责任编辑:陈烽 邮箱:179652384@qq.com

随着我国综合国力不断增强,境外间谍情报机关在我国密集展开行动,搜集我国政治、经济、军事、科技等方面的重要核心机密,对我国公民的渗透策反也出现了一些新方法、新手段。随着此类案件的披露,相关情况进入公众视线。

境外黑手伸进军工单位,策反手段多种多样

近期,针对境外间谍情报机关围绕我国国防军工领域实施情报窃密活动,四川省国家安全机关展开了代号为“扫雷”的专项行动,一举抓获四名涉嫌危害国家安全的人员。

这四人互相并不相识,其中有两位还是90后,外方人员以经济利益为诱饵,通过网络进行搭讪渗透,最后成功策反 。业内人士提醒,境外间谍人员对我国公民的渗透策反堪称无孔不入、无所不在,每个公民都应该提高防范意识,共同维护国家安全。

“兼职”高薪诱惑 “境外采访人员”网购资料

四川某国防军工单位热表车间的90后青年文某平常没事会玩手机QQ,2014年10月某一天在QQ“附近的人”一栏中突然弹出了一名网友“H”,资料显示“附近单位职工需要兼职的请联系我”。

在文某表明自己是国防军工单位员工的身份后,“H”自称是境外某报社的记者,希望文某能提供工作中接触到的内部资料,并承诺每月支付3200元的报酬。在经济利益的驱使下,文某先后多次向H提供了所在单位生产军品的型号、月产量、使用的特殊材料等涉密信息。

同样是90后的王某,在这家国防单位的技术部门任职,父母都是国家公职人员,因对现有的工资待遇不满,王某在网上寻求兼职时结识了“H”,“H”的QQ签名为“兼职赚外快,待遇优,非直销,诚信至上”。而王某被兼职每月3、4千元的收入冲昏了头脑,认为提供的单位动态情况只要不属于涉密信息,就可以打打擦边球,于是频频为对方提供军品设计定型情况、样品编号、试验时间节点、出现故障情况等信息。

就这样,两位90后为境外机构做起了“兼职”,实际上是在提供涉密信息。

“猎头公司”百万年薪诱惑 成境外间谍发展目标

有人提供消息,也有人犹豫不决,但却也留下巨大隐患。2014年,参加工作近10年的吴某有了离职的想法,他在某招聘网站上投放简历,并留下了联系电话。工作履历一栏中,表明“有某国防军工单位的工作经历”。不久,吴某收到了某“猎头公司顾问”发来的电子邮件,要求吴某提供工作证明,以便求职。吴某将自己与单位签订的劳动合同,以及印有自己照片、所在部门、姓名的工作证件,扫描后发送至对方邮箱。

很快,对方通知吴某被聘用,工作内容就是提供所在国防军工单位尚未公开的内部信息,年薪高达50至120万元。面对如此丰厚的报酬,吴某虽然动了心,但结合曾在单位接受的保密教育及自身认识,意识到对方可能是境外间谍人员。

吴某摇摆不定的态度,也使其成为境外间谍情报机构发展的重点目标,留下了巨大安全隐患。

“境外航天迷”寻找目标 推荐朋友被策反

上述三人都是自己出问题,还有的是将朋友推荐给境外机构,导致被策反,这样自己也就成了帮凶。2013年年初,在某国防军工单位技术部门供职的李某接到亲戚电话,称一境外朋友“S”想了解一些航空航天方面的知识,有着保密意识的李某婉言拒绝了,但在亲戚多次劝说下,李某还是与“S”建立了联系。

“S”以公司做市场调查准备进军航空航天领域为由,要求李某利用工作之便搜集关于航空航天方面的期刊、杂志、论文等资料。由于单位内部资料管理较严,李某多次借阅资料未果,没能如期完成“S”交待的任务。为顾及情面,李某向“S”推荐了在某航空航天大学读研究生的同学程某,导致程某被策反,李某也因此成为境外间谍情报机关的帮凶。

境外谍报人员通过网络 行搭讪渗透

从上述的这几个案例可以看出,境外间谍情报机关在策反我国公民时已表现出一些新手段和新手法,比如他们会通过论坛、求职网站、社交平台等,将ID虚设到我国重点单位附近,以虚设的单位或个人身份,主动寻找有国防军工单位背景的人员,以拉拢感情、利益诱惑等手段套取国家机密。或者发布虚假岗位信息,预留QQ、微信等联系方式,守株待兔等待我国公民主动联系,建立所谓的聘用关系,从一开始搜集公开信息逐步发展到搜集、报送重点单位内部资料,从而达到窃密的目的。而在这四起破获的案件中,有三起都是通过网络来策反嫌疑人的。

除了利用网络外,境外间谍情报机关还会指使被策反人员,提供可能被利用人员的联系方式,物色新的被策反人员,以此扩大关系网,拓宽信息渠道。在这四起案件中,李某没能完成境外间谍情报机关交给的任务,随后又推荐了自己的朋友,结果导致朋友被策反。

被策反人员呈现“年轻化”趋势

境外间谍机构充分利用网络是一方面,在策划对象方面,也呈现出年轻化的趋势。在近期四川省国家安全机关抓获的四名涉嫌危害国家安全的人员当中,有两人就是90后。

其实,境外间谍情报机关策反的人员涵盖各行各业、各个年龄阶段,但目前80、90后成为我国网民的主体,由于涉世不深、防范意识薄弱等因素,被境外间谍情报机关策反利用的案件呈逐年上升的趋势。因此,强化对这个群体的安全防范教育显得尤其重要。

(据央视新闻)

军事情报都是如何被泄露的?

综合一些案例可以发现,在新时期的情报战中,网络和社交软件已经成了泄密的主要方式。

案例一:间谍收买“的哥”,QQ收集情报

今年3月份,据河南电视台报道,河南省首次公布一起间谍案。开封市一名的哥段某,跟境外间谍在QQ上认识,后者以请段某兼职的名义,让段某获取军事情报,并通过互联网发往境外。自2013年7月起,段某先后收到境外支付的酬金共4万余元。

开封市国安局干警表示,段某发往境外的信息包括部队大型的调动情况,如出了多少军车、启动了多少飞机架次,以及部队平常的训练强度和规模、军事演习的强度和规模等情况,“这就涉及了部队非常核心的动向信息。”

案例二:混入军属微信群,打听内部情况

据《解放军报》4月6日报道,军队家属的微信群,也成为间谍刺探情报的一个新手段。

3月上旬以来,第20集团军某旅官兵家属打开微信,都能收到提示信息——“姐妹们,保密无小事,军嫂也有责,当心‘第三只眼’盯上您……”

原来,随着该旅野外驻训、国际维和、军事演习等各项工作相继展开,家属们在日常聊天中常常会交流一些信息,包括部队什么时候走、去哪里、去多久等。

有段时间,微信群里还经常有陌生人打听部队内部情况。了解情况后,网络保密监督员将陌生人踢出了微信群,并将有关线索报给旅保卫部门,防止了泄密事件发生。

案例三:网上论坛“钓鱼”军迷泄密

据《解放军报》3月份的报道,不少军迷在网络上的论坛发帖,同样是网络泄密的一个隐患。

文章中列举了军迷泄密的几种方式。比如,为了增加帖子的“分量”,有的军迷不惜翻墙越障、草地潜伏,偷拍军事装备的“靓照”。

此外,一些间谍通过在论坛里“钓鱼”窃取情报。窃密者有意抛出错误言论,如故意将某些武器的性能参数说错,引得“资深军迷”给出“靠谱”答案,套出更多有价值的信息,更有甚者遭到“利”诱,充当了境外情报机构的“马前卒”。

(据《新京报》)

如何提高防泄密意识?

很多人可能会觉得自己的工作与机密无关,因此无须防范,但实际上境外间谍情报机关瞄准的,不仅仅是国防军工单位的核心技术人员,任何外围人员乃至每一个公民都有可能在不知情的情况下被利用。我国宪法和相关法律都规定,公民有维护国家安全的义务。作为普通公民应该如何提高防范意识,共同维护国家安全呢?

四川大学法学院教授魏东表示,在现代社会,国家的安全是一体的、多方位的,该自己说的才能说,不该自己说的不能说。尤其是涉及到重要工作的岗位,比如国防科工委、军工企业的相关工作人员,都要有防范意识,要遵守保密制度、防范制度。在人与人的交往中,尤其是与一些具有境外背景因素的人交往时要多一根弦。

另外,公民的职业道德修养不仅关系到个人的发展,也关系到国家安全,树立正确的人生观、价值观是加强职业道德修养的前提。赚钱应当通过合法、正当渠道获取,天上不会掉馅饼,切莫为了蝇头小利而出卖国家机密。对于亲戚朋友提出的帮忙请求,切莫麻痹大意,要分清亲情与法理。

如果公民意识到或者发现自身行为涉嫌危害国家安全利益,要及时向国家安全机关投案自首,将危害减小到最低程度。我国《反间谍法》规定:实施间谍行为,有自首或者立功表现的,可以从轻、减轻或者免除处罚;有重大立功表现的,给予奖励。千万不要有侥幸心理,要牢记:天网恢恢,疏而不漏,心存侥幸,必入法网。

(据央视新闻)