近期，国家安全机关破获一起重大间谍案件。经查，犯罪嫌疑人郝某受境外间谍情报机关指挥，长期潜伏在我核心要害部门窃取情报，最终因间谍罪被判处无期徒刑。

海归博士被判无期 长期潜伏窃取情报

资料照片

潜伏我要害部门窃取情报 郝某被判无期

学成归国的郝某按照外方要求，想方设法应聘进入了我中央某部直属研究所，成为我重点涉密单位的正式工作人员。在研究所工作期间，郝某多次与外国间谍人员秘密接头，把自己搜集到的情报提供给外方，然后收取间谍经费。

警示三：境外间谍情报机关及其代理人始终紧盯我核心要害部门，大肆对我重点领域开展情报渗透窃密活动，严重威胁我国家安全和发展利益。

在境外间谍情报机关指挥下，处心积虑一心想获取更多情报的郝某，被借调到中央某部工作，负责一项重要涉密工程。就这样，一枚境外间谍情报机关的钉子深深扎进了我核心要害部门。

经鉴定，郝某向境外间谍情报机关提供的情报，涉及中央某部敏感项目及内部人员情况，其中机密级国家秘密5项、秘密级国家秘密2项，刑法第一百一十一条规定的情报14项。最终，郝某因间谍罪被判处无期徒刑，剥夺政治权利终身。

国家安全机关提示

发现间谍行为拨打12339

哪些是间谍行为？

间谍组织及其代理人和其他境外机构实施或指使、资助他人实施危害中国国家安全的活动；

境内外机构、组织、个人与间谍组织相勾结实施危害中国国家安全的活动；

接受间谍组织及其代理人任务；

参加间谍组织；

窃取、刺探、收买或者非法提供国家秘密或者情报；

策动、引诱、收买国家工作人员叛变；

为敌人指示攻击目标；

进行其他间谍活动。

哪些人更应警惕被策反利用？

留学、高校师生、军事发烧友、军工企业、国防科研单位人员、年轻网友等。

据国家安全机关统计，以上人员容易被境外间谍机构策反，可能会被利用。

发现间谍怎么办？

拨打举报电话：12339

举报网站：www.12339.gov.cn

公民举报间谍行为，起到重要作用的，将给予重金奖励。

（来源：央视网、国家安全部、央视新闻）

留学攻读博士期间 遇到“好心人”

留学生郝某在攻读博士学位期间，因赴某国参加国际学术会议，来到该国大使馆办理签证，使馆人员表示要对其申请进行审核。事后不久，一位名为T的使馆官员主动致电郝某，热情地表示，希望就签证事宜与其当面沟通。

这位名叫T的使馆官员正是某国间谍情报机关派驻在使馆的工作人员，面对涉世未深的郝某，T知道他的目标来了。

见面后，T详细了解郝某的个人信息、研究内容、就业打算等情况，表示愿意为郝某提供签证帮助，想和郝某交个朋友。郝某以为自己遇到了好心人，当即表示愿意和T交朋友，双方互留联系方式。就在这一刻，郝某已经被境外间谍情报机关所套路，一步步走向外方设定的圈套。

警示一：境外间谍情报机关长期觊觎我留学人员群体，并利用签证环节物色有价值的目标对象，主动进行贴靠。以签证官身份出现的情报人员，对于涉世未深的年轻学生而言，具有很强的欺骗性。

此后一段时间，T通过请客吃饭、赠送礼物等方式，逐步与郝某密切关系，还善解人意地提出在国外留学读书开销很大，可为郝某提供一份兼职工作。

在T的安排下，郝某参加了一次“工作面试”，并很快凭借自己撰写的两篇论文得到了不错的报酬，这让他对T更加信任。

又过了几个月，T热心介绍自己的同事L，与即将完成学业的郝某认识。在郝某毕业回国前，L亮明了自己间谍的身份，将郝某策反，双方正式建立秘密情报关系。

警示二：国家安全机关掌握，请客吃饭、邀请旅游、赠送礼品、提供兼职等都是境外间谍情报机关人员拉拢我留学人员的常用手段。待关系密切、时机成熟就会实施策反。

智能家居便利 安全意识牢记

随着人工智能和物联网技术的普及，智能门锁、扫地机器人、智能全屋温控等智能家居逐渐普及，已经融入现代社会工作生活的方方面面，显著地提升了人们的生活质量。值得注意的是，智能家居产品的敏感数据若被别有用心之人利用，可能造成信息泄露，对国家安全构成威胁。

“无声的监听者”

智能音箱设备如被别有用心人员或组织恶意植入木马程序，可能绕开使用授权和监管要求，在未被唤醒状态下记录用户语音，并将非法收集获取的用户数据上传至云端存储。不法分子可能会通过远程操控，持续记录用户日常对话内容，侵犯个人隐私，让家里的智能音箱变成“无声的监听者”。这种智能音箱设备一旦被放置在涉密敏感场所，并被境外间谍情报机关操控掌握，很有可能于无形中泄露国家秘密。

“暗中的窥探者”

智能摄像头如在云端视频加密、用户身份验证、密码设置等方面技术防范不到位，则有可能被不法分子通过技术手段获取摄像头的控制权，进而导致用户信息或视频内容泄露，甚至在不知不觉中进行实时监控。如果安装在涉密敏感场所的视频采集设备存在安全漏洞并接入互联网，将造成失泄密风险。

“隐形的潜入者”

智能门锁可通过密码、生物特征识别或手机APP控制开关，人们不再需要随身携带钥匙，为工作生活提供了极大便利。但个别劣质智能门锁因存在设计缺陷，攻击者可以通过简单的工具在几秒钟内将其破解并打开。如果这类智能门锁设备被用于保护涉密场所，一旦不法分子通过网络攻击或物理手段将其破解，就能在敏感区域“畅行无阻”，对国家安全造成威胁。

国家安全机关提示

身处万物互联时代，我们在享受智能家居给工作生活带来便利的同时，也要提高防范意识，树牢保密观念，不给境外间谍情报机关通过智能家居设备漏洞危害我国家安全的可乘之机。

注意挑选合规设备

在购买智能家居设备时，注意选择正规品牌、通过正当渠道，优先挑选通过国家安全认证（如CCC标志）或符合国际安全标准的产品。

妥善设置隐私权限。

在使用智能家居设备时，应为智能家居设置保密性较高的强密码，关闭非必要的收集和共享个人信息的权限及远程控制功能，及时安装官方补丁修补设备漏洞。

了解掌握安防知识

在使用智能家居设备时，要自觉提高学习意识和风险意识，持续关注最新数字安全风险和防御策略，主动学习如何识别数据信息泄露、恶意钓鱼攻击等常见的数字安全威胁场景，积极向家庭成员、身边朋友普及如何安全使用智能家居设备的知识，尽可能地规避相关风险。家居智能化是科技改变生活的潮流，是人类生活便利化的途径。过好生活，也应过安全的好生活。广大人民群众在尽享智能家居产品带来便利时，也要提高智能家居产品使用的安全意识，尤其要避免将不符合保密要求的智能设备应用于涉密敏感场所，共同筑牢维护国家安全的人民防线。（来源：国家安全部）

责任编辑/王睿卿 E-mail:fzbfyzk@126.com