跨境卖惨终成空

“画面要暴力血腥”“要动感，要抓拍”“效果要‘惨’”……这不是片场，而是境外反华组织精心策划的一场“政治避难”闹剧。近日，国家安全机关破获了一起境内人员在反华组织教唆下，伪造“受迫害”材料，损害我国家利益的案件。

“精心”准备的剧本

张某早年因企业经营不善背负债务，便萌生赴境外务工的想法。然而，出国后的情况与张某的设想天差地别。因其不具备合法身份，时刻面临着被遣返的风险，高昂的生活成本和缺乏保障的工作境况使得张某难以立足。就在张某走投无路时，某境外反华组织伸出“援手”，教唆张某编造所谓在境内“受迫害”的故事，承诺张某可通过“政治庇护”获得合法居留身份。在该组织的安排下，张某选择铤而走险，并多次参加在我驻外使领馆前的反华活动。

为提高“受迫害”的真实性，该反华组织成员递给他一份精心准备的剧本，要求他拍摄影像资料。张某随即与境内亲属金某联系，表达其需要相关“佐证材料”。金某明知此行为违法，但在张某利诱下，组织两名人员假扮警察，前往张某父母家中伪造现场，拍摄数张所谓“警察暴力执法”的照片，并发送给张某。然而，境外反华组织在收到照片后，未履行对张某的所谓“承诺”，张某个人境况仍未改变。

确凿的违法事实

国家安全机关掌握情况后，依法对涉案人员开展行政执法工作。起初金某对个人违法行为避重就轻，意图蒙混过关，但在我国家安全机关严格规范的执法、扎实完善的证据面前，其放弃侥幸心理，如实供述了违法活动事实。该案中，张某为一己之利，参加境外反华活动，抹黑祖国，为反华势力提供煽宣“弹药”，但最终竹篮打水一场空。金某在明知张某要求违法的情况下，仍组织人员伪造相关材料。上述人员的行为不仅触犯国家相关法律，更损害我国家形象，危害我国家利益。

国家安全机关提示

《中华人民共和国反间谍法》第七条规定，中华人民共和国公民有维护国家的安全、荣誉和利益的义务，不得有危害国家的安全、荣誉和利益的行为。

《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。

广大公民应擦亮双眼，保持警惕，如遇境外反华组织诱骗欺诈等可疑情况，可通过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者直接向当地国家安全机关进行举报。

涉密学术研究 谨防别有用心之人

在科研创新与学术交流日益频繁的当下，涉密学术研究已成为国家安全的重要内容。涉密学术写作、交流、合作有哪些泄密风险点？

泄密风险点有哪些？

信息设备隐患。电脑编辑写作、网络查阅传输、手机沟通联络是学术写作绕不开的路径，但涉密信息与非涉密信息转换，涉密设备与非涉密设备传输时，若操作不当可能存在泄密风险。特别是使用未做防护的联接互联网设备处理、拷贝涉密信息时，就有可能给境外间谍情报机关留下窃密之机。

违规发布泄密。工作发现，个别研究人员保密意识缺失，为提高论文采用率，在论文中违规引用未公开的内部数据甚至是涉密资料，且相关责任单位未严格履行保密审查相关程序，导致涉密论文被公开收录至互联网学术期刊检索系统，为境外间谍情报机关通过公开渠道开展情报搜集，窃取到我学术科研领域国家秘密提供便利。

虚假合作陷阱。学术合作是推动学术进步的重要方式，但涉密学术项目的合作需慎之又慎。个别境外间谍情报机关可能会伪装成科研机构或高新企业，抛出看似诱人的合作项目，要求参与方提供涉密研究数据、技术方案等。一旦轻信此类虚假合作，不仅会导致学术成果泄密，还可能使整个科研项目陷入被动，给国家安全造成威胁。

国家安全机关提示

学术写作、交流与合作不仅是学术成果的展现，更是维护国家安全的重要组成部分。高校师生、专家学者以及相关研究人员在公开发表论文和报告、开展学术交流与合作时，应树牢保密意识，严守保密底线，让间谍窃密无处遁形，共同构筑起坚不可摧的学术保密防线。

严格设备使用。进行涉密学术写作时，务必使用经过保密部门检测认证的专用电脑及存储设备，并确保设备处于安全的工作环境中。定期对设备进行杀毒、系统更新，及时修补漏洞。严禁将涉密文件存储在个人云盘、共享文件夹等公共空间，拷贝文件时使用单位配发的加密U盘，杜绝电子设备泄密风险。

强化保密意识。主动学习《中华人民共和国保守国家秘密法》等法律法规，积极参加单位组织的国家安全教育和保密教育，掌握了解反间防谍知识，增强国家安全意识，提升国家安全素养。无论是在国内外杂志、期刊公开发表论文著述等，还是在国内外学术活动公开交流论文观点，都应根据有关规定严格履行保密审查程序，确保文章内容不涉及国家秘密、工作秘密和内部敏感信息。

谨慎开展合作。开展学术合作特别是与国(境)外机构或人员合作时，应对合作项目认真评估，把好立项关，将保密审查作为必经程序。对涉及国家秘密的项目，应尽量避免由外方承担或参与合作。确需由外方承担或参与合作的，应当按照国家有关法律法规，报主管部门批准后方可实施，不得擅自将涉密项目发包给外国组织或个人，也不得擅自与外国组织或个人开展涉及国家秘密的科研合作。

广大公民和有关单位应自觉提高防范意识，履行保密安全义务，做好日常防护。若发现可疑线索，应第一时间通过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。

旧手机 换菜刀行不行？

安全处置守护“数字身家”

“旧手机、旧电脑换菜刀、换不锈钢盆！”这与时俱进又略带夸张的吆喝，您是否也曾听过？一些闲置的“电子家当”，很多朋友会考虑出手置换，主打一个该省省该花花。那么，其中的风险隐患您又是否了解？

通讯录记录着社交网络，聊天记录关联着亲朋好友，相册存储着私密瞬间，浏览记录承载着兴趣偏好，地图定位描绘着出行轨迹……一部经久使用的智能手机，就像一个浓缩的数字人生档案袋，如果随意交出，其中蕴含的信息安全风险便悄然升级。

账户信息遭窃。旧手机中存储的个人身份信息、关联的银行账户、使用的支付或登录密码一旦被不法分子通过技术手段恢复获取，可能危及个人隐私、财产安全。

隐私数据丢失。旧手机存储的个人社交账号、活动轨迹、生理数据等，若未经妥善处理，存在被不法分子用于分析机主个人特征、社交关系、行为习惯及活动轨迹的风险，可能衍生出诈骗、身份盗用等问题。

工作信息泄露。旧手机中可能存储工作邮件、会议记录、客户资料等敏感数据，如这些信息被不法分子恢复，可能导致工作信息泄露，给单位和个人造成损失。更有甚者，如手机曾接入单位内网，不法分子可能利用其残留的网络配置信息（如VPN设置），作为入侵企业核心系统的通道。

此外，旧手机中未退出的云端账号还可能成为黑客攻击的突破口。如手机曾绑定过智能家居，黑客甚至可能远程操控家中智能设备窃听窃视。

国家安全机关提示

简单恢复出厂设置还不足以彻底清除旧手机中的个人信息，专业的数据恢复技术能轻易击破这层屏障，回收流向的不确定性也让这些敏感数据面临更大的安全风险。对于个人而言，可以从以下几方面保护自己的“数字家当”：

彻底清除数据。先退出手机上的所有应用程序（尤其是支付、社交媒体、邮箱等含重要数据的APP）账户登录状态；关闭手机自带的“查找设备”功能，防止追踪定位；最后再恢复出厂设置，覆盖旧数据痕迹。

销毁关键硬件。处置设备前，务必取出手机内的SIM卡和存储卡，并自行保管或剪毁，或确保其在正规机构处置流程中被粉碎处理，杜绝后患。

正规渠道回收。将淘汰的手机交予资质齐全的回收机构，优先选择手机品牌官方以旧换新计划、大型电商平台的回收服务或具有国家认证资质的专业电子废弃物回收处理企业。

培养保密意识。在日常生活中，避免在手机中存储身份证或银行卡照片、密码明文等敏感信息；如确需在手机内存储，务必使用可靠加密软件或设备自带的保险箱功能；及时删除不再需要和含有个人信息的文件或图片。

（均转自国家安全部微信公号）

责任编辑/王睿卿 E-mail:fzbfyzk@126.com