

盛夏时节，蝉鸣声声，又到了一年一度的高校毕业季。答辩冲刺、论文定稿、材料归档、离校手续、求职签约……各项事务接踵而至。对于即将毕业的涉密研究生而言，临近毕业，虽然忙碌，但安全保密不能松懈。一旦发生失泄密事件，不仅影响个人前途，还有可能损害国家安全和利益。

《涉密研究生与涉密学位论文管理办法》规定，涉密研究生是指直接参与涉及国家秘密的教学、科研项目、任务等工作或者在教学、科研过程中接触、知悉、产生和处理较多国家秘密事项的在读研究生。在毕业季，希望广大涉密研究生们做到：忙而不乱、繁而不疏，学业圆满收官，保密万无一失。

别让科研心血“付诸东流”

毕业论文、研究课题、实验数据等学术成果，往往是境外间谍情报机关长期觊觎的目标。私自拷贝留存涉密资料、随意丢弃科研底稿等行为可能造成难以挽回的损失。

把好审查关。涉密学位论文公开发表前须严格依规完成保密审核与脱密处理，绝不随意简化程序，绝不擅自公开发布。

把好清理关。涉密资料、存储介质、实验数据等载体要按规移交或销毁，不能私自“留存备用”，防止留下失泄密隐患。

别让青春记忆“藏有秘密”

在涉密实验室随手拍下一张照片，发朋友圈时不慎开启精准定位，随口说出所参与项目的敏感数据，随便透露自己即将入职某个涉密单位……这些言行都有可能被别有用心之人捕捉、拼凑，甚至让自己沦为境外间谍情报机关精准围猎的对象。

守好发布关。不在各类涉密管控区域拍照打卡、发布定位，不上

传包含敏感场所、涉密内容的图文影像。

守好交际关。社交时把握言语尺度，不透露在读期间接触的涉密研究内容和入职涉密岗位情况，不打探他人涉密相关信息。

别让职业起点“因小失大”

实习离岗交接、求职面试应答、入职岗位适应，是学子奔赴职场的必经之路。身份转变的同时，保密责任不应该缺位。面试中为凸显个人能力泄露原单位内部信息，入职初期因规章不熟随意传播工作内容……这些潜在的泄密风险，不仅会让自己触碰保密红线、承担相应责任，还有可能造成工作秘密甚至国家秘密外泄。

把好交接关。实习离岗时全面清理个人办公设备与电子账号，将所有工作文件、技术资料、涉密载体按规移交。

把好求职关。不因求职心切逾越保密纪律边界，投递简历和作品集前做好脱密处理，不将涉密项目作为求职“敲门砖”；入职前主动研习保密法规与岗位制度，筑牢从业保密根基。

这个群体要注意 又是一年毕业季

国家安全机关提示

少年负壮气，奋楫启新程。研究生求学之路，是学识积累的过程，也是锤炼、担当的过程。保密工作没有“毕业季”，安全要求没有“过渡期”。希望大家常怀敬畏之心，严守保密纪律，筑牢安全防线。如发现任何危害国家安全行为的可疑线索，请通过12339国家安全机关举报电话、网络举报受理平台（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。（摘自6月27日微信公众号“国家安全部”）

游戏数据岂能用于军事目的

近期，有外媒披露，某知名手游旗下人工智能公司获取了游戏用户上传的近300亿份环境扫描数据，可能将这些数据用于训练能识别和理解物理空间的人工智能模型。由于该人工智能公司与某国军工企业有合作关系，相关模型可能被用于军事目的。该报道引起了全世界对“民用数据军事化应用”的担忧，也为数智时代的数据安全问题再次敲响了警钟。

看不见的“扫描仪”

AR（增强现实）技术，通过将虚拟信息叠加到真实场景中，可以让用户获得虚实融合的交互体验。上文提到的游戏名义上是依托AR实景交互的“增强现实互动”，实质上则是诱导玩家完成精确的三维点云扫描，实时采集地理信息数据。

采集维度远超常规拍照

AR技术可一并捕捉视觉纹理、空间深度及物体尺寸，甚至能复现局部三维空间，采集信息量远超普通照片。

采集过程极具隐蔽性

安装软件时，面对内容繁琐的使用协议，用户往往会选择“一键同意”，不细看就授予软件诸多重要权限。相关软件会持续采集信息并实时上传，而用户却难以察觉数据的具体流向。

坐标绑定精度超乎想象

每一帧AR画面都强制捆绑高精度GPS坐标、海拔高度、设备朝向等信息。这枚“时空胶囊”式的数据结构，能精准复现拍摄者的行动轨迹与观察视角，为后续分析提供绝对基准。

擦亮双眼，筑牢防线

近年来，国家有关部门不断加强监管，在测绘准入、数据出境等关键环节严把关口，防范化解了一系列风险隐患。维护地理空间数据安全既离不开政府部门的依法履职，也离不开每一位用户的支持参与。

权限管理“小气”一点

安装地图、AR类软件时，遵循“最小必要”原则，非必要不授予“始终定位”和“相机/相册”权限。应用闲置时，及时关闭进程，阻断后台静默运行。

敏感区域“谨慎”一点

在军事管理区、军工单位、港口码头、通信枢纽、科研院所等敏感区域，不拍摄、不扫描、不打卡。如发现某款应用的“热门打卡点”异常集中于涉密区域，应提高警惕。

可疑任务“多想”一点

谨慎对待境外机构或不明平台以“调研”“游戏测试”等名义发布的数据采集任务。涉及拍摄街景、测绘地形、记录人流量等兼职，可能是非法测绘的幌子，切勿因小利而忽视地理信息安全。

“我能把你亲属招进国安局”

近期，国家安全机关会同有关部门破获一起冒用国家安全机关工作人员身份招摇撞骗的案件。涉案人员姚某因犯招摇撞骗罪，被依法判处有期徒刑两年，缓刑两年。

姚某好逸恶劳，为了骗取钱财心生冒充国家机关工作人员的恶念。他认为，国家安全机关是涉密单位，工作人员身份不易被核实，遂将自己伪装成“国家安全部工作人员”，并在常住地附近租下一间办公室作为窝点，散播可以“安排工作”“解决问题”等消息。姚某还通过街边“办证广告”联系不法商家，伪造公章，并购买大量制服式服装，伪装警察身份。

2024年年末，姚某与社会人员孙某结识，谎称具备将孙某亲属招录进国家安全机关工作的能力，并通过出示伪造的国家安全机关文件增强其言辞的可信度。孙某信以

为真，向姚某支付了4.6万元好处费。2025年年初，姚某向孙某亲属发送虚假短信，制造“录用”假象，并向孙某交付盖有伪造印章的“录取通知书”。此后，孙某请托之事再无进展。

姚某迟迟不能兑现承诺，让孙某对姚某的身份产生了怀疑，遂拨打了12339国家安全机关举报电话进行了举报。国家安全机关受理举报后，查明姚某招摇撞骗情况属实，立即会同有关部门对其采取刑事强制措施。经审讯，姚某如实供述了自己编造“国家安全部工作人员”身份骗取钱财的经过。最终，姚某因犯招摇撞骗罪，被依法判处有期徒刑两年，缓刑两年。

国家安全机关提示

《刑法》规定，冒充国家机关

工作人员招摇撞骗的，处三年以下有期徒刑、拘役、管制或者剥夺政治权利；情节严重的，处三年以上十年以下有期徒刑。冒充人民警察招摇撞骗的，依照前款规定从重处罚。

国家安全机关开展人员招录、执法办案、宣传教育等工作，均有严格的制度规定和纪律要求，任何打着国家安全机关旗号“展示涉密文件”“承诺帮忙安排工作”的行为均是不法分子设下的圈套。广大人民群众如果发现冒充国家安全机关工作人员招摇撞骗的问题线索，可通过12339国家安全机关举报电话、网络举报受理平台（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。

（摘自6月24日微信公众号“国家安全部”）

（摘自6月29日微信公众号“国家安全部”）