请及时通过 12339 国家安全机关举报受理电话、网络举报平台（www.12339.gov.cn）、国家安全部微信公众号举报受理渠道或直接向当地国家安全机关进行举报，共同筑起维护国家安全的钢铁长城。

小心网络广播里的声波毒蛊

“系统告警！境外某不明 IP 正伪装成普通用户登录我辖区某中学的网络广播系统，企图入侵攻击并篡改播报内容。”干警小李紧盯屏幕前不断涌现变动的数据，皱起眉头……“立即锁定，阻断链路！”干警老张指着屏幕，准备迎接一场硬仗。某市国家安全局的办公室内，一场网络安全保卫战正在打响。

抽丝剥茧明真相

攻击者是谁？他们是如何突破防护网入侵的？国家安全机关立即对该中学互联网平台及网络广播系统全面缜密分析检查。分析发现，对手利用境外网络为跳板，以海量数据为掩护躲避追踪，与之前发现的某境外反华敌对组织手法十分相似。该组织长期运用网络对我境内多个校园网络广播开展大面积、高频次网络攻击，企图破解校园网页及内设广播系统的口令密码，远程操控校园广播、传播有害言论。

此次遭到攻击的学校，因网络广播系统直接搭载在校园公开网页上，登录密码简单设置为一串相连的数字，给了敌人可乘之机。国家安全机关当即指导该学校的相关管理部门进行整改，从源头切断境外入侵渠道，及时消除了危害。

多措并举防风险

国家机关、人民团体、企业事业组织和其他社会组织承担本单位反间谍安全防范工作的主体责任，落实反间谍安全防范措施，对本单位的人员进行维护国家安全的教育，动员、组织本单位的人员防范、制止间谍行为。应建立防火墙和加密认证系统，关闭非必要端口，提升密码强度，修复安全漏洞，监测运行状态，定期升级系统，做好必要的网络安全技术防护，确保网络广播系统安全稳定运行。要积极开展网络安全宣传，提高广大网民抵御不良信息、错误言论的意识和能力。

商用密码：守护数字安全的关键力量

商用密码为守护国家安全、社会秩序与公民隐私发挥重要作用。《商用密码管理条例》为商用密码使用管理提供法治保障。

铸就数字时代安全盾牌

“商用密码”是指采用特定变换的方法对不属于国家秘密的信息等进行加密保护、安全认证的技术、产品和服务。在数字主权时代，商用密码以“技术盾牌”之姿构建起维护国家安全的三重防护体系：数据安全的“加密铠甲”。针对政务、金融等敏感信息，商用密码以动态加密算法将存储数据转为密文“掩体”，传输中以安全协议

构建“加密隧道”，全流程阻断信息泄露风险，让数据流转更安全。

网络空间的“免疫屏障”。对关键基础设施的网络攻击，商用密码以数字签名、区块链认证等技术构建“智能门禁”，精准识别合法设备，实时数据校验模块毫秒级拦截篡改，守护网络安全。

产业安全的“自主引擎”。我国已实现商用密码全产业链国产化，自主研发的密码算法安全性获国际认证，打破技术垄断，助力我国在数字经济竞争中掌握主动权。

夯实国家安全法治根基

新修订的《商用密码管理条例》

从多个层面，为商用密码在维护国家安全中的应用提供坚实法律支撑。

《条例》新增“进出口”章节，对技术实施清单管理，严格把控关键密码技术跨境流动，维护国家核心利益。

《条例》“应用促进”章节在鼓励合规使用商用密码的同时，严厉打击利用其从事危害国家安全等违法犯罪活动，避免密码技术被恶意利用。

《条例》与《网络安全法》《国家安全法》等法律衔接，要求关键设施运营者采购密码产品需通过国家安全审查并定期评估，实现全链条监管。

国家安全机关提示

商用密码在维护国家安全中发

挥着不可替代的关键作用。用好商用密码，维护国家安全，需要多方协同发力共筑安全防线。

严格技术标准。严格遵循国家标准与行业规范进行商用密码生产，探索加强密码研发，确保算法和产品自主可控，杜绝安全漏洞。

规范密码管理。健全商用密码使用管理制度，规范密钥管理流程，加强内部人员培训，定期维护升级密码系统，提升密码安全应用能力。

增强防护意识。主动学习商用密码安全知识，增强安全防范意识，妥善保管个人密码信息，切勿登录存在数字证书风险提示的网站；严格遵守相关法律法规，发现安全隐患及时上报。（均转自国家安全部微信公众号）