

在光影交织的叙事长河中，隐蔽战线题材影视剧始终是一个特殊的存在。它将镜头聚焦于没有硝烟的战场，对准那些献身于阴影中的无名英雄，以悬疑迭起的剧情和血肉丰满的角色，让观众在屏息凝神的反转中感受激烈的无声较量，以艺术化表达揭开“间谍可能就在身边”的残酷真相，对“国家安全无小事”展开直观深刻的诠释，警醒我们绷紧心中的安全之弦，点燃维护国家安全的使命炬火。本期起，本版回顾那些优秀的隐蔽战线题材影视剧，感受神秘、神奇、神圣的隐蔽战线，敬请关注。

和平年代，在社会的隐秘角落，无声的战争仍在悄然上演。谍战电视剧《对手》，以其独特的视角和深刻的主题，将这场没有硝烟的战争呈现在观众面前，让我们深刻认识到国家安全的重要性以及每个人在维护国家安全中的责任与使命。

智斗狡猾对手 深挖潜藏暗线

18 年前，因执行任务失败，境外间谍李唐和丁美兮不得已假扮夫妻，继续在大陆潜伏。李唐以出租车司机的身份穿梭在街头巷尾，方便对外联络，执行任务，丁美兮以中学教师身份为掩护，时常色诱目标人物，获取情报。十多年的潜伏生涯，两人早已疲惫不堪，也曾想过自首，却因种种原因不得继续执行上线的各种任务。面对训练有素，又潜伏大陆 18 年之久、对大陆情况无比熟悉的台湾间谍，厦门市国家安全局专案组组长段迎九带领组员迎难而上，凭借高超的侦察技术和丰富的反间谍经验，历经艰难险阻，最终将这对外谍夫妇绳之以法，展现了国家安全机关人民警察全力以赴投身维护国家安全事

业，以生命赴使命，以热血铸忠诚的感人故事。

警惕身边间谍 防止渗透破坏

《对手》突破了传统谍战剧的制作模式，以当代都市为背景，创造性地以间谍视角，从日常琐碎生活作为切入点，让“反间谍”概念进入人们的日常生活，以更强烈的感染力警示观众增强国家安全意识。剧中台湾间谍李唐和丁美兮“一地鸡毛”的中年危机式间谍设定，打破了观众既往通过影视剧作对间谍的固有认知，让观众意识到间谍并非遥不可及，神秘陌生的存在，可能就是潜伏在身边的普通人，他们利用寻常身份作为掩护，在市井中搜集情报、传递信息，于阴暗处潜伏窥视、伺机渗透破坏，妄图损害我国国家安全。随着剧情的

《对手》：反间谍 共筑国家安全钢铁长城

深入，境外间谍的手段更加层出不穷，这也彰显了当前反间谍工作面临更加严峻复杂的斗争形势。剧中，李唐和丁美兮及其他台谍以威逼利诱、美色诱惑等各种方式，对涉及多个领域的各色人物开展策反、窃密活动。

事实上，近年来，境外间谍情报机关对我渗透窃密愈发活跃，各类间谍情报活动的主体更加复杂，手法更加隐蔽、目标更加多元、领域更加广泛，对我国家安全构成威胁。国家安全机关工作发现，境外间谍情报机关将我党政机关、国防军工、科研机构、高等院校及我驻外机构人员视为重点关注对象，且近年来更逐渐将目光投向我青年群体。他们假借交流调研、咨询服务、兼职招聘等理由，主动贴靠，通过感情拉拢、攀拉利诱，甚至栽赃胁迫等卑劣手段，开展情报搜集活动，危害我国国家安全。

依靠人民力量 共筑钢铁长城

《对手》不仅展现了国安干警的英勇与担当，更强调了全民参与在维护国家安全中的重要性。面对艰巨复杂的反间谍形势，不仅要靠专门机关，更需要依靠人民力量。剧中，12339 国家安全机关举报受理电话反复出现，在广告牌、海报和剧情演绎中给观众留下了深刻印象，为观众介绍了参与反间谍斗争的有效途径，提升了广大人民群众维护国家安全的参与感、获得感。国家安全的根基在人民、力量在人民。人民的认同和支持是维护国家安全的不竭动力。为进一步动员全社会力量共同维护国家安全，国家安全部颁布实施的《公民举报危害国家安全行为奖励办法》对公民举报奖励工作进行了全面规范，以法治思维和法治方式加强正面引导，强化奖励激励，充分发挥法治固根本、稳预期、利长远的作用，提升举报奖励工作专业化法治化水平。国家安全机关将在党中央的坚强领导下，深入学习贯彻习近平法治思想，坚持总体国家安全观，发挥职能优势，汇聚起全社会维护国家安全的强大合力，同人民群众一道构筑起反间谍的钢铁长城。

警惕扫描成泄密“推手”

在数字化浪潮时代，扫描类软件凭借高效的文字识别和图文转换功能，成为办公和生活场景的快捷助手，给我们带来诸多便利。然而在日常使用中，个别人员由于保密意识缺乏、风险感知不足，使得这一快捷助手变成了泄露国家秘密、突破保密防线的“推手”。

近期某机关工作人员因贪图便利，违规使用互联网扫描软件扫描涉密会议纪要，使该文件被自动备份至网盘。但其网盘账号密码遭暴力破解，使得攻击者获取了其在 3 年间扫描的 127 份涉密文件，后泄露文件经境外社交媒体传播，造成重大失泄密事件，对我国家安全构成现实威胁。

潜在隐患需留意

传输路径未设防

目前市面上大部分的扫描类软件和程序基于开发公司提供的云端数据库对用户提供的文件进行识别和分析。这也就意味着在扫描软件

运行、处理和反馈的多个阶段中，文件内容将数次在互联网上进行传递，如不慎将涉密敏感内容扫描上传，将为不法分子窃取个人隐私、甚至国家秘密提供可乘之机。

权限索取超常规

个别扫描软件在安装时，会申请超出正常扫描需求的权限，如获取麦克风、通讯录、相册、短信记录等权限。一旦用户轻易授权，软件便可获取设备内的各类信息，可能会导致设备中储存的身份信息、账户数据等重要信息数据被窃取。

云端存储有漏洞

不少扫描软件提供云端存储功能，云存储的安全性主要取决于其加密技术、访问控制以及服务商的安全措施。但在实际应用中，这些技术手段难以达到绝对的完善。一旦账号被破解或服务商自身存在系统漏洞，又或者遭受境外间谍情报机关的攻击，均可能导致存储在云端的信息泄露或被恶意利用。

恶意软件巧伪装

有案例显示，个别伪装成扫描

软件的恶意程序存在于部分非官方应用市场或网站，用户一旦下载安装，它们便在设备后台悄然运行，自动扫描并窃取设备内的信息数据。

提高警惕筑防线

国家安全无小事，保密没有“局外人”，广大人民群众，特别是涉密岗位工作人员，要切实提高安全意识，自觉规范软件应用使用行为，做好信息安全防护。

严格落实保密规定

时刻牢记“涉密不上网、上网不涉密”，严禁通过任何互联网渠道传输、保存或处理涉密资料。严禁使用联网扫描软件扫描识别涉密信息，不能以方便工作为由将涉密文件在线上储存。

谨慎选择扫描软件

尽量从官方应用商店下载经过安全认证的扫描软件，以降低下载到恶意软件的风险。在下载前，可通过查看软件的用户评价和开发者信息，了解其信誉度和安全性。

严格管控软件权限

在安装扫描软件时，仔细查看软件申请的权限列表。只授予软件运行所必需的权限，警惕应用软件敏感和超范围权限请求，定期检查已安装软件的权限设置，及时关闭过度授予的软件使用权限。

加强数据存储安全

慎重选择服务商提供的照片、通讯录等信息自动备份到云端功能。在将数据进行云端存储之前，可通过专业软件对数据进行加密，或者使用网盘自带的加密功能，直接在上传文件时选择加密选项。对于需要共享的文件，建议在分享前启用“提取码”功能，并关闭其余操作权限，避免过度共享导致数据泄露。扫描软件的泄密风险不容小觑。我们务必擦亮双眼、提高警惕，时刻防范隐藏在扫描软件背后的泄密风险，严格保护信息安全。在这场没有硝烟的信息安全战中，每个人都是防线，让我们携手共进，守护国家与个人的信息安全，绝不让扫描软件成为失泄密的“帮凶”。（均转自国家安全部微信公众号）