留学生被间谍策反

真实案例细节披露

张某，某境外高校毕业生，因在境外学习期间被境外间谍情报机关拉拢策反，从事间谍活动，被依法处理。

以为是“伯乐”，背地下“毒手”

2006年，因高考失利，在苦读一年语言预科之后，张某以优异的成绩进入了某国排名前列的高校。因为成绩出色，张某成为了班长，负责联系该校的中国留学生，并且得到了该校校领导凯迪的“赏识”，担任其中文老师，两人也因此成了“忘年交”。

然而，就是这个“忘年交”，一步步地把张某推向了境外间谍情报机关精心设计的陷阱，使他深陷其中，不能自拔……

一天，正在读大三的张某被凯迪叫到办公室，凯迪向张某热情介绍了两个外国人，并称张某是自己的学生，学业表现非常出色，一定可以“帮助”他们做事。于是自称埃克森、伊森的两个外国人与张某交换了联系方式，并在之后的日子里请张某帮忙提供该校中国留学生的情况，还答应给予张某丰厚报酬。随着交流联系的深入，他们对张某的要求也越来越多，索要的信息也越来越敏感。

一次，二人向张某提出需求时，直接向其亮明了该国间谍情报机关工作人员的身份，并以张某之前提供的敏感信息为威胁，要求张某加入该国间谍情报机关。在金钱利诱和威胁下，涉世未深的张某沦为了帮助他们窃密和监视中国留学生的“提线木偶”。

以为是“救星”，其实是“灾星”

接下来的时间里，张某浑浑噩噩地一边读书、一边定期向该国间谍情报机关提供他们想掌握的情况，逐渐放下了“心理包袱”。

临近毕业时，许多国内科研院校赴该国开展招聘或者组织交流活动。由于善于交际且外语能力突出，张某频繁与这些机构接触，自己也有了回国就业的想法。但因为张某无法达到这些科研院校要求的“所有课程成绩必须为A”基本要求，难以实现回国工作的目标。就在此时，凯迪再次找到了张某，告诉张某自己不仅可以帮助他更改成绩单，甚至还可以写一封推荐信，让张某得到进入国内某科研院所工作的机会。作为交换，张某要在回国以后继续配合完成埃克森、伊森的任务。

面对利益的诱惑，张某最终选择了服从，彻底坠入犯罪的深渊。

以为是“帮助”，其实是“陷阱”

在对方的“帮助”下，张某回国后如愿进入某科研院所工作。但在自身侥幸心理和境外间谍情报机构威逼利诱下，张某并未第一时间向国家安全机关报告，仍然继续为境外间谍情报机关工作。因资历尚浅，接触到的技术资料和涉密文件无法满足对方变本加厉的“需求”，在境外间谍情报机关的指导下，张某成为了所里的“热心人”。

同事小李急着下班，张某就“热心”地帮他收整桌面，待确认小李走后，张某立即打开小李电脑，窃取其涉密文档；同事老王有涉密资料需要销毁，张某就“热心”地帮助他整理盘点，并在过程中偷偷将境外间谍情报机关“感兴趣”的文件私藏起来……这些涉密资料最终都落入了境外间谍情报机关的手中，造成了我国科研数据的泄露。

天网恢恢，疏而不漏。国家安全机关经缜密侦查，及时锁定了张某的违法犯罪活动，并对其依法实施审查。最终，张某受到了法律严惩。

国家安全机关提示

本案中，在境外间谍情报机关感情拉拢、金钱引诱、控制胁迫下，张某一步步行差踏错，迷失自我，最终走上违法犯罪的道路，白白葬送了自己的大好前程和美好青春。

在境外留学、出访、旅游等期间，要牢固树立国家安全意识和反间防谍意识，及时发现各种别有用心的“热络”背后的阴谋。面对境外间谍情报机关的各种拉拢策反活动，要把牢防线、守住底线，严防掉入境外间谍情报机关预设的陷阱。

《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。（该案例根据真实案件改编，文中人物均为化名）

是如何有机可乘的？『网络间谍』

当前，网络空间已经成为境外间谍情报机关对我国开展间谍活动的重要阵地。国家安全机关工作发现，近年来，境外“网络间谍”利用我重要单位安全防范不到位、工作疏忽、贪图便利等机会，持续通过各种方式，攻击我境内重点要害单位、部门、企业的信息化系统，并建立隐蔽传输通道，持续窃取我重要敏感数据，危害我国数据安全、网络安全。

网络漏洞被“遗漏”

境外“网络间谍”常用各种网络测绘平台，对已经曝光的网络漏洞进行扫描，一旦发现重要单位未及时修补漏洞，便会立即开展针对性攻击窃取数据。近期，国家安全机关工作发现，某军民融合企业包括办公平台在内的多个系统，因软件更新不及时，存在高危安全漏洞，导致“门洞大开”。该企业漏洞被境外“网络间谍”发现，并利用漏洞入侵、植入木马病毒，窃取了企业重要生产业务数据及客户信息，对我军事装备技术发展造成危害，进而威胁我军事安全和科技安全。

运维厂家遇“合围”

国家安全机关工作发现，境外“网络间谍”高度关注“软件供应链”企业，企图通过钓鱼邮件等方式，持续不断地攻击相关企业，并把掌握系统管理权限的运维人员作为攻击窃密的首选目标。

小李是某邮件系统厂家运维人员，具备远程管理账号和系统管理员账号权限，负责为客户的邮件系统提供技术支持。为了贪图便利，小李经常在电脑上记录甲方客户的账号密码和系统管理员账号密码。境外“网络间谍”利用开源情报信息提前锁定了小李运维人员身份，并对小李的电脑进行了网络攻击，窃取了其电脑中的客户账号密码表，进而通过网络跳板，对上千家重点要害单位邮件系统实施窃密。由于小李掌握的是管理员级别的账号密码，境外“网络间谍”获取了大量重点要害单位内部邮件数据，造成了严重的现实危害。

测试设备遭“不测”

近期，某具有较好网络安全防护能力和安全防护措施的大型国有企业莫名存在加密流量在凌晨传输到境外，且每次发往不同IP地址的可疑情况。国家安全机关经缜密侦查证实，境外“网络间谍”以该公司网络出口设备、内网闲置设备为跳板，层层渗透到该公司核心内网，持续窃取该企业重要数据。

经分析发现，此前该企业在测试某网络系统时，布设了一台测试设备，并放开了该测试设备的各类权限。测试结束后，设备未及时下线。境外“网络间谍”正是发现了这一“可趁之机”，以其作为跳板，通过内网渗透，发起网络攻击，并成功窃取该企业核心基础数据，造成我国重要民生基础数据被窃取。

国家安全机关提示

根据《反间谍法》《网络安全法》《数据安全法》等有关规定，间谍组织及其代理人实施或者指使、资助他人实施，或者境内外机构、组织、个人与其相勾结实施针对国家机关、涉密单位或者关键信息基础设施等的网络攻击、侵入、干扰、控制、破坏等活动属于网络间谍行为。公民和组织应当与国家安全机关共同做好针对网络间谍的安全防范和调查处置工作，针对发现的疑似网络间谍行为，应当及时向国家安全机关报告。

反间谍安全防范重点单位应当加强对涉密事项、场所、载体等的日常安全防范管理，采取隔离加固、封闭管理、设置警戒等反间谍物理防范措施；应当按照反间谍技术防范的要求和标准，采取相应的技术措施和其他必要措施，加强对要害部门部位、网络设施、信息系统的反间谍技术防范。

《反间谍法》第三十六条规定，情况紧急，不立即采取措施将对国家安全造成严重危害的，由国家安全机关责令有关单位修复漏洞、停止相关传输、暂停相关服务，并通报有关部门。

《网络安全法》第二十二条规定，网络产品、服务的提供者应当为其产品、服务持续提供安全维护。发现其网络产品、服务存在安全缺陷、漏洞等风险时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。

（均转自国家安全部微信公众号）

责任编辑/王睿卿 E-mail:fzbfzyk@126.com