南京航空航天大学保密宣传教育参考资料

（2020 年第 1 季度）

参考学时：2 小时

（一）以案说法

谨防“节假日泄密”

国之利器，以安为先。在工作中，少数涉密人员把保密当作“松紧带”，在节假日的节骨眼泄了劲、破了功，导致“节假日泄密”现象时有发生。近期国家统一发布了几例在节假日期间的失泄密案件，从时间节点可分为了“节前、节中、节后”三种情况，供大家学习。

一、节前泄密案件

案例 1:为抢时间，疏忽大意

2013 年 12 月 31 日，某县单位收到两份机密级通知，局长黄某批示“转发各单位”。该局指挥中心主任王某考虑到临近元旦，书面印制已来不及，难以发放到位，且其当日还需陪同领导视察，便安排副科长钱某通过网站挂发。钱某为方便各县级单位查阅使用，擅自扫描，发布到部门门户网站上，造成泄密。案件发生后，有关部门给予王某党内严重警告;给予钱某党内警告、撤销副科长职务处分;给予黄某行政记过处分。

案例 2:加班干活，带密回家

2016 年 4 月底，某部委下属事业单位工作人员朱某拟利用“五一”假期核对文件，从涉密计算机中将电子稿刻成光盘擅自带回家，存储到家用笔记本计算机中。工作完成后，朱某忘记从计算机中删除。9 月初，朱某家人将计算机送给其刚上大学的表弟唐某使用。唐某重装操作系统，并将期中的文档(包括上述文件)发送至朱某所用互联网电子邮箱，造成泄密。案件发生后，有关部门给予朱某行政警告处分，责令作出深刻书面检查，在单位内部通报批评。

二、节中泄密案件

案例 3:违规操作，网上办公

2013 年 1 月 30 日，某市单位收到 1 份秘密级通知，该单位副主任纪某安排工作人员吴某起草转发通知(未标密)，将上述秘密级通知作为附件。2 月 11 日，某县单位收到通知后。当时正值春节，办公室主任张某考虑到已通知各个下属单位，假期工作全在网上安排，就让网站值班员罗某扫描文件，通过内部 OA 系统转发，造成泄密。案件发生后，有关部门给予张某严重警告处分;对纪某、吴某、罗某进行通报批评，责令作出深刻检查。

案例 4:分内之事，委托他人

2012 年“五一”期间，某市单位机要员严某按工作习惯，电话通知业务处处长刘某领取 1 份秘密级密码电报。当时刘某在家休息，未看到文件原文，便电话安排工作人员强某领取并办理。强某擅自遮去电报报头与密级标识，扫描后通过内部 OA 系统转发，造成泄密。案件发生后，有关部门给予强某行政警告处分，责令作出书面检查，取消年度评优资格;给予刘某行政警告处分;责令严某及办公室主任郭某作出书面检查，取消当年评优资格。

三、节后泄密案件

案例 5:节前工作，抛之脑后

2012 年 12 月 31 日，某涉密单位办公室机要秘书章某到当地市委办公室，领回两份秘密级文件。2013 年 1 月 4 日，元旦假期结束，章某返回单位上班，但忘记了曾在节前领取过两份秘密级文件。直到 2014 年 3 月 19 日清退文件时，章某才发现文件丢失，后经多方查找仍无下落，造成泄密。案件发生后，有关部门给予章某党内警告处分。

案件 6:未做衔接，责任不清

2014 年 9 月 30 日，国庆放假前一天，某市单位为办公室工作人员配备一台涉密计算机，放在公用办公桌上。当日，该办公室另一名工作人员肖某请假，不知此

事。10 月 8 日，国庆假期结束，肖某误以为是为他配备的非密计算机，擅自接入互联网，导致违规外联。案件发生后，有关部门给予肖某行政警告处分。

四、案例分析

错误的行为必然受错误的心态支配。“节假日泄密”之怪现象，很大程度上源于错误的心态作祟，也说明部分涉密人员对保密工作的不重视。

1、赶工心态--“工作必须完成”。在案例 1 中，王某认为节前事必须节前毕，在安排转发通知时，只考虑尽快完成工作，未注意到工作方式是否合规，习惯性地让下属将涉密文件发布上网;在案例 2 中，朱某在本着对业务工作负责的态度，宁可牺牲个人假期，也要在家加班，工作必须完成，但他的“赶工”漠视了保密规章制度，终尝苦果。“加班不回家，回家不加班”的原则是不仅可以有效保护国家秘密的安全，同时也是对自身辛勤劳作的保护。

2、无主心态--“大家/以前这么做，我也这么做”。在案例 3 中，张某认为单位假期工作全在网上办理，就想当然地安排网站值班员，通过内部 OA 系统，对涉密文件进行转发;在案例 4 中，刘某接到严某电话通知，既未到单位加班也未看到原文件，仅根据过去办事经验，电话安排工作人员强某办理涉密文件。在保密工作领域，像张某、刘某这般执行保密制度不坚定，持有“大家/以前这么做，我也这么”的心态，其根本原因就是“无主心态”。

3、**停歇心态--“节假日就应该休息一下”。**在案例 5 中，章某将节前接收涉密文件的事忘得一干二净，在事后一年多时间中也不曾记起;在案例 6 中，肖某节后上班，看到办公室里的新设备，不仅未主动了解设备来由，还理所当然留作己用，严重缺乏对节日前后保密工作的衔接。对于涉密人员来讲决不能因为节假日，忽视保密制度规定的执行，在保密工作中出现节假日的断层。(转自《保密工作》杂志)

（二）警示案例

案例 1：情急求助文印店，两次违规遭追责

案例：2013 年 10 月，某研究所科研生产处调度岳某无法按期完成某军工产品鉴定审查会会议材料准备工作，在请示项目主管李某同意后，委托会务人员赵某开车前往不具备保密条件的文印店复制相关涉密资料。李某对复制提出了保密要求，赵某进行了全程监督。2014 年 3 月，该所质量技术处副处长徐某同样的原因，在经项目主管陈某同意后，再次前往上述文印店复制涉密材料。陈某对复制提出保密要求，徐某及质量技术处工作人员樊某进行了全程监督。两次复制未造成泄密后果。事件发生后，有关部门给予陈某、徐某党内严重警告处分，并处经济处罚；给予李某党内警告处分，并处经济处罚；对该所所长、保密委员会主任姜某，党委书记申某，以及岳某、赵某、樊某等进行通报批评，并处经济处罚。

案例点评：本案中，某研究所工作人员出于工作需要复制涉密资料，却在情急之下求助周边文印店，且时隔数月，再度犯下相同错误。由此可见，该研究所存在严重的内部监管“真空”问题。尤其两次违规行为均事先经过项目主管的同意，虽未造成实际泄密后果，却也难掩从领导干部到工作人员“重业务、轻保密”的思想，认为只要能办成事，偶尔违反保密规定也无妨，直至突破保密红线。应当明确的是，机关、单位复制涉密文件、资料原则上应在本机关、单位办公室、文印室、制作室进行；确需到机关、单位外复制的，应当委托具有涉密资质的单位承担，且场所要采取相应的安全保密措施。周边文印店、图文公司等显然不具备如此保密条件，即使有意识地对其提出保密要求、进行全程监督也不安全，我们应当坚决防止此类低级错误，避免给国家秘密安全造成危害。（转自《警钟长鸣——窃密泄密案例警示教育读本》）

案例 2：个人 U 盘乱拷贝，传网泄密悔莫及

案例：2015 年 5 月，隶属于某县政府办公室的县信息管理中心信息管理员黄某，用个人 U 盘从县政府办综合科文印室刘某使用的、未设置密码口令的涉密计算机拷贝 1 份秘密级文件，并在未履行信息公开保密审查程序的情况下，擅自将该文件上传至县政府门户网站，造成泄密。事件发生后，有关部门给予黄某警告处分，对刘某进行通报批评，对负有领导责任的县信息管理中心副主任进行通报批评。

案例点评：本案存在以下几个泄密因素：一是涉密计算机没有设置口令。口令是计算机及其信息系统的 第一道安全防线，涉密计算机信息系统通过口令验证用户身份，区分和控制访问。口令设置如果不符合保密规定，很容易被破解，破解者可以冒充合法用户进入涉密计算机窃取信息。二是使用个人 U 盘从涉密计算机拷贝文件。在涉密计算机与非密计算机之间进行信息交换，必须采取保密防护措施。个人持有的移动存储介质无法按照保密要求进行管理，且往往连接过互联网，存在很大的安全风险。三是信息未经过保密审查。黄某个人就擅自决定将信息上传至县政府门户网站，可见单位保密审查机制不健全。我们必须从中吸取教训，对于涉密计算机，严格按照规定设置口令，并定期更换；私人移动存储介质不能用于存储、处理涉密信息；信息公开需要履行保密审查程序。（转自《警钟长鸣——窃密泄密案例警示教育读本》）

（三）问题与对策

视频会议正当时，这些泄密隐患不得不防……

疫情之下，中国开始进入“云开工”模式，在线复工、远程办公、视频会议蔚然成风。特别是视频会议，受到了空前关注，相关类型产品在各手机应用平台下载量暴增。

视频会议，顾名思义，是指两个或两个以上不同地方的个人或者群体，通过视频进行及时且互动的沟通，来完成会议目的。

它是一种典型的音视频实时通信：在通信的发送端，将图像和声音信号转换成数字信号，在接收端重现视觉、听觉可获取的信息，与电话会议相比，具有直观性强、信息量大等特点。

但与此同时，其中的泄密隐患也在逐渐凸显……

视频会议泄密隐患

1 非法网络窃听、窃视

视频会议支持“云办公”，意味着大量参会人员进入视频会议网络时所处的物理环境及网络接入环境均为未知。在这种情况下，会议内容可能会遭到黑客的窃听、窃视。

去年 7 月，某知名远程视频会议软件被安全研究人员发现存在严重安全漏洞。黑客可以利用此漏洞远程开启目标用户的摄像头进行窃视，即便用户卸载该视频会议软件也无济于事。

2 参会人员身份冒用

视频会议同样存在参会人员身份被冒用的风险。在一些较大规模的视频会议中，可能就有居心叵测者，伪装身份进入会议。假如安全人员或会议管理员不能及时发现，就会导致因信息泄露而遭受损失。

3 会议内容被窃取、篡改

实时录制、存储视频会议内容，对于会议备忘、后期观摩等具有重要意义，但这也给不法分子非法窃取或篡改会议内容以可乘之机。一旦会议内容遭到篡改，企业将无法获得确切、真实的会议内容，甚至有可能因错误的信息而做出有偏差的工作部署。

视频会议保密要点

加强视频会议的安全保密管理，除了要选择正规渠道、高性能的视频会议软件，还应注意做如下几点。

1 严格权限管理

视频会议应当结合高安全性的身份认证机制，如 IP 地址限定、基于智能卡的网络身份认证产品，使用户不能绕过系统管理层直接通过网络地址收看重要视频会议内容。

另外，还应当对通过身份认证的合格用户进行权限管理控制，以防止非法或者非授权的用户看到不在权限范围内的相关内容。

2 强化密钥安全

在现有的视频会议系统密码体系下，加密和解密的密钥可能是相同的，因此密钥的管理十分重要，使用一段时间后必须进行修改，并且应当提高密码强度，如阿拉伯数字+英文字母+特殊符号等。

3 及时更新软件

一般而言，软件面市后，服务提供商会通过各方监控平台主动嗅探，发现攻击苗头后启动应急响应进行阻断，并进一步分析漏洞，更新补丁。这也要求视频会议用户要关注相关软件信息提示，及时更新软件版本，务必确保信息安全。

重要提醒

需要提醒的是，党政机关如需召开涉密会议，应当在符合保密要求的场所进行，会场及设施设备应当经保密技术检查检测，会场内还应当加装移动通信和无线网络屏蔽设备，**万不可使用不具备保密条件的电话电视会议系统，以防止国家秘密的泄露。**

（转自《保密观》）

（四）自测试题

1.不得在连接互联网的计算机上存储、_____、_____国家秘密信息。

2.涉密计算机的密级应按照存储和_____信息的_____确定。

3.未经本单位_____管理部门审批，不得自行对涉密计算机进行格式化并重装操作系统。

4.涉密载体复制应当加盖复制机关、单位戳记，并视同原件管理。（　　）

5.任何组织和个人不得擅自对外提供国家秘密资料。（　　）

6.发现国家秘密载体在使用中下落不明，应当在 8 小时内向本单位保密工作机构报告，向上级报告不应超过 24 小时。（　　）

7.存储过国家秘密的涉密存储介质不能（　　）密级使用。

A 提高　　B 调整　　C 解除　　D 更改

8.违反《中华人民共和国保守国家秘密法》的规定，（　　）泄露国家秘密，情节严重的，依照刑法有关规定追究刑事责任。

A 故意　　B 故意或过失　　C 过失　　D 擅自

9.任何情况下，不得向境外传递（　　）国家秘密载体。

A 机密级　　B 秘密级　　C 绝密级　　D 内部

10.涉密场所通信设备的使用要求是（　　）

A 禁止接入国际互联网　　B 可以接入公共信息网

C 可以接入内部非涉密信息系统　　D 可以与普通电话线连接使用

南京航空航天大学保密宣传教育参考资料

（2020 年第 2 季度）

参考学时：2 小时

（一）举案说法

警惕机关单位保密制度“休眠”

□姚 斌

根据保密法第七条规定，机关单位应当实行保密工作责任制，健全保密管理制度。一个单位保密管理好不好，很大程度上就体现为保密制度健全不健全。部分单位在保密管理过程中，一方面奉行制度“第一”，另一方面又放任制度“休眠”，导致泄密案件频发。笔者拟从一起泄密案件出发，简要分析这一现象的表现、成因及危害，进而提出唤醒制度“休眠”的办法。

从泄密案件看保密制度“休眠”

1.案情回顾。2018年7月，有关部门在工作中发现，A涉密单位组织处工作人员刘某在文件柜中存放6份绝密级文件复印件，涉嫌违规复印绝密级国家秘密。经查，上述复印件形成于2003年至2005年间。据刘某称，这些文件并非其所复印，而是由组织处时任处长王某在退休前转交，其为在写材料时参考使用，就一直保留在文件柜中。经进一步核实，相关文件还历经其他几名保管人，但因时间久远、人员流动，现已无法查明违规复印责任人。案件发生后，有关部门对刘某进行诫勉谈话和通报批评，责令作出深刻检查，取消2018年度评优资格。

2.案件背后的制度“休眠”现象。办案人员在工作中发现，A涉密单位存在较为严重的保密制度“休眠”问题。目前，该单位共制定出台了30项保密制度，形成了厚厚一本保密制度汇编，其中包括《A涉密单位文件复印管理办法》。根据该办法规定，复印涉密文件须报部门负责人审批，对每份复印件编号、签收和统一管理，确保知悉范围最小化。但由于各部门均配有复印机，工作人员也可以随意出入复印室，实际上并没人真正照此执行，相关复印件也未按涉密文件管理，大范围存在不审批、不登记、不清退情况，泄密隐患严重。

办案人员在工作中还发现，除A涉密单位外，还有不少机关单位也存在类似情况。他们制定出台保密制度后，在内部发文件、开学习会，但是事后没有认真执行实施，使得保密制度“写在文件上、贴在墙上、挂在嘴上”，就是“没有落实到行动上”。对于陷入“休眠”状态的保密制度而言，其存在意义就只剩下形式和数量，在保密管理中起不到规范作用，实际效果也就等同于无制度。如此一来，发生泄密案件是迟早的事。

保密制度为何长期“休眠”

1.对制度建设重视表面化。对保密制度重视与否，决定了保密制度的执行程度，

两者是知与行的关系。办案人员在调查中发现，A涉密单位部分领导干部和工作人员看似明白保密制度重要性，讲起来头头是道，但实际上并不遵守，说一套、做一套，并不想真正按保密制度办事，表现为知行分离、言行不一致。还有一些机关单位问题更严重，他们表面上重视保密制度建设，实际上只是为了做样子、应付检查，制定制度平时不执行，只是在保密检查时拿出来给人看，这样制度那样制度都有了，好像保密制度体系健全完善了，保密管理也就加强了。

2.存在“制度自动实施”观念。制定保密制度目的是解决保密管理中的问题，但问题解决的关键还是在于将制度落实下去。在上述案例查结后，A涉密单位组织开展了一系列整改工作，其中包括制定两项新保密制度。这也反映出实践中存在一种矛盾现象：一方面不执行制度、问题解决不了，另一方面又不停为了解决问题制定出台制度。古语有云：“徒法不足以自行。”保密制度建设不是制造机器人，不是制定出台就会自动运转，必须要由明确责任主体遵照执行，由机关单位保密工作机构监督落实，这样保密制度才能运转起来，取得实际效果。

3.对制度执行抱有抵触心理。制定制度难，执行制度更难。在一些机关单位内部，执行保密制度容易遭致多方面阻力。据A涉密单位有关保密干部反映，该单位制定出台了手机保密管理制度，但部分领导干部和工作人员认为，开会将手机放进保密柜容易耽误事，不愿意按该制度操作，普遍存在将手机带进涉密会场情况。诚然，保密制度多为约束性条款，对涉密事项要求高、要求严格，执行中总会遇到这样那样的困难，存在执行阻力。如果保密干部缺乏高度的责任心和坚定的意志力，就会使保密制度执行半途而废，陷入“休眠”状态。

保密制度“休眠”带来的危害

1.破坏保密工作氛围。保密工作氛围形成是潜移默化的，与保密制度执行息息相关。在上述案例中，A涉密单位普遍存在违规复印涉密文件情况，说明该单位保密工作氛围极为松懈。从表面上看，这是工作人员集体缺乏保密意识；从深层次看，这是该单位保密制度执行缺失。培养保密工作氛围，必须在执行保密制度、遵循保密制度的实践中进行。如果制定出台保密制度又束之高阁，有章不循、有规不依，再好的制度都会变成“一纸空文”，造成工作人员对保密工作不重视，乃至对整个单位保密工作氛围都产生负面影响。

2.助长不良违规风气。严格执行保密制度，可以引领良好的保密风气。如果一个单位对保密制度“光制定、不执行”，或者“重制定、轻执行”，即使制定再多、再好，也必然会助长违反保密制度的不良风气。在上述案例中，A涉密单位制定出台了大量保密制度，但未严格执行，也未对违反保密制度的行为进行纠正，使保密制度刚性产生了动摇，严重削弱工作人员的规矩意识。正如刘某所说，“这些制度刚出台时，大家都是重视的，但是过一段时间，看到保密制度并未真正执行，也没人因违规被查处，就不重视了，自己也成了不执行制度的一分子”。

3.影响保密管理权威。保密工作机构开展保密管理的权威性，源于对保密制度的严格执行。无论多健全完善的保密制度，只要有一个地方没有执行到位，工作人员就会产生质疑，进而滋生对保密工作机构的信任危机，保密管理也将变得难上加难。在上述案例中，A涉密单位保密办负责同志说，其曾在单位内部大会小会上反复

强调，不得随意复印涉密文件，要求各部门严格审批，但由于该单位过去执行保密制度不到位，导致保密办提的要求都没人听，说什么、做什么都是白费功夫。

唤醒“休眠”的保密制度

1.要做到“三个抓”。一是抓态度。要重视保密制度的制定和执行，克服对制度建设重视表面化，明确制定制度不是为了做摆设、应付检查考核，而是为了贯彻执行、解决实际问题。二是抓认识。贯彻执行保密制度，就怕制度执行过程中对业务与保密关系认识不统一，导致“说起来重要、干起来次要、忙起来不要”，必须时不时拧拧螺丝、敲敲脑壳，形成“保密制度必须执行”统一认识。三要抓落实。保密制度执行中的阻力不可避免，机关单位保密工作机构要以高度的责任心和坚定的意志力，理性分析、耐心讲解，采取有效措施，切实化解、克服阻力。

2.要做到“三个用力”。一是在关键环节上用力。要聚焦保密制度落实的关键环节发力加压，围绕节点、突出重点、疏通堵点，稳步推进制度落实，决不在执行的节骨眼上搁浅。二是在问题导向上用力。推动保密制度贯彻落实，最大阻力多是来源于机关单位内部，保密工作机构不能看到意见大、执行难就妥协让步，必须盯住原本要解决的问题，逐一推动制度落实。三是在监督检查上用力。要用好监督检查“推进器”，对不予执行、执行不到位、敷衍塞责行为要坚决予以纠正，对违反保密制度行为要坚决予以问责，该通报的通报，该处理的处理，确保保密制度落实到位。

3.要做到“三个精准”。一是精准契合实际。将保密制度执行到位，前提是要有科学管用的好制度。机关单位制定保密制度必须突出可操作性，不能机械照搬上级规定，要把保密工作要求与本单位实际结合起来，做到“上接天线、下接地气”。二是精准执行到底。在保密制度制定出来之后，机关单位要明确制度执行主体和监督主体，启动制度实施程序，强化贯彻执行，抓好督促落实，一直抓到“最后一公里”，直到落地见效。三是精准抓好整体落实。要注重突出保密制度体系性特点，发现问题不能简单地“头痛医头，脚痛医脚”，要以点带面、层层突破，通过抓住一项制度执行，推动整体保密制度落实。

责任编辑/孙战国

(转自《保密工作》杂志)

（二）警示案例

案例 1： QQ 在线图便利 传递共享致泄密

案例：2013 年 10 月，某重要涉密文件在互联网上被泄露。经查，该县教育局办公室主任马某为及时组织传达某会议精神向县委某部门办公室主任周某索要市委有关部门的会议文件。周某手中的文件则来自其上级某部门办公室主任洪某。洪某在明知该材料属于国家秘密的情况下，仍要求办公室副主任王某通过 QQ 在线传递给周某。周某收到文件后，在县委组织的会议上进行了发放，并于会后通过 QQ 邮箱传递给马某，马某又将该文件上传至 QQ 群共享文件夹中，供各中小学传达学习。某中学办公室主任从 QQ 群文件共享中下载了该文件，刊登至学校门户网站，造成泄密。事情发生后，洪某、周某受到党内严重警告处分，王某受到党内警告处分；有关部门对负有领导责任的人员进行了诫勉谈话，并责令作出书面检查。

案例点评：QQ 是点对点的聊天平台，而 QQ 群是多人聊天交流的公众平台，群主在创建群后，可以邀请好友或者有共同兴趣爱好的人到一个群里聊天，属于开放性平台。通过 QQ 传递和 QQ 群共享国家机密，无疑相当于将其暴露在网络空间，全无保护。本案中，洪某、周某、王某等人通过 QQ 聊天工具传递国家秘密，致使国家秘密处于失控状态，最终泄密，根本原因还在于缺乏保密意识和保密技能。该过程牵涉多人，只要有人稍有警觉，都有可能减轻负面影响。由此，我们应该时刻警醒，并自觉加强保密知识和技能的学习，提升保密素养，尤其在享受即时通讯工具带来便利的同时，更应该清醒认识安全保密的重要性。

（转自《警钟长鸣——窃密泄密案例警示教育读本》）

案例 2：偷拍文件存电脑 非法获密被判刑

案例：2013 年 10 月，有关部门在工作中发现，某省研究机构人员陆某非法持有一份密级文件的数码图片。经查，2013 年 5 月，陆某在某机关研究室副主任赵某的办公室内看到这份涉密文件，趁赵某不备，用手机偷拍文件，并储存在个人计算机中，直至被有关部门发现。2014 年 5 月，司法机关以非法获取国家秘密罪判处陆某有期徒刑两年。

案例点评：当前，手机使用已经深入社会生活的方方面面，也不可避免地给保密管理带来严俊挑战。手机特别是智能手机，集录音机、照相机、摄像机、定位仪、掌上电脑于一体，具有视频通话、宽带上网、位置服务、大容量数据存储及处理等多种功能，在方便生活和工作的同时，也存在通信内容被截获监听、存储信息被窃取利用、用户位置被定位跟踪以及被控制成为窃听窃照工具等多种安全保密隐患，为窃密互动提供了可乘之机。本案中，陆某趁机关研究室副主任赵某不备，用手机偷拍机密级文件并存储在个人计算机中，一方面违反普通手机使用保密规定和计算机使用相关规定，存在严重泄密隐患；另一方面其行为系主观故意，已构成非法获取国家秘密罪，最终受到法律的严惩。我们务必从中吸取深刻的教训。

（转自《警钟长鸣——窃密泄密案例警示教育读本》）

（三）问题与对策

慎点！这些邮件很可能是黑客布下的陷阱

近期，如果您的电子邮箱中收到标题为《最新版新冠肺炎诊断和预防措施》《武汉旅行信息收集申请表》之类的邮件，一定要提高警惕，谨慎点击，因为这极有可能是黑客布下的陷阱。

早在新冠肺炎在我国肆虐期间，就有消息称境外黑客对我国发起网络攻击和渗透。如今，在疫情防控常态化之下，境外黑客组织仍不断尝试窃取我国医疗卫生行业的相关机密，往往利用新冠疫情题材诱使用户执行木马程序，最终达到窃取情报的目的。

黑客是指未经授权或利用网络系统漏洞等方式进入计算机系统的非法入侵者，**“非授权入侵”是黑客的基本特征，**对网络安全构成了严重威胁。

黑客常用的入侵手段

1.利用计算机安全漏洞攻击

这是黑客最常用的攻击方式。黑客在攻击之前，会先通过安全扫描工具扫描准备入侵的网络，再通过探测攻击目标来发现、确认安全漏洞，并通过代码等进入计算机，

最后发起攻击，非法执行自己想要的程序。

2.通过口令弱点攻击

许多用户安全意识不足，所采用的密码安全级别比较低，黑客往往通过暴力破解，尝试用不同的排列组合，可轻易获取用户的账号权限。

3.植入木马程序

最常用的方法就是把特定程序依附在合法程序中，一旦用户触发该程序，那么依

附在内的黑客指令代码会同时被激活，这些代码将完成黑客已指定的任务。

4.伪造信息攻击

黑客通过发送伪造的路由信息，构造源主机和目标主机之间的虚假路径，使流向目标计算机的数据包经过黑客操作的计算机，从而获取数据包中的敏感信息。

如何防范黑客入侵

习近平总书记明确指出，没有网络安全就没有国家安全。黑客是影响网络安全的因素之一，黑客入侵会使计算机运行瘫痪，造成个人、企业信息泄露。甚至有些黑客会非法闯入机关内网，窃取高度敏感信息，危害国家安全。

那么我们在日常生活中，如何做才能防范黑客入侵呢？除了上文提到的谨慎点开陌生邮件，我们还需要做到以下几点：

1.启用防火墙

防火墙是计算机与网络连接后，起到保护作用的部分，常用的 windows 7 和 Windows 10 等操作系统均有自己的防火墙，开启后能在一定程度上保护电脑不被黑客入侵。

2.提高口令强度

个人用户应提高口令强度，应采用数字、英文大小写和特殊字符相结合的 8 位以上密码，可极大降低被黑客暴力破解密码的风险。

3.安装网络病毒拦截灭杀软件

目前有很多优秀的安全厂商研发了比较可靠的安全工具，安装后可实时监控电脑运行状态，定期更新特征库和病毒库，在黑客入侵的时候及时拦截灭杀。

4.不浏览黄赌网站

赌博涉黄网站是黑客植入木马程序的首选地带，用户在浏览相关网站的同时，终端有很大可能被植入木马程序。

黑客攻击导致的安全事件危害不容小觑，尤其在全球抗击疫情的特殊时期，保护好我们的信息安全至关重要。特别是机关、单位工作人员更要牢记“涉密不上网、上网不涉密”的要求，严格防范黑客攻击。

（转自《保密观》）

（四）自测试题

保密小测试

判断题

1 就确定国家秘密知悉范围的基本原则，甲乙二人发生争论。甲认为，确定国家秘密的知悉范围应按照级别需要原则和最小化原则，级别越高知悉的国家秘密越多。乙认为，应按照工作需要原则和最小化原则确定国家秘密知悉范围，与级别无关。乙的观点是正确的。（ ）

2 对于一个单位来说，级别最高的主要领导，由于决策的需要，应当知悉本单位的所有国家秘密；对于中层干部来说，并不需要所有人知悉国家秘密，或者某个人知悉所有国家秘密，但应当科学限定在最小范围。（ ）

3 工作需要原则和最小化原则是确定国家秘密知悉范围基本原则。对于一个单位来说，因工作需要必须知悉国家秘密的，才能合法接触、知悉国家秘密，且需要限定在最小范围，级别高并不代表必须知道国家秘密，一个单位级别最高的主要领导也不一定必须知悉所有的国家秘密。（ ）

4 按照有关规定，定密工作的程序必须规范：由承办人对照保密事项范围提出国家秘密确定、变更和解除的具体意见，再由定密责任人审核批准并承担法律责任。其中，承办人必须就相关事项应该确定何种密级、保密期限、知悉范围或者是否变更、解密提出具体意见。（ ）

单项选择题

5 假设：全国及各省、自治区、直辖市居民消费价格指数在公布前为秘密级国家秘密事项。那么，某个县、区或者市的居民消费价格指数在公布前，可以（ ）。

A. 作为商业秘密进行管理　B. 作为工作秘密进行管理　C. 确定为秘密级国家秘密

6 涉密岗位，是指在日常工作中（ ）或者（ ）接触、知悉国家秘密事项的岗位。

A. 产生 经常　B. 经管 偶尔　C. 产生 经管 经常

7 按照有关规定，涉密人员的确定、上岗，应当按照以下（ ）程序。

A. 确定人员，确定岗位，保密教育，背景审查，报告备案

B. 确定人员，确定岗位，背景审查，保密教育，报告备案

C. 确定岗位，确定人员，背景审查，保密教育，报告备案

8 我国保密工作体制的核心是（ ）。

A. 一个机构，两块牌子　B. 依法行政　C. 党管保密

南京航空航天大学保密宣传教育参考资料

（2020 年第 3 季度）

参考学时：2 小时

（一）举案说法

密件经手责任重　切勿违规受惩处

□宋筱婷

涉密文件保密管理，可谓“老生常谈”，在不同场合、以不同视角被屡屡提及。但我们往往忽视的是，涉密文件保密管理，并非个体所能独立完成，在整个文件运转过程中，往往存在多名经手人，一人发生疏忽，则整个安全屏障即被打破。所以，以“人”为视角，深入研究从“入手”“倒手”再到“出手”的整个经手过程中如何做好保密管理，是确保涉密文件万无一失必须审慎思考的问题。

典型案例

一、密件“入手”环节

案例1：2018年4月，某市机要部门通知原市检验检疫局服务中心文件专管员周某紧急去取一套涉密文件，但周某忙于手头其他工作，难以走开。周某认为，取文件而已，反正谁去都一样，便未向分管领导报告，私自委托新入职尚未接受保密培训的驾驶员赵某帮其代领。赵某领取文件后，出于炫耀心理，在返回途中于车内私自用手机将其中3份机密级文件首页进行拍照，并实时在微信群“相亲相爱一家人”中发布，造成泄密。案件发生后，有关单位对赵某作出解除劳动合同，并移交司法机关的处理；取消周某文件专管员资格，责令作出书面检查，并处罚金1000元；对服务中心主任文某进行诫勉谈话；给予该局办公室主任刘某党内警告处分，对副局长任某、局长奉某进行约谈，并责令作出书面检查。

案例2：2014年1月下旬，临近春节放假，某单位机要员李某已收拾完桌面办公用品，准备放假。“李某，快来帮忙分年货啦！抓紧时间，别耽误大家过节。”李某一听，来了精神，火速支援，在单位办公楼前的小广场上和大家一起忙活起来。正忙得热火朝天，市委的机要车来送机要文件了，李某的心思一心记挂着年货，便在办公楼门口签收了装有9份秘密级文件的6个信封，随手放在大楼一楼就近的窗台上（未拆封、未登记），分完年货后，也忘记将信封带回办公室。2月底清退文件时，李某才发现密件已丢失。后经该单位、市保密局及当地公安机关全力查找，仍未能找回。案件发生后，有关部门给予李某开除党籍、公职处分，给予该单位保密办主任潘某撤销党内职务、行政降级处分，给予党委书记姜某党内严重警告、行政记大过处分。

二、密件“倒手”环节

案例3：2019年1月，有关部门在工作中发现，某市政府部门办公室刘某使用QQ软件传输涉密文件扫描件。经查，刘某为收件方，发件方为同处室的同事霍某。原来，为尽快完成某项目申报任务，其他部门同事王某通过机密级涉密计算机将材料以压缩包形式发给霍某，督促其抓紧按要求开展工作。因时间紧、任务重，霍某仅粗粗查看了压缩包中的一级目录，未发现存在于二级目录中的1份机密级文件，便用光盘将该压缩包从涉密计算机中导出，复制到自己的连接互联网计算机上并通过QQ发给刘某。案发时，刘某也尚未及时查看压缩包中所有文件，未发现其

中包含密件。目前，此案正在进一步查处中。

案例4：2019年2月，夜已深，某市政府业务部门工作人员望某在办公室加班整理文件，发现一份传阅的机密级会议纪要对业务工作具有很强的指导和借鉴意义，便产生了全文留存以便学习参考的想法。望某知道，按规定若想留存密件需履行报批手续并使用涉密复印机进行复印，但涉密复印机由单位文印室统一管理，已经锁门。此时的望某已十分疲惫，实在不想第二天再“折腾”了，便关了办公室的门，偷偷用手机对该文件进行了拍照，并使用手机软件对拍摄的涉密文件进行文字识别后发送至自己的办公用互联网计算机上，转化为Word文档进行编辑。目前，此案正在进一步查处中。

三、密件“出手”环节

案例5：2016年12月，有关部门在工作中发现，某参公事业单位研究室主任蒋某在连接互联网的计算机中违规存储、处理大量涉密材料，其中绝密级国家秘密1份、机密级国家秘密12份、秘密级国家秘密59份，涉及国家秘密数量多、时间跨度大。经查，蒋某为转业干部，曾辗转部队多个部门工作，业务经验丰富。该计算机中存储、处理的涉密文件为其2008年转业时私自留存。据蒋某称，其日常有收集资料的习惯，认为这种做法对新岗位熟悉工作帮助很大。事件发生后，有关部门给予直接责任人员严厉处分。

案例6：2015年5月，有关部门在工作中发现，某县县委宣传部一台连接互联网的计算机违规存储、处理国家秘密信息。经查，该计算机使用人为工作人员易某。同年3月，工作人员陈某因临盆在即，产假交接工作过程中，贪图省事，未按规定履行工作交接手续，在未告知相关领导及同事的情况下，私自将移动硬盘中的部分涉密文件与非涉密文件一并拷贝至易某使用的非涉密计算机上（内含3份秘密级文件）。易某接手工作后，工作量激增，未能及时对陈某交接的电子文件过目，导致对该情况未能及时发现并作出正确处理。事件发生后，有关单位给予陈某、易某行政警告处分，在全地区范围内进行通报批评；并对县委宣传部主要领导进行诫勉谈话。

案件分析

需要说明的是，本文未将故意卖密牟利、对外提供等极端恶劣情形包含在内，仅限于机关单位日常工作的范围内分析讨论。

一、从主观意识上看

1.故意，即主动追求或被动放任行为后果发生的情况。一是主动追求。案例1中赵某将涉密文件首页拍照后主动发布至微信群就属于典型的主动追求泄露后果发生。此类案件中，行为人往往通过泄露后果的实现来达到某种私人目的。该目的并不一定是经济利益，也可表现为图炫耀、还人情或讲义气等，甚至是为了作为自己处于某种状态、位置的证明。二是被动放任。案例4中望某违规传递、案例5中蒋某私自留存、案例6中陈某违规交接的行为，都属于将涉密文件置于危险境地，对后续可能产生的危害后果持放任态度，不予考虑。上述情况的根源都在于将个人的利益、便利凌驾于国家秘密安全之上。

2.过失，即行为存在瑕疵却对行为后果持否定态度的情况。一是疏忽大意。案例2中李某因忙于手头其他工作对密件随手放置，案例3中霍某、刘某及案例6中易某未能对文件及时查看均属于此类情况。在文件经手过程中，往往存在阻碍行为人审慎履职的特殊情况、特殊时间点等客观因素是案件发生的重要原因。特殊情况，如时间紧、任务重；特殊时间点，如节假日前夕、休假前夕、场所变动前夕等，此类案件多发易发。二是

过于自信。明知违规但自认为没有危害或危害不会发生。案例1中作为文件专管员的周某，自认为不会出问题，在明知文件“专管”要求的情况下，仍私自委托新人赵某代领文件，最终追悔莫及。

二、从行为方式上看

1.密件“入手”环节。可以表现为私自委托不属于涉密文件知悉范围人员去收取密件导致泄密；或收取密件时心存旁骛，忙于其他工作、私人事务，如放假、下班、就医等，对密件随手处置泄密；或“入手”时不按规定置于保密柜中，随意放于桌面、玻璃柜、抽屉等位置，导致文件丢失或被他人复印、窃取等。实践中，还曾发生取件返程途中违规乘坐公共交通工具将密件遗失的情况。

2.密件“倒手”环节。从对象上看，分为“倒”给别人和“倒”给自己。可以表现为对自己传阅的文件不认真审阅，未能及时发现文件密级、保密期限、发放范围等核心要素，导致通过互联网违规传递；或贪图便利，明知不符合保密规定，仍然违规复印、扫描、摘录、汇编；或为参考学习，私自拍照上传至互联网计算机中等。实践中，还曾发生为了将字体放大方便观看而将文件拍照后上传至互联网计算机的情况。

3.密件“出手”环节。可以表现为该移交不移交，将手中密件隐匿不交或私自留存备份，从阶段性经手变为长期持有，后续或自用、或贩卖，进而造成泄密或泄密隐患；也可以表现为“一揽子”移交，不按规定将密件、非密件分类移交，不详细告知接手人注意事项，甚至“单方”移交，不与接手人发生接触，自顾自办理完毕。这极易导致接手人对情况不了解，进而造成误操作，形成连锁反应。案例6就属于这种情况，实践中还曾发生不告知移交的计算机中存在涉密文件导致接手人误连互联网的情况。

应对措施

一、加强保密教育，树正思想“三观”。一是树正“利益观”。将国家利益时刻放在首位，严禁将密件作为实现个人目的的工具和手段，绝不能将个人利益凌驾于国家秘密安全之上。二是树正“业绩观”。完成工作不拖延固然重要，但保量更要保质，不能因时间紧、任务重就放松了工作标准和要求，坚决杜绝各种图便利、走捷径的行为。三是树正“大局观”。真正确立“文件保密一盘棋”的思想，从自身做起。在密件“出手”环节要坚决摒弃“文件出手脱干系”的错误思想，坚持“扶上马、送一程”，完整、准确交接，认真讲解，有效避免接手人遗漏。在密件“入手”环节要坚持认真、细致的工作作风，对入手文件不能简单放置，要逐一过目，做到心中有数，发现问题，及时处理，将失泄密隐患消于无形。

二、推进保密管理，强化制度落实。一是科学、合理配置资源。合理配置人力资源，在涉及核心、紧急、重大工作且文件经手数量巨大时，或抽调专人帮助工作，或灵活机动设置岗位替补，有效防范个人“多线作战”、工作过于繁重导致工作失误的情况。合理配置办公资源，尤其是经手密件数量多、密级高的岗位，及时配备涉密计算机、涉密扫描仪、涉密复印机，为便利工作创造条件，尽可能杜绝“因公”图便利受惩处的情况，保护好文件经手人工作的积极性和主动性。二是组织签订专项保密承诺书。立足密件经手流程，结合具体岗位职责，签订专项保密承诺书，详细列举具体岗位职责、密件经手风险点及相关法律责任，既明晰了工作标准和要求，又起到了保密教育的现实效果。三是组织定期检查，及时发现隐患。针对文件经手数量大、密级高的人员和部门，定期组织自查、互查和抽查，实行纸质、电子密件全覆盖，以有效防范丢件、漏件、私留、私泄、私拷、私传、误传等情况的发生。此外，对为追求个人利益主动泄密，且造成文件内容大范围泄露的，依法依规严肃处理，绝不姑息；构成犯罪的，移交司法机关，依法追究刑事责任。

责任编辑/孙战国

(转自《保密工作》杂志)

（二）警示案例

案例 1：情急求助文印店，两次违规遭追责

案例：2013 年 10 月，某研究所科研生产处调度岳某无法按期完成某军工产品鉴定审查会会议材料准备工作，在请示项目主管李某同意后，委托会务人员赵某开车前往不具备保密条件的文印店复制相关涉密资料。李某对复制提出了保密要求，赵某进行了全程监督。2014 年 3 月，该所质量技术处副处长徐某同样的原因，在经项目主管陈某同意后，再次前往上述文印店复制涉密材料。陈某对复制提出保密要求，徐某及质量技术处工作人员樊某进行了全程监督。两次复制未造成泄密后果。事件发生后，有关部门给予陈某、徐某党内严重警告处分，并处经济处罚；给予李某党内警告处分，并处经济处罚；对该所所长、保密委员会主任姜某，党委书记申某，以及岳某、赵某、樊某等进行通报批评，并处经济处罚。

案例点评：本案中，某研究所工作人员出于工作需要复制涉密资料，却在情急之下求助周边文印店，且时隔数月，再度犯下相同错误。由此可见，该研究所存在严重的内部监管“真空”问题。尤其两次违规行为均事先经过项目主管的同意，虽未造成实际泄密后果，却也难掩从领导干部到工作人员“重业务、轻保密”的思想，认为只要能办成事，偶尔违反保密规定也无妨，直至突破保密红线。应当明确的是，机关、单位复制涉密文件、资料原则上应在本机关、单位办公室、文印室、制作室进行；确需到机关、单位外复制的，应当委托具有涉密资质的单位承担，且场所要采取相应的安全保密措施。周边文印店、图文公司等显然不具备如此保密条件，即使有意识地对其提出保密要求、进行全程监督也不安全，我们应当坚决防止此类低级错误，避免给国家秘密安全造成危害。（转自《警钟长鸣——窃密泄密案例警示教育读本》）

案例 2：个人 U 盘乱拷贝，传网泄密悔莫及

案例 :2015 年 5 月 ,隶属于某县政府办公室的县信息管理中心信息管理员黄某，用个人 U 盘从县政府办综合科文印室刘某使用的、未设置密码口令的涉密计算机拷贝 1 份秘密级文件，并在未履行信息公开保密审查程序的情况下，擅自将该文件上传至县政府门户网站，造成泄密。事件发生后，有关部门给予黄某警告处分，对刘某进行通报批评，对负有领导责任的县信息管理中心副主任进行通报批评。

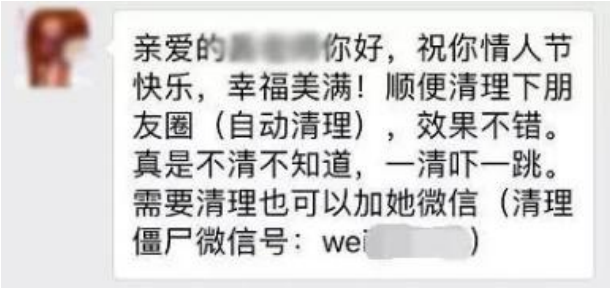
案例点评：本案存在以下几个泄密因素：一是涉密计算机没有设置口令。口令是计算机及其信息系统的 第一道安全防线，涉密计算机信息系统通过口令验证用户身份，区分和控制访问。口令设置如果不符合保密规定，很容易被破解，破解者可以冒充合法用户进入涉密计算机窃取信息。二是使用个人 U 盘从涉密计算机拷贝文件。在涉密计算机与非密计算机之间进行信息交换，必须采取保密防护措施。个人持有的移动存储介质无法按照保密要求进行管理，且往往连接过互联网，存在很大的安全风险。三是信息未经过保密审查。黄某个人就擅自决定将信息上传至县政府门户网站，可见单位保密审查机制不健全。我们必须从中吸取教训，对于涉密计算机，严格按照规定设置口令，并定期更换；私人移动存储介质不能用于存储、处理涉密信息；信息公开需要履行保密审查程序。（ 转自《警钟长鸣——窃密泄密案例警示教育读本》）

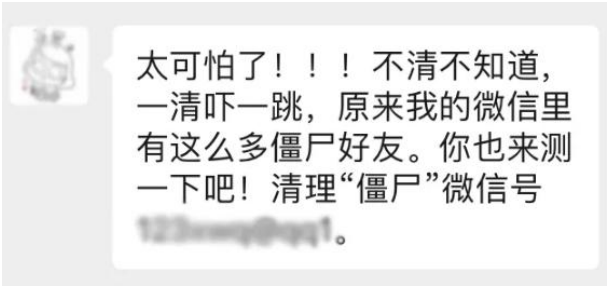
（三）问题与对策

警惕！这种微信“清粉”服务你还敢用吗？

现如今，微信已经占据人们生活的方方面面，出于工作、社交等各种原因，微信好友越加越多，但很多好友往往是因“一面之缘“加上的，加上之后再无联系。
为了控制微信好友人数，及时清理那些没有互动、没有联系，甚至对方已将你拉黑或删除的“僵尸粉”，大家会定期或不定期地手动清理一波“好友”，但由于手动清理比较麻烦，于是很多号称零误差的批量“清粉”软件应时而生。

相信大家或多或少都收到过这种类似的消息：**不清不知道，一清吓一跳，原来我的微信里有这么多僵尸好友。你也来测一下吧！清理“僵尸”微信号***。**



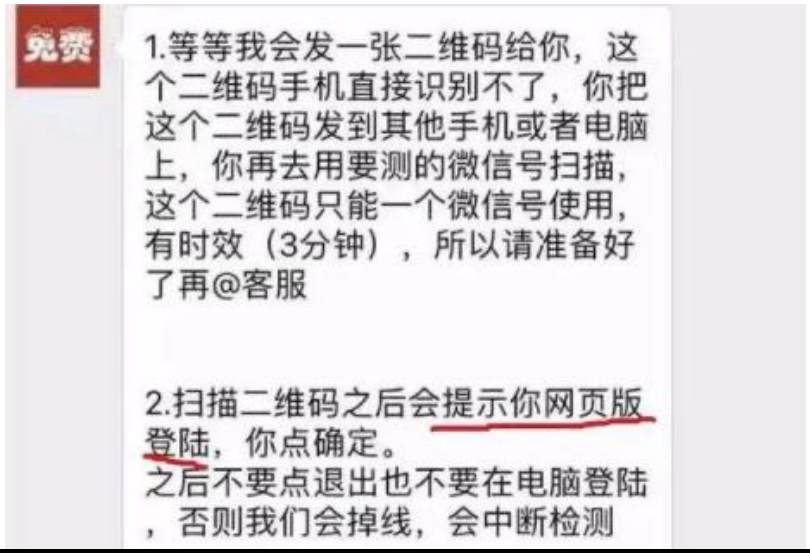


注意！！！千万别跟着去“清粉”！

现在有很多网络平台宣称可提供“清粉”服务，并号称绿色清理、免打扰、免下载、无痕清粉。但如果你真使用了**“清粉”服务，那就“中招”了！**

“清粉”软件如何运行

当购买“清粉”服务后，商家会发来一个**自称 “登录自动检测系统”的二维码**，让用户扫描登录后进行自动清粉。据信息安全专家介绍，**“清粉”原理是通过应用集群控制软件控制待清理微信账户，令该账户自动向其所有好友群发消息，再由群控软件根据“信息是否能够成功发送接收”来识别其中哪些是“僵尸粉”并删除。**



其实，一旦扫码完成，他人就获得了登录你微信电脑端的权限，将存在以下风险。

“清粉”软件的风险

1.个人隐私泄露

群控软件一旦“接管”账户，个人将失去微信的唯一控制权，意味着隐私会毫无保留地被他人掌握，好友数据、聊天记录、家庭住址、单位性质及社会关系等信息会被盗取并作为商品出售。很多用户在成功“清粉”后，会收到大量骚扰电话，而且能够精准说出个人的具体信息。

2.导致财产损失

不法分子在精准掌握个人信息的基础上，能够增加诈骗成功概率，降低诈骗成本。同时，不法分子可以直接使用你的微信账号，获取好友信息，并伪装成你对亲友进行网络诈骗。甚至，还可以直接盗用个人微信支付、绑定银行卡中的资金。

3. 散发不良信息

能够在你毫不知情的情况下，将你拉入到各种不良群聊，并不断用垃圾消息进行轰炸骚扰。还可以伪装成你，在你的工作群、家庭群、朋友圈，散发淫秽色情等不良信息。不仅会给领导、同事、亲友留下“坏印象”，引发不必要的麻烦，甚至有可能引发大量投诉而被封号。

4.植入木马病毒

不法分子利用微信的控制权，可在手机中植入木马病毒，手机一旦被木马控制，就会变成移动的窃听器、窃视仪，还可能被远程控制，被不法分子获取系统的使用权，导致各种安全隐患。

防范措施

1. 拒绝“清粉”服务

提升对个人信息与数据权限的安全保护意识，切勿尝试各类所谓清理“僵尸粉”的工具。微信数据显示，截至 2020 年 6 月底，微信共对上百万个明确使用“清粉”软件等外挂的账号，进行了短期或永久限制处理。

2.慎扫来源不明的二维码

扫描二维码可以快速实现信息传递、网页链接跳转、手机支付、凭证发放等功能。由于二维码不能被人眼直接识别编码内容，极易被心术不正的人利用。扫描恶意二维码后，有可能打开钓鱼网站、触发恶意程序和木马病毒的自动下载程序等，因此一定慎扫、不扫

来源不明的二维码。

3.遇到相关骚扰信息可举报投诉

如果收到清理“僵尸粉”的广告，可以在微信**个人聊天窗口点击右上角菜单—投诉—存在欺诈骗钱行为**，或者在**微信群聊窗口点击右上角菜单—投诉—群成员存在欺诈骗钱行为**。微信安全团队提醒用户，不要使用破坏微信软件协议或具有外挂功能的插件及软件。如遇安全风险，可通过微信客户端、腾讯 110 小程序进行投诉。

（转自《保密观》）

（四）自测试题

保密小测试

判断题

1 某省直机关采购了一批计算机，对于拟淘汰的计算机如何处理，甲乙两人意见不一。甲认为，淘汰的全部计算机可以捐献给对口扶贫县的中小学校，以物尽其用。乙认为，淘汰的计算里有大部分属于涉密计算机，必须按照国家有关涉密载体销毁管理的规定进行处理，不能擅自捐赠。乙的观点是对的。（ ）

2 为了节约开支，机关单位可以将淘汰的涉密计算机交本机关、本单位非涉密部门使用。（ ）

3 某机关工作人员深夜遇到需要紧急处理的涉密文件，但自己的涉密计算机出现了故障。因事情紧急，为了不耽误时间，他使用自己随身携带的家用笔记本电脑处理涉密信息，顺利完成了工作，且他为了安全保密，处理工作时特意把笔记本电脑与互联网断开，待处理完涉密信息，打印完毕并删除后才连接互联网。他的做法是对的。（ ）

4 涉密存储介质经文件删除并格式化处理后，仍不得作为非涉密存储介质使用。（ ）

单项选择题

5 某机关领导外出公干时公文包被窃，经找回后发现包内钱物丢失，涉密文件完好无损，这一事件（ ）。

A.不应视为泄密事件　　B.属于泄密事件

C.在不能证明文件未被不应知悉者知悉时，按泄密事件处理

6 机关单位对所产生的国家秘密事项，解密之后需要公开的，应当（ ）。

A.直接公开　　B.依照信息公开程序进行保密审查

C.提交本机关、本单位主要负责人决定是否公开

7 违反《中华人民共和国保守国家秘密法》的规定，（ ）泄露国家秘密，情节严重的，依照刑法有关规定追究刑事责任。

A.故意　　B.过失　　C.故意或过失

8 存储过国家秘密的涉密存储介质可以（ ）密级使用

A.降低　　B.提高　　C.解除

南京航空航天大学保密宣传教育参考资料

（2020年第4季度）

参考学时：2小时

（一）举案说法

加大工作秘密保护 刻不容缓

□吴 瑞

典型案例

案例1：某县政协经联委干部柳某，为方便撰写该县《政协志》，在未经保密审查的情况下，将自行收集的5000余份政协系统电子文件资料（含标“机密”4份、标“秘密”6份），于2015年3月通过互联网计算机上传到个人百度云网盘账户，直至保密检查被发现。经鉴定，上述10份标密文件资料不属于国家秘密事项，但部分文件资料包含政协工作敏感信息、工作秘密，按照有关规定不得公开。事件发生后，有关部门给予柳某行政警告处分。

案例2：2013年，某省民族事务委员会（宗教局）时任文书黄某，在负责制作当年《全省民委主任（宗教局长）会议材料汇编》时，由于缺乏保密意识，未与提供材料的业务处室核对文件是否涉密以及控制接触范围，将汇编文件直接存储在连接互联网的计算机上处理并打印。2016年5月，黄某调离省民委（宗教局），在办理工作交接时，也未对该计算机内的相关文件进行清理、移交。2017年8月，有关部门在自查自评督查工作中发现，现任文书刘某使用（原为黄某使用）的计算机内存储的《全省民委主任（宗教局长）会议材料汇编》涉嫌涉密。经鉴定，该文件为工作秘密。事件发生后，省民委（宗教局）将黄某的违规行为通报其本人及现任职单位，并在本系统内通报。

以上两起案件都是在汇编文件过程中违规处理工作秘密，暴露出的共同问题是部分机关单位工作人员保守工作秘密的意识缺失，相关的管理制度和监督机制也没有很好地建立健全。

案例3：2017年8月，某省公安厅刑事侦查总队综合执法支队干部黎某从机要科领取了6份标密文件（4份机密级、1份秘密级、1份警务工作秘密）后，前往修理厂修车，期间不慎将上述文件丢失。刑侦总队当即向省公安厅汇报，同时全面组织查找文件，并找回5份文件，但1份警务工作秘密文件查无下落。事件发生后，有关部门给予直接责任人黎某党内严重警告和行政记大过处分，对负有监管、领导责任的支队长和支队政委分别进行通报批评和保密约谈。

案例4：2016年11月，某县公安局民警聂某为撰写学位论文搜集材料，从该市公安综合信息网下载了有关特种行业管理的文件资料26份（其中标“内部”3份），并通过光盘刻录将上述文件资料转存于个人的笔记本电脑。经鉴定，上述文件资料中有1份属于警务工作秘密。事件发生后，有关部门给予聂某通报批评处理。

公安机关是目前为数不多的对工作秘密进行明确和规范的部门之一，对警务工作秘密的定义、具体范围、标识方法做出较为具体的规定，是对国家秘密之外的其他内部敏感信息进行系统保护的一个范例。

案例5： 2015年2月，某市110报警服务台接到举报电话，内容涉及重大治安事件线索。市公安局将含有电话举报内容及领导批示要求的接警单送往市交通委员会执法支队，请求开展协查。执法支队临聘人员夏某在将接警单送单位负责人之前，私自阅知了全部内容并用手机对接警单拍照，然后上传QQ群。经过多次转发，接警单照片迅速在微信群和QQ群中大范围传播，导致在全市一定范围内造成了不良影响和群众心理恐慌，严重干扰了地区维稳处突工作。事件发生后，有关部门对3名责任人作出不同程度的处理。

案例6： 2017年12月，某县辖区内发生一起交通事故，现场造成1人死亡、多人重伤。事故发生次日，案发地所在的镇行政执法中队中队长包某等人将事故现场的监控录像视频以及其他部门现场拍摄的收集证据视频，转发给与事故处理无关人员。相关视频流出后，在微信、微博、论坛上不断扩散，对事故调查和舆情导向造成较大负面影响。事件发生后，县纪委给予主要责任人包某政务处分，有关部门对其他责任人分别进行诫勉谈话。

工作秘密在互联网上传播和扩散，经常会迅速引发社会舆情关注，极有可能在较大范围内对具体工作以及相关机关单位工作秩序造成严重影响。这也是信息化时代泄密渠道多元化、影响复杂化的一个突出特点。

工作秘密管理现状

工作秘密是机关单位在公务活动和内部管理中产生的事项和信息，一旦泄露便会影响管理职能的正常行使，直接干扰机关单位的工作秩序。《公务员法》规定公务员应当履行“保守国家秘密和工作秘密”的义务，《法官法》《检察官法》《警察法》《海关法》等法律法规也分别有审判工作秘密、检察工作秘密、警务工作秘密和海关工作秘密的表述，但都没有在法律层面规定工作秘密的内涵和外延。与国家秘密的定密权限、定密依据、要素内容、专用标志均具有严格的法定性不同，工作秘密事项主要由各级机关单位自行确定，除个别部门和地方就工作秘密出台过专门的规范性文件外，目前尚未有全国统一的制度规范，机关单位从本地方本系统的工作惯例、业务需要出发，各自确定工作秘密管理体制、方法和措施的做法比较普遍。总体上看，当前工作秘密的保护和管理职责实际上由机关单位各自承担，缺乏专门的管理法规，也没有一个归口管理、统一指导的主管部门，存在不少薄弱环节，导致泄露工作秘密事件时有发生，给相关工作造成较大被动。

强化工作秘密管理措施

国家秘密的实质要素是关系国家安全和利益，而工作秘密涉及公务活动和内部管理，两者都是由机关单位产生，存在一定的内在联系，在外在表现上也具有很多相似之处。特别是两者都具有保密信息的一般属性，在一定时间内只限于一定范围人员知悉，而且在特定条件下可以相互转化。泄露工作秘密，不仅会直接扰乱工作秩序，严重的还会损害国家安全和利益。

加大工作秘密保护力度，强化工作秘密管理，可以在三个层面采取措施：宏观层面，需要以法规的形式明确工作秘密的定义和范围，确定和解除权限、方法和程序，保护（管理）的总体标准和基本制度，监管体制和追责机制等，尤其需要指定一个或数个部门对总体工作进行统筹指导和监管。中观层面，各部门可以研究制定专门的工作秘密事项范围，明确工作秘密的具体范围和控制范围，也可以参考司法、教育等部门保密事项范围的体例，在确定国家秘密事项的同时，也明确规定工作秘密的范围和内容。微观层面，机关单位要结合具体的工作性质、业务特点，在保密“两识”教育培训中增加工作秘密保护的内容，增强干部职工的风险意识和防范技能，同时规范、强化工作秘密的日常管理，把工作秘密管理纳入到以国家秘密为主体的信息安全保密整体工作中统一部署、集中监管、加强防范，杜绝泄露工作秘密事件的发生。

责任编辑/齐 琪

(转自《保密工作》杂志)

（二）警示案例

案例 1：学生上网求资助 被诱卖密悔已迟

案例：2012 年 4 月，某航海学校学生徐某考入某重点大学，但囿于家庭条件困难便想到在网上发帖寻求学费资助。不久，自称境外投资咨询公司研究员的“Miss Q”回帖，询问其就读院校、专业等信息，并表示愿意提供帮助。很快，徐某就收到 2000 元汇款，但“Miss Q”随即提出希望徐某帮忙搜集部队装备采购方面的期刊资料，作为资助学费的回报。徐某爽快答应，但未能在航海学校图书馆找到相关资料便作罢。5 月，徐某又主动联系“Miss Q”，对方向他提供一份“田野调研员”的兼职，月薪 2000 元，主要负责到附近的军港码头和造船厂拍摄军事设施和军舰，同时记录在修船舰的情况，并提供标有船舰方位标识的电子地图文档。案发后，徐某承认自己做“调研员”不久就意识到对方是搜集我军事情报的境外间谍，但利诱当前，难以拒绝。2013 年 5 月，徐某被国家安全机关依法审查。

案例点评：近年来，境外间谍情报机关开始针对学生群体实施大规模网络策反活动，学生涉世未深，防范心理不强，加之经常活跃在网络和社交平台，很容易成为境外势力锁定的目标。境外间谍情报机关惯以金钱诱使学生参与情报搜集、分析和传递。多数学生在网上求职或网聊过程中被境外间谍盯上，最初提供信息时可能并不知情，但部分人在觉察对方身份的情况下仍因贪利而持续配合，直至被国家安全机关依法处理。此案警示机关、单位工作人员，刺探、窃密、间谍等活动无时无刻不在我们身边发生。只有树立国家安全观念，增强防间保密意识，不为金钱所诱惑，不被贪欲所控制，坚守底线，才能远离境外间谍情报机关布下的陷阱。

（转自《警钟长鸣——窃密泄密案例警示教育读本》）

案例 2：复制密件擅遮挡 连锁效应致泄密

案例：2015 年 1 月，某县政府工作人员毛某值班当日收到上级下发的 1 份秘密级密码电报，县主管领导要求交县安监局承办。毛某未经请示批准，擅自遮挡文件头、密级标志和“密码电报不得复印”等内容，进行复印，交给县安监局工作人员刁某。刁某根据局领导要求，加上县安委办文件头，在复印室再次复制上述涉密文件，并发至安委会成员单位。该县教育体育局领取文件后上传至县教育网，造成泄密。事件发生后，有关部门给予毛某行政记过处分，给予刁某行政警告处分并调离工作岗位，对县政府办、县安监局、县教育体育局负责人分别进行通报批评和诫勉谈话。

案例点评：国家秘密标志是一种法定的文字与符号标识，用以表明所标识的物品（载体以及设备、产品等）承载内容属于国家秘密，并提示其密级和保密期限。根据保密法规定，复制涉密载体应当履行报批手续，不得擅自改变原件的密级、保密期限和知悉范围。本案中，毛某未经请示批准，擅自遮住文件头、密级标志、“密码电报不得复印”等内容进行复印，属违规操作；复印件没有国家秘密标志，导致后面收到该文件的机关、单位并不能认清其国家秘密属性，最终被不知情的教育体育局上传至互联网，造成泄密。毛某掩耳盗铃、自欺欺人的违规行为，应当引起我们的深思并切实引以为戒。

（转自《警钟长鸣——窃密泄密案例警示教育读本》）

（三）问题与对策

手机泄密，防不胜防——警惕你身边的“不定时炸弹”

随着移动互联网和智能终端的不断发展，手机的用途涵盖了生活的方方面面，成为了人们的必备品。

但与此同时，手机与个人的“无缝衔接”也给我们带来了很多烦恼。比如，近年来，有关手机泄露用户数据的信息就屡见报端，时而引发大家对“信息裸奔”的恐慌。

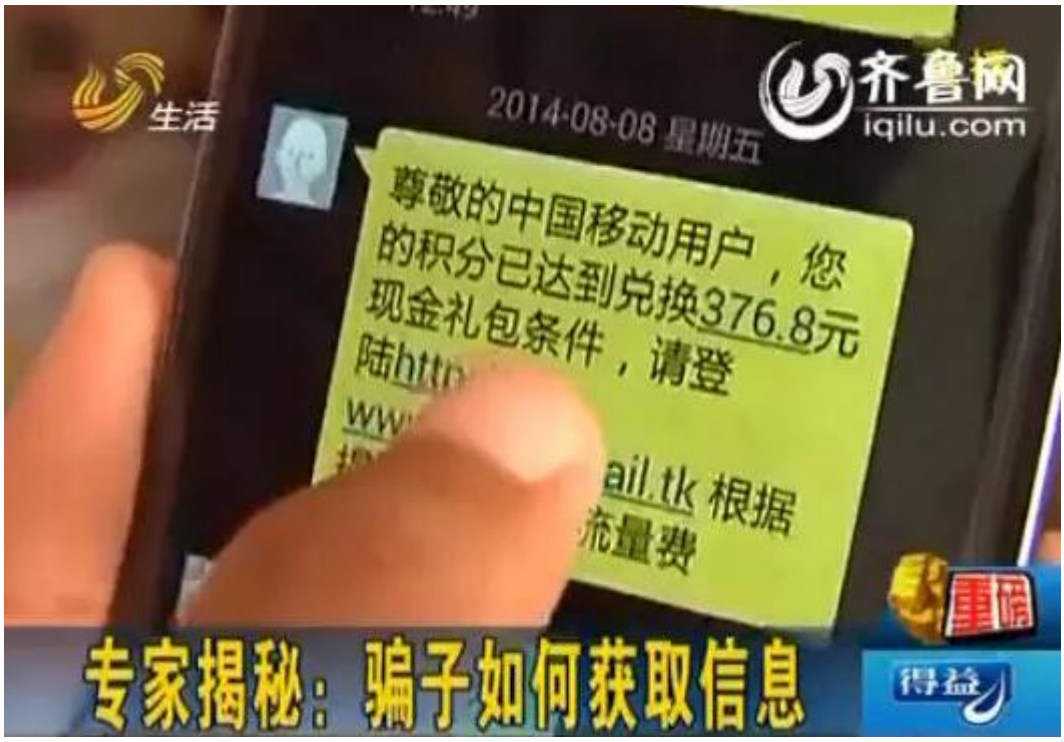
其实，手机信息泄露不仅会给公民个人造成经济损失，影响社会和谐，甚至有可能被不法分子利用，窃取国家秘密，损害国家安全和利益。

手机泄密四宗罪

1.通信网络漏洞

手机之所以泄密，很大一部分原因在于其通信网络漏洞。因为手机以无线信号方式进行通信，只要使用相应的接收设备，就可以发送并接收信息。

对此，一些不法分子可能会在涉密单位相对集中的区域，利用伪基站对周边手机信号进行接收，然后冒充运营商，给手机用户发送诈骗短信，引其上钩。



2.间谍软件植入

现在手机神通广大，大家在上网、接收彩信、下载安装文件时，都有可能被植入间谍窃密软件。这样，当我们进入涉密场所或者召开涉密会议时，手机就变成了一个个可怕的“窃听器”“偷录机”。

另外，还有一些涉密人员，使用他人赠予的手机，也有可能被别有用心的人安装上窃密软件，从此“城门大开”。

早在 2015 年，美国“棱镜门”揭秘者爱德华·斯诺登就曾在采访中曝光英国间谍

使用“蓝精灵组件”侵入他人手机，以盗取照片、数据并进行远程监听，一时间国际舆论哗然。

3.定位功能隐患

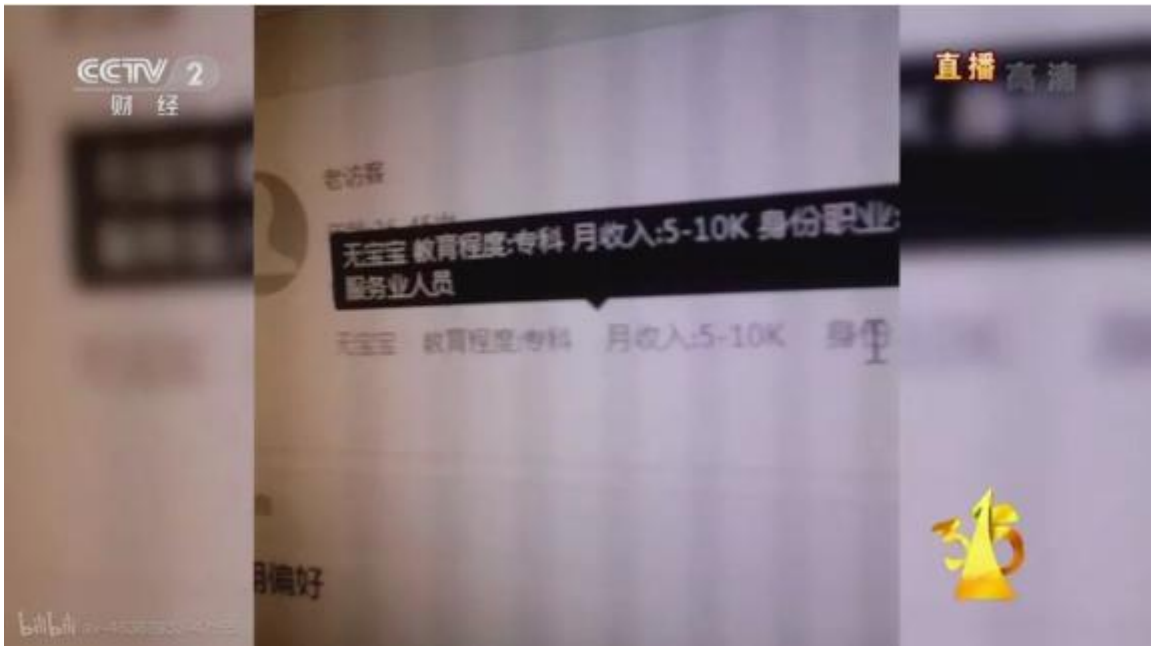
手机除了正常通信信号被接收、安装间谍软件被监听外，其定位功能也有可能造成涉密人员和重要涉密单位位置信息泄露。不法分子可能通过手机芯片进行定位，这样可以追踪到涉密人员，甚至能够通过手机掌握到涉密单位的坐标、海拔高度、精确范围。

2011 年，卡扎菲在苏尔特近郊被俘后遭击毙。很多人不知道，将卡扎菲逼进绝路的是手机泄密。英国《每日电讯》指出，正是卡扎菲拨通手机被美军定位，从而彻底暴露了自身行迹。

4.无线网络陷阱

当手机 WiFi 功能开启，就能自动接入附近无口令设置的无线网络，为黑客入侵手机创造便利条件。另外，不法分子也可以通过 WiFi 接入点对涉密单位进行定位。

2019 年 3·15 晚会上就曾曝光一款通过 WiFi 窃取他人隐私的“神器”——探针盒子。该盒子即“WiFi 探针”，能够基于 WiFi 探测技术，获取 90 米范围内手机访客的个人信息：婚姻状况、收入、就业年限、教育程度一目了然。



加强保密管理

小小手机关系着国家安全，除了严格落实国家有关手机保密管理的相关规定，涉密单位还应当从哪些方面加强具体管理，让手机不再成为泄密的“不定时炸弹”呢？

一、完善制度管理。各涉密单位应当根据自身实际情况，出台手机管理制度，如指定专人对手机保密进行监督管理，对在手机保密管理方面成绩突出的工作部门给予奖励等。

二、加强技术防护。有关单位还应当加强保密技术防护措施，如在涉密会议召开期间和要害部门部位日常工作中开启电磁干扰和防护功能；为单位配备电磁屏蔽室、

手机屏蔽柜、手机屏蔽袋等；采用手机探测技术手段检查手机是否被带入涉密场所，有效避免手机泄密。

三、强化保密意识。心不设防则防不胜防，普及手机窃密手段和泄密危害也是单位加强手机保密管理的重要举措。通过有效宣传措施，普及手机保密常识，强化保密意识。使涉密人员在使用手机上网、购物、社交时，提高防范能力和警觉意识，杜绝谈论与工作有关的涉密信息，避免造成无意识泄密。（转自《保密观》）

（四）自测试题

保密小测试

判断题

1 按照有关规定，业务工作接受上级业务部门垂直管理的单位，保密工作以上级业务部门管理为主，同时接受地方保密行政管理部门的指导。（ ）

2 保密法及其实施条例、公司法、国家保密标准、相关司法解释都是我国保密法律制度体系的重要组成部分。（ ）

3 为境外窃取、刺探、收买、非法提供国家秘密、情报罪，背叛国家罪，非法获取国家秘密罪，过失泄露国家秘密罪都属于我国刑法规定的与保守国家秘密有关的罪名。（ ）

4 保密干部，是依照保密法律规定，组织开展保密工作的人员，是开展保密工作的主体，是做好保密工作的组织保证。甲乙两人对保密干部范围的认定产生争论。甲认为，保密干部包括各级保密委员会组成人员、各级保密行政管理部门工作人员、各级保密工作机构的专兼职工作人员。乙认为甲的观点不对，保密干部不但包括甲主张的三类人员，还包括机关单位涉密岗位的工作人员。甲的观点是正确的。（ ）

单项选择题

5 国家秘密的变更是指（ ）的变更。

A.密级、保密期限、密点　　B.保密期限、知悉范围　　C.密级、保密期限、知悉范围

6 某中央机关印发1份机密级文件，国家秘密标志为“机密★10年”，8年后，按照保密法律法规的规定，该涉密文件需要降低为秘密级国家秘密。那么，该涉密文件的保密期限最长还有（ ）年。

A.10年　　B.2年　　C.12年

7 甲机关向乙机关去函征求对某机密级国家秘密文件的意见，乙机关只有秘密级国家秘密定密权，没有机密级国家秘密定密权。乙机关复函时涉及了该机密级国家秘密的实质内容，复函应当（ ）。

A.请上级机关定密　　B.作出秘密级国家秘密标志　　C.作出机密级国家秘密标志

8 按照保密法律法规的规定，某机关执行中央下发的秘密级文件过程中产生的涉密文件资料，应当确定为（ ）。

A.秘密级国家秘密　　B.机密级国家秘密　　C.内部资料

南京航空航天大学保密宣传教育参考资料

（2021 年第 1 季度）

参考学时：2 小时

（一）举案说法

警惕！这些政府信息泄密，只因一件事没做好……

互联网时代，信息公开正日益成为机关单位密切联系群众的窗口、桥梁。但与此同时，时有发生的泄密事件提醒我们，要重视信息公开的保密审查，避免因泄密给政府工作带来负面影响，甚至给国家安全造成损害。

泄密隐患引人忧

案例 1：某市政府网站刊登秘密级文件。经查，该市某机关起草并印发了 1 份秘密级文件。为督促大家更好地落实文件精神，市政府工作人员刘某未履行保密审查程序，擅自将涉密文件上传至市政府网站，造成泄密。

案例 2：某区门户网站刊登机密级文件。经查，在开展某专项工作期间，该区委宣传部副部长郭某向组织部借阅上级下发的包括机密级文件在内的工作资料，阅后交给宣传部工作人员高某。高某未经郭某允许，也未履行信息公开审批手续，擅自隐去保密标识，将文件扫描后发布在该区门户网站，造成泄密。

案例 3：某市安监局网站刊登机密级文件。经查，某年元旦前（12 月 31 日下午），该局收到两份通知（各带 1 份机密级附件）。考虑到临近元旦放假，书面转发不能及时发放到位，该局某部门主任李某安排技术科副科长祁某通过网站转发文件。祁某仅对通知的内容进行了核实，却未核实附件是否涉密，直接将通知刊登在单位网站上，造成泄密。

保密审查未重视

以上案例之所以发生，均因行为人在将信息公开前，未严格落实保密审查制度，充分反映出个别机关单位信息公开保密审查工作存在较大隐患。

1. 保密审查成虚设。案例 1、2 中，相关单位虽制定了保密审查制度，但在操作中没有严格执行，结果导致工作人员“一顿操作猛如虎”，直接把涉密文件上传到网站。这并非个例。实践中，很多单位非常重视网站的内容建设，狠抓信息发布更新，有些部门为了赶进度、充内容，不严格履行先审查后发布的正规流程，而是边发布边审查，甚至只发布不审查，直接把单位工作动态、内部文件甚至从其他部门转载的信息上传至互联网，造成泄密。

2. 保密审查存漏洞。政府信息公开的保密审查是一项政治性、政策性和技术性都很强的工作，理应引起高度重视。但个别单位却存在着审查人员责任心不强、保密审查走过场的情况。如有的只审查文件标题或者文件首页有没有国家秘密标识，不审查文件内容；有的只看文件正文，不审查附件。案例 3 中祁某仅核实通知而不看附件，结果把涉密附件上传至网络，可见其保密审查完全流于表面。

3. 保密知识太匮乏。以上 3 起案例背后，折射出相关单位的工作人员缺乏保密基本常识。特别是案例 2 中，高某明知文件为机密级国家秘密，还擅自隐去文件保密标识以便“成功入网”，“神操作”实在让人震惊。

审查制度严落实

亡羊补牢，为时未晚。机关单位要做好政府信息公开工作，须特别重视并落实保密审查制度，尤其应做到如下几点：

1.严格审查流程。要本着“谁公开、谁负责、谁审查”“先审查、后公开”和“一事一审”原则，严格履行审批程序，认真落实审批责任，切实做到人人尽责、层层把关，及时排除泄密隐患和风险。

2.明确审查重点。明确将转发文件、扫描文件、汇编文件、转载文件、通知附件等作为重点审查对象，确保对拟公开信息逐页审查、逐份审查，做到不留死角和漏洞。

3.加强检查查处。定期对机关单位信息公开工作进行保密检查，对存在问题的，发现一起，整改一起，严格责任人员处理，并加强通报力度，以便其他单位能够反观自照，及时发现工作中的薄弱环节和突出问题，有针对性地改进提升。

（转自《保密观》）

（二）警示案例

一名大学生走向深渊的警示

□李宇斐

2018年3月26日，在某大学校园内，有关部门工作人员对在读研究生薛玲（化名）出示证件并予以拘传，一阵惊愕和恐慌过后，她似乎意识到了缘由，反问“是因为Charles的事情吗”，随后便被带走审查。

一

从正式入学开始，薛玲就展现出极强的独立自主能力，与其他同学不同，出身贫寒的她不仅要完成学校统一安排的课程、参与导师的科研项目，还要挤出时间去做兼职来维持自己的各种花销。她不在意别人的看法，一心想着好好珍惜这3年的时光，为未来争取一个好前程，不辜负父母和乡亲们对自己这只“山窝里飞出的金凤凰”的期望！

2017年8月的一天，薛玲在某微信兼职群里看到有人发布“港口船只统计工作，一周3到4次，一次200元”的招聘信息，便与对方联系，发布人“Charles”自称某市政府部门工作人员，主要做港口开发工作，需要统计各码头的船只数量作参考，请薛玲每周分3次对停靠在某码头附近的军船和商船进行拍照，附上相关数量信息，就可以领取报酬，并强调要注意保密，不要被人发现。薛玲有所迟疑，不懂为什么不能被人发现，“Charles”解释只是记录船只的数量，不用害怕，薛玲认为这份兼职报酬还算可观，并且不占用太多时间，便打消疑虑，添加了“Charles”的微信，接受其进一步的工作安排。

二

次日傍晚，按照“Charles”的指导，薛玲早早来到码头附近，仔细勘察了周边地形后，进入六一广场边上一栋大楼的8楼，找到一个靠窗位置，趁没人注意，拿起手机对着码头进行拍摄，数清楚船只的数量，一并发送给“Charles”。薛玲很快便收到“Charles”转来的200元红包，她不禁喜出望外，没想到任务竟如此简单！

一直到12月上旬，薛玲保持每周3次的拍摄频率，“Charles”对她也越来越信任，逐渐增加了任务要求，不仅对拍摄码头军舰的角度和清晰度有了特殊要求，还另外让其拍摄军事、航天、航空之类的期刊封面，强调要不公开发行的内刊。然后，其谎称自己在国外出差，不方便使用微信，支付报酬的方式也改成了支付宝。“Charles”指导薛玲注册了多个英文邮箱，并传授她加密发送的方法，要求连接公共Wi—Fi把照片发给自己。为此，薛玲在学校图书馆寻找相关期刊，还特意办理了公共图书馆的读者证，拍

了五六十个期刊封面给“Charles”，再根据其要求，对特定期刊详细内容进行拍摄。

随着时间推移，“Charles”所提要求不断增多，薛玲越来越怀疑其并非政府部门工作人员，而是新闻里看到过的境外情报人员。此时，薛玲已经麻木，虽然心里有点恐慌，但弄不清事情的严重程度，怀着侥幸心理越陷越深，直到2018年3月被带走审查。

经查，“Charles”真实身份为境外情报人员，薛玲为其提供的照片共涉及1项机密级国家秘密，累计获取酬劳28000余元。2019年12月，薛玲被以为境外刺探、非法提供国家秘密罪判处有期徒刑5年，剥夺政治权利1年，没收财产人民币3万元。

三

薛玲的光明前程彻底被打破，究其原因，最重要的还是缺乏基本的保密意识和保密常识。她的悲剧也并非个例，抛开其高等教育背景不谈，薛玲的惨痛教训只是为数众多的体制外人员泄密案件的缩影，一方面反映出部分机关单位保密管理工作存在薄弱环节，给了不法分子窃取国家秘密的可乘之机；另一方面，也提醒我们，必须堵塞“体制外人员”的泄密漏洞，切实增强公民的保密意识，让保密观念深入人心，进一步筑牢安全保密防线。

加强全民保密“两识”教育。保密之要，关键在人。《宪法》明确规定，中华人民共和国公民必须遵守宪法和法律，保守国家秘密。保密法也规定，每个公民都有保守国家秘密的义务。当前，公民接受保密知识普及和保密意识培养的渠道、体系尚不完善，对保密知识和保密规定知之甚少的情况还较为突出，不少人认为保守国家秘密只是党政机关、企事业单位等体制内人员的职责和义务，这与保密教育的覆盖面不无关系。因此，必须拓宽保密宣传教育渠道和范围，加强公民保密“两识”教育。一方面，借助各媒体平台加强对典型失泄密案例的报道，以案说法，切实提高广大公民的保密意识，让公民认识到保密与自身息息相关。另一方面，加大保密宣传普及力度，让保密知识进课堂、进社区，逐步深入每个公民心中，推动养成良好的保密习惯。

强化重点领域保密管理。近年来，重大军事设施、军事基地频频遭到刺探窃密，警示相关部门必须进一步加强保密管理。保密法规定，军事禁区和属于国家秘密不对外开放的其他场所、部位，应当采取保密措施，未经有关部门批准，不得擅自决定对外开放或扩大开放范围。具体来说，一方面，要制定针对性强、行之有效、切实管用的规章制度，堵塞泄密漏洞，对涉密场所和敏感地带进行全方位监管，不给不法分子窃取国家秘密的可乘之机；另一方面，要加强日常监督检查，通过定期组织保密检查发现问题漏洞，严肃问责体系，开展整改补救。

加大责任人员惩处力度。保密管理要“抓早抓小”，发挥保密检查、通报、问责的“利剑”作用，树立保密法纪威严，将泄密风险消除在萌芽状态。一方面，机关单位要建立完善的保密责任追究体系，严格落实惩戒规定，对违反保密制度的行为要坚持原则，严肃追责，以此推动保密管理制度落到实处；另一方面，有关部门要进一步完善相关法律法规，加强对社会人员、体制外人员保密违法行为的监管和惩处力度，同时也提醒、引导相关社会单位增强保密意识。

责任编辑／孙战国

(转自《保密工作》杂志)

回眸·2020

2020年度国内窃密泄密事件盘点

□本刊综合

2020年可谓风云诡谲。这一年，新冠肺炎疫情蔓延全球，大国竞争复杂激烈，地区热点乱变交织，不断出现的变数使保密工作形势愈加严峻复杂。回首本年度主要媒体公布的诸多窃密泄密事件，几大特点值得关注。

远程办公泄密高发

年初，新冠肺炎疫情拉动了远程办公需求。虽然在应用场景多元化方面，远程办公有无法比拟的优势，但其信息安全隐患也不可小觑。特别是一些机关单位工作人员，在讨论工作时不加注意，把涉密敏感信息一并“上云”，造成了工作秘密、国家秘密的泄露。

比如，广西南丹县疾控中心熊某、工作人员区某泄露疫情防控工作材料问题。1月26日，熊某在未经审批的情况下，擅自将该县新冠肺炎疫情防控材料通过QQ发送到本单位工作群。区某发现这一信息后，随即将原文转发到其个人微信群，并被其他群内成员转发扩散，造成一定社会影响。无独有偶。2月1日，内蒙古乌海市一名街道工作人员在开车巡查过程中，收到微信文件“关于做好与某人密接人员排查的函”后，想把此函通过微信转发给街道主要负责人，但因当时正在开车，点击错误，把文件发到了朋友群中，虽然发现后立即撤回，但仍给工作造成了被动。

据统计，湖南、陕西、宁夏等多地都曝出类似事件。事后，当事人虽然被严肃追责，但其泄密行为引发的不良影响难以挽回。

间谍活动仍然猖獗

据报道，今年国家安全机关组织实施“迅雷-2020”专项行动，破获了数百起间谍窃密案件。随着我国综合国力不断提升，境外间谍情报机关对我国的情报渗透活动也更加活跃。他们以我国党政机关、军工企业和科研院所等单位的核心涉密人员为目标，千方百计进行拉拢策反，开展窃密破坏活动。

其中，张建革案十分具有典型性。某军工研究所工作人员张建革，在赴国外访学的过程中遭到间谍策反。该间谍多次为其解决生活问题，不仅用豪华轿车带他外出旅游、去高档餐厅用餐，为他提供高薪兼职工作，还允诺要为其女儿赴国外留学和取得居住权提供帮助。得知对方间谍身份后，张建革在巨大的利益面前仍然选择卖密，在回国后立即开始搜集军工情报，导致我国多种还没有投入现役、没有列装的武器装备，就这样被泄露出去。最终，张建革因犯间谍罪被法院判处有期徒刑十五年。

涉密人员叛逃首度披露

今年，我国国家安全机关还首次公布了多起涉密人员叛逃案件。

王丕宏曾任我国某航空研究所副总设计师，其妻赵汝芹同样曾是该研究所的技术人员，两人均掌握国家秘密。从1999年起，王丕宏和赵汝芹就开始预谋移民某西方国家，他们向单位隐瞒情况，伪造材料，私自申领因私护照，并通过移民中介公司办理了手续。2002年春节期间，两人利用探亲的机会，携子秘密前往该西方国家，并取得该国国籍。王丕宏夫妇消失后，国家安全机关迅速将他们纳入工作视线，侦查发现，王丕宏到达国外后，一直在该国从事航空领域相关工作。由于掌握我国大量科研机密，又在国外从事相同领域工作，王丕宏夫妇的叛逃，对我国军事安全、科技安全造成重大威胁。2017年，二人用外籍身份入境，被国家安全机关拿获。河南省洛阳市中级人民法院以叛逃罪判处王丕宏有期徒刑三年，赵汝芹有期徒刑两年。

王丕宏夫妇到案后不久，曾任我国某国防军工研究院技术人员的苗敬国也因叛逃罪被国家安全机关抓获。作为重点涉密人员，他于2003年擅自携妻儿离境赴某西方国家滞留不归，并于2007年加入该国国籍。苗敬国因叛逃罪被判处有期徒刑两年。

“学者”沦为窃密中间人

在上述“迅雷-2020”专项行动中，有关部门还抓获了一批台湾间谍，引起社会广泛关注。

比如蔡金树案。某天，一名自称郭佳瑛的台方间谍与早年在大陆求学、自20世纪90年代开始从事两岸交流活动的台湾学者蔡金树取得联系，获得对方信任后，郭佳瑛利用蔡金树的人脉成立协会和电子媒体，以聊天、约稿等方式试图向大陆人员套取情报。据统计，此案涉及大陆涉台工作部门人员、重要智库专家、知名媒体记者等50多人。2020年7月，蔡金树因间谍罪被判处有期徒刑四年。

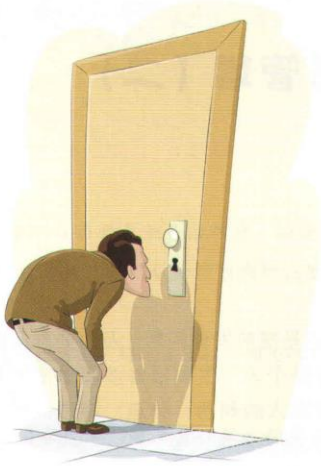
施正屏案。施正屏原为台湾师范大学教授，后在台湾“国安局”间谍周德益的劝服下成为其搜集情报的工具。在搜集情报的过程中，周德益根据情报的重要性给施正屏付费，从几万到十几万不等。在利益的诱惑下，施正屏在2005年到2018年之间以台湾学者身份到大陆搜集情报，内容涉及政治、经济、两岸关系、政策法规等多个领域，通过公开套取、打探刺探、金钱收买、物质利诱等手段获取“一带一路”、亚太战略等方面数据和内容，对我国国家安全和利益造成损害。

有关部门特别指出，像蔡金树、施正屏这样的学者已经成为情报机关经常发展利用的对象。

窃密目标转向公众

境外情报机构还利用各种手段试图通过社会公众窃取我国家秘密。

2020年4月，刚刚来到大连务工的赵某在网上查找招聘信息时，与一名自称姓叶的女子取得联系。对方说自己是搞城市规划设计的，急需招聘兼职人员来帮她拍摄一些城市风景照，并给出了日薪200元人民币的工资待遇。



工作第一天，在叶某的遥控指挥下，赵某先后来到大连的港口、造船厂周边拍摄照片，并记录下沿途的地理环境，通过手机发送给叶某。随着时间的推移，叶某布置的任务不断加码。为了方便拍摄港口中停泊军舰进行维护的照片，叶某甚至要求赵某到造船厂周边的高层公寓租住，还称如果赵某找机会进入造船厂工作，每月将获得更多的报酬。今年4月中旬，赵某无意间看到电视台播放的全民国家安全教育日节目后，突然对叶某的身份产生了怀疑。经过一番思想斗争，赵某在家人陪同下主动向国家安全机关自首。鉴于赵某主动投案，且尚未对我国国家安全造成实质危害，国家安全机关依法免于追究其刑事责任。

对此，有关部门表示，针对受欺骗、受胁迫从事间谍活动且能主动彻底交代问题、认罪悔罪的中国公民，国家安全机关将坚持教育为主、惩治为辅，进一步凝聚全社会维护国家安全的强大合力。

情报攻防成舆论焦点

近年来，国内外媒体有关间谍情报活动的报道越来越多。特别是香港国安法推出后，一些西方人士和媒体加大力度炒作“干涉渗透影响”和“间谍威胁”，其言论和报道或明或暗指向中国、俄罗斯、伊朗等国。特别是“五眼联盟”成员之一澳大利亚，更是把自己包装成国际间谍情报活动的“受害者”。

但据媒体披露，近年来澳大利亚从未停止过对别国的间谍情报攻势，我国曾多次破获澳情报人员间谍活动。澳方渲染“中国间谍威胁”的言行，更是贼喊捉贼。

据悉，2018年我国执法部门对一起间谍案件进行侦查时，在境内发现并现场抓获澳情报安全部门间谍，当场起获用于间谍活动的器材、经费以及刚刚搜集的情报资料。而除在中国境内实施间谍情报活动外，澳情报安全部门在其本土和第三国也针对华人开展策反活动。有关部门曾破获案件，澳情报安全部门将一名华人策反后，安排其到位于堪培拉附近的斯旺岛秘密基地进行专业的间谍培训，之后又将他派遣回中国大陆搜集情报。澳情报安全部门甚至在驻华大使馆设立了北京情报站，负责管理在华情报活动，兼管澳在日本、韩国、蒙古国等地的情报活动。

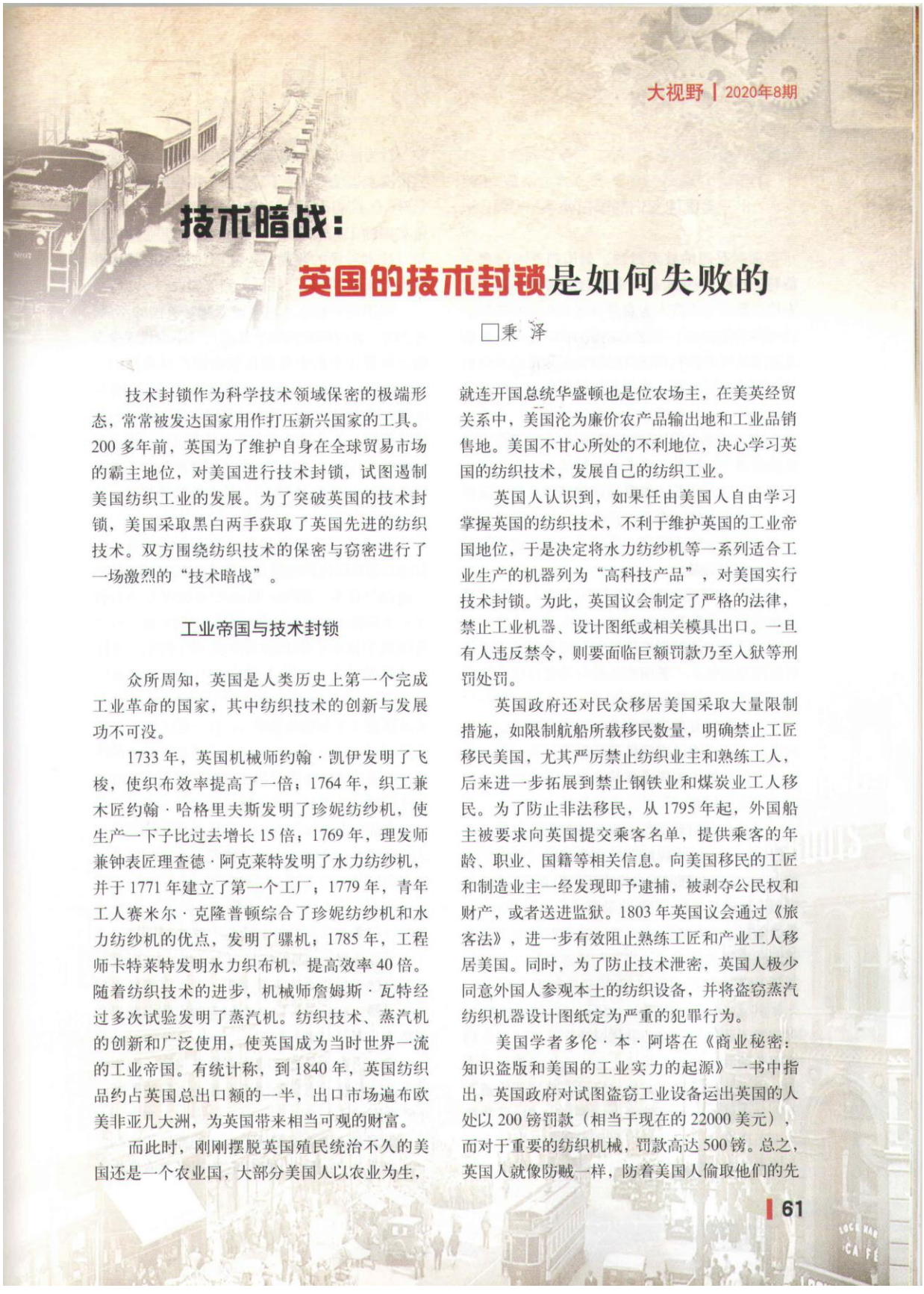
消息指出，澳情报安全部门对中国大肆开展技术窃密活动由来已久。20世纪八九十年代，中国驻澳大使馆在修建过程中，澳情报安全部门就暗动手脚，在建筑内部安装了大量窃听器材，包括当时最先进的拾震式窃听器和高频、低频电磁感应式窃听装置，几乎覆盖了每层楼板，甚至连使馆储藏室也未能幸免，以至于中国政府只能在澳重建大使馆。近年澳情报安全部门对中国驻澳机构和人员的监控力度越来越大，并且大规模约谈、骚扰在澳华人，要求提供华人社区和中国使领馆的情报，甚至将有些人发展成情报线人。据有关部门掌握，在澳华人学者冯崇义就是澳情报安全部门发展利用的线人。冯崇义就职于悉尼科技大学，常年在境外反华媒体上充当“中国问题专家”对我国进行污蔑攻击，2017年，外媒还曾炒作冯崇义回国返澳时被“扣押”的消息。

总而言之，随着我国加速崛起，国内外信息安全保密形势不容乐观。提高失泄密防范能力，加强全民保密法治教育迫在眉睫。

责任编辑／齐 琪

(转自《保密工作》杂志)

（三）保密大视野



技术暗战：英国的技术封锁是如何失败的

□秉 泽

技术封锁作为科学技术领域保密的极端形态，常常被发达国家用作打压新兴国家的工具。200多年前，英国为了维护自身在全球贸易市场的霸主地位，对美国进行技术封锁，试图遏制美国纺织工业的发展。为了突破英国的技术封锁，美国采取黑白两手获取了英国先进的纺织技术。双方围绕纺织技术的保密与窃密进行了一场激烈的“技术暗战”。

工业帝国与技术封锁

众所周知，英国是人类历史上第一个完成工业革命的国家，其中纺织技术的创新与发展功不可没。

1733年，英国机械师约翰·凯伊发明了飞梭，使织布效率提高了一倍；1764年，织工兼木匠约翰·哈格里夫斯发明了珍妮纺纱机，使生产一下子比过去增长15倍；1769年，理发师兼钟表匠理查德·阿克莱特发明了水力纺纱机，并于1771年建立了第一个工厂；1779年，青年工人赛米尔·克隆普顿综合了珍妮纺纱机和水力纺纱机的优点，发明了骡机；1785年，工程师卡特莱特发明水力织布机，提高效率40倍。随着纺织技术的进步，机械师詹姆斯·瓦特经过多次试验发明了蒸汽机。纺织技术、蒸汽机的创新和广泛使用，使英国成为当时世界一流的工业帝国。有统计称，到1840年，英国纺织品约占英国总出口额的一半，出口市场遍布欧美非亚几大洲，为英国带来相当可观的财富。

而此时，刚刚摆脱英国殖民统治不久的美国还是一个农业国，大部分美国人以农业为生，就连开国总统华盛顿也是位农场主，在美英经贸关系中，美国沦为廉价农产品输出地和工业品销售地。美国不甘心所处的不利地位，决心学习英国的纺织技术，发展自己的纺织工业。

英国人认识到，如果任由美国人自由学习掌握英国的纺织技术，不利于维护英国的工业帝国地位，于是决定将水力纺纱机等一系列适合工业生产的机器列为“高科技产品”，对美国实行技术封锁。为此，英国议会制定了严格的法律，禁止工业机器、设计图纸或相关模具出口。一旦有人违反禁令，则要面临巨额罚款乃至入狱等刑罚处罚。

英国政府还对民众移居美国采取大量限制措施，如限制航船所载移民数量，明确禁止工匠移民美国，尤其严厉禁止纺织业主和熟练工人，后来进一步拓展到禁止钢铁业和煤炭业工人移民。为了防止非法移民，从1795年起，外国船主被要求向英国提交乘客名单，提供乘客的年龄、职业、国籍等相关信息。向美国移民的工匠和制造业主一经发现即予逮捕，被剥夺公民权和财产，或者送进监狱。1803年英国议会通过《旅客法》，进一步有效阻止熟练工匠和产业工人移居美国。同时，为了防止技术泄密，英国人极少同意外国人参观本土的纺织设备，并将盗窃蒸汽纺织机器设计图纸定为严重的犯罪行为。

美国学者多伦·本·阿塔在《商业秘密：知识盗版和美国的工业实力的起源》一书中指出，英国政府对试图盗窃工业设备运出英国的人处以200镑罚款（相当于现在的22000美元），而对于重要的纺织机械，罚款高达500镑。总之，英国人就像防贼一样，防着美国人偷取他们的先

进技术。

美国国父们的黑白两手

面对英国的技术封锁，美国当然不会束手待毙。1789 年夏天，华盛顿总统收到一封秘密来信。英国一位商人有意将自己在英国的纺织厂迁至弗吉尼亚州，他愿意出资 1000 英镑，采购先进的纺织机器和其他仪器设备，只要当地政府帮忙解决雇工问题，他还可以带来熟练工匠培训年轻学徒。

这对于致力于突破英国技术封锁的华盛顿总统而言，无疑是一个天大的好消息，他立即致信弗吉尼亚州州长，着重强调了新技术对美国新兴工业的重要性，希望予以大力支持。同时，华盛顿总统还在信末强调，要注意保密，避免给英国商人惹来麻烦。

然而，华盛顿总统的希望落空了。弗吉尼亚州参议院将此事拒之门外，州众议院态度模糊不定。联邦司法部部长伦道夫和国务卿杰斐逊先后提醒华盛顿："英国商人的行为已违反英国的限制性规定，您最好离这事远一点儿。"不得已，华盛顿总统只好再次致信弗吉尼亚州州长，口气有所转变："据说出口机器是犯罪行为……以秘密方式诱使他国国民违反其法律，对我合众国总统而言有失体面。"

美国首任财政部部长汉密尔顿则没有华盛顿总统的顾虑，他旗帜鲜明地主张奖励"偷窃"。1791 年，汉密尔顿向国会提交了一份重要文件《关于制造业的报告》，主张奖励那些给美国带来"非凡价值进步和秘密"的人。这其实就相当于呼吁美国政府资助技术"偷窃"和机器走私。在杰斐逊等人阻挠之下，国会没有接受这份报告。

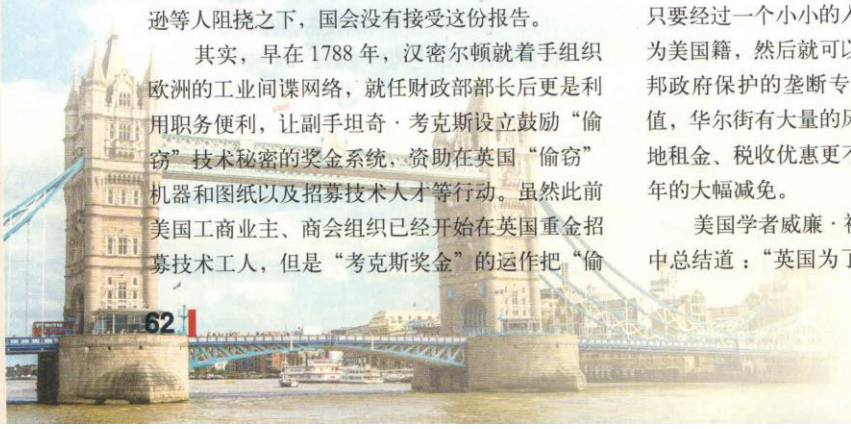
其实，早在 1788 年，汉密尔顿就着手组织欧洲的工业间谍网络，就任财政部部长后更是利用职务便利，让副手坦奇·考克斯设立鼓励"偷窃"技术秘密的奖金系统，资助在英国"偷窃"机器和图纸以及招募技术人才等行动。虽然此前美国工商业主、商会组织已经开始在英国重金招募技术工人，但是"考克斯奖金"的运作把"偷窃"行为提升到了政府层面。美国的工业间谍甚至把汉密尔顿的《关于制造业的报告》印制了上千份，在英国广为散发，宣传新大陆的美妙生活，让英国的工人们了解美国发展纺织工业的决心及对技术移民的奖励……意图将英国的技术和熟练工源源不断地"移民"到美国去。

美国的种种不光彩手段激起了英国的不满。英国的一家反移民报纸曾报道："不少代理像泰晤士河岸上空的水鸟在这里盘旋，对我们的工匠、机械师、手艺人等如饥似渴，他们正想带领这些人踏上美国。"因此，英国政府加大了对移民的管制，并对美国政府提出严正抗议。面对英国的抗议，为了国家"体面""尊严"，美国政府表面上停止了对"偷窃"技术的公开奖励，转而推出专利法。

在汉密尔顿的鼓动下，美国很快修订了专利法，强调以保护知识产权的名义，隐晦地鼓励"偷窃"技术。例如，该法明确规定专利的授予对象只能是美国人。从中世纪后期开始，欧洲各国授予技术型专利的对象都不分国籍，美国反其道而行之，实际上就是企图连人带技术一起"偷"。同时，该法规定专利申请人按照程序要求递交文件并缴纳费用后，由一般工作人员审核后即可授权，无须高级官员审核专利申请的内容。也就是说，一般专利法通用的审查制被改为了注册制。这就意味着无论是通过什么手段获得的技术都可以得到美国政府的保护。在这部专利法的鼓励下，美国国内迅速掀起了全民山寨英国技术的风暴。

当时，美国推出了针对来自英国技术创业者的"一条龙"服务：只要你有技术（不管通过什么手段获得），哪怕只是个穷光蛋，来到美国，只要经过一个小小的入籍宣誓，就可以直接变更为美国籍，然后就可以在美国申请专利，获得联邦政府保护的垄断专利权。根据技术的市场价值，华尔街有大量的风险资本参与投资，至于土地租金、税收优惠更不用说，都是直接给予若干年的大幅减免。

美国学者威廉·福斯特在《美洲政治史纲》中总结道："英国为了维持它对纺织业的垄断，



曾经先后在1765年和1774年颁布法令，禁止受过训练的工人移民到美国去，但是美国资本家很快就克服了这些困难，从英国引诱去了一些技工，并偷运了一些机器与图样到美国，抄袭英国的机器并加以改良。”

“英雄”还是“小偷”

在美国黑白两手策略的攻击下，英国的技术封锁逐渐崩溃。其中塞缪尔·斯莱特和弗朗西斯科·洛厄尔是导致英国技术封锁崩溃的两个关键人物。

1768年，塞缪尔·斯莱特出生在英国德比郡一个富裕的农民家庭。14岁时，斯莱特来到父亲的好朋友斯特拉特的纺织工厂里当学徒工，一干就是整整7年。斯莱特所在的纺织工厂就是水力纺纱机的发明人理查德·阿克莱特与斯特拉特合作开办的。因此，在斯特拉特的纺织厂里，斯莱特看到的是世界上最先进的纺纱机器。凭借着勤奋好学，斯莱特很快全面掌握了阿克莱特水力纺纱机技术，并积累下了大量丰富的实践经验，成为纺织工厂里最优秀的纺纱工人。

斯莱特21岁时，学徒生涯结束。老板任命他为纺织厂的高级管理人员并参与新工厂的设计和建造。然而，斯莱特野心勃勃，丝毫不满足于寄人篱下。一天，当听说大洋彼岸的美国愿意支付高昂奖金给阿克莱特水力纺纱机的建造者，他非常兴奋，决定到美国去开辟人生的新天地。鉴于英国技术封锁的严格，斯莱特深知移民美国一旦败露，自己将会被投入监狱。于是，他凭借着惊人的记忆力，花费大量时间，牢牢记住阿克莱特水力纺纱机的每一个细节，并周密计划，连家人都没有告诉，化装成英国农业工人的模样登上了驶往美国的轮船。

1789年11月，斯莱特顺利抵达纽约，很快便和罗德岛纺织集团的布朗家族一拍即合。当时布朗家族正陷入纺织生产的困境，大量的纺纱机械设备不能正常运转。斯莱特花费了大约一年的时间，调用记在头脑中的技术资料，反复试验，终于成功复制出了阿克莱特水力纺纱机。几年之后，有了资金的斯莱特与布朗家族分道扬镳开始自己创业，先后建立了13家自己的工厂，打造了一个庞大的纺织帝国，成为著名的商业大亨和百万富翁。

稍晚一些，波士顿商人弗朗西斯科·洛厄尔为美国成功“偷窃”了英国纺织业的另一项“高科技产品”——卡特莱特水力织布机。洛厄尔在开展国际贸易业务时结识了不少英国纺织商人，建立了彼此信任的密切关系。1810年，洛厄尔赴英国养病。在此期间，他经常参观各地的纺织厂。这位哈佛大学数学专业的毕业生，拥有非凡的记忆力。他和斯莱特一样，每次参观时都牢牢记住机器结构的任何一个细节，回到住处时在图纸上画出机器设计图。到回国前夕，他已经把卡特莱特水力织布机的技术构造资料深深印刻在脑海中。

1812年，在销毁所绘制的全部图纸后，洛厄尔启程回国。英国政府怀疑洛厄尔很可能是工业间谍，命令英国海军拦截了其所乘船只。但令英国人大失所望的是，他们将洛厄尔携带的行李及所乘船只翻了个底朝天，仍一无所获，不得不放人回国。随后，洛厄尔和其他机械师一起，凭借牢记的技术资料，在美国迅速复制出卡特莱特水力织布机，并建立了美国第一家“综合”纺织厂，使原棉转化为成品布的全部流程都在一个工厂内进行。在接下来的几年里，他们完成了由斯莱特发起的美国纺织业生产革命。

如今，在美国，斯莱特被誉为“美国工业革命之父”，洛厄尔被视为改变美国纺织工业历史的“英雄”，被美国人所铭记。而在英国，斯莱特则成了“叛徒”的代名词，洛厄尔被看作逍遥法外的“小偷”。

（参考资料：《商业秘密：知识盗版和美国的工业实力的起源》《美洲政治史纲》《英美知识产权风云录：强者的皇冠与弱者的武器》《欧美工业革命中科学技术的引进与利用》《走私者之国：非法贸易如何造就美国》《美国如何“偷师”英国技术》等）

责任编辑/李 杰

(转自《保密工作》杂志)

（四）自测试题

保密小测试

判断题

1 小张因工作调整调动到其他单位，处室负责人叮嘱其对本人持有的办公设备、文件资料等进行清理移交，小张认为只要将办公电脑及“红头文件”整理归档、清理移交即可。（ ）

2 某机关单位工作人员为了撰写领导讲话，摘录、引用了一份机密级文件的有关涉密内容，在这份讲话稿完成后，应重新确定密级、保密期限和知悉范围，但不得低于机密级。（ ）

3 机关单位应当定期审核所确定的国家秘密，对需要延长保密期限的，应当在原保密期限届满前重新确定保密期限，且只能由原定密机关单位作出相关决定。（ ）

4 国家秘密的保密期限，除另有规定外，绝密级不超过30年，机密级不超过20年，秘密级不超过10年。（ ）

单项选择题

5 加强涉密人员管理是确保国家秘密安全的重要内容，涉密人员保密管理坚持谁主管、谁负责，并遵循科学确定、严格审查、（ ）、全程监督原则。

A．分类管理　　B．奖优罚劣　　C．按人定岗

6 在实际工作中，需要根据国家秘密事项的性质和特点，按照维护国家安全和利益的需要，对国家秘密事项作出保密时间限度的规定，以下哪一项不是保密期限的具体表现形式（ ）。

A．解密时间　　B．解密条件　　C．解密申请

7 在下列职责中，应由机关单位定密责任人承担的是（ ）。

A．对确定、变更和解除机关单位国家秘密提出具体意见

B．对机关单位产生的尚在保密期限内的国家秘密进行审核，作出是否变更或解除的决定

C．在机关单位产生国家秘密时，依据有关保密事项范围提出定密具体意见

8 年产生、处理（ ）国家秘密达到3项（件）的，可以确定为核心涉密岗位；年产生、处理机密级以上国家秘密达到（ ）项（件）的，可以确定为重要涉密岗位；其他则可以确定为一般涉密岗位。

A．绝密级　6　　B．机密级　6　　C．绝密级　9

责任编辑/武 薇

南京航空航天大学保密宣传教育参考资料

（2021 年第 2 季度）

参考学时：2 小时

（一）举案说法

严防涉密会议泄密

□袁 健

涉密会议的保密管理涉及人员、载体、场所等多个方面，涵盖环节多，稍有不慎就会造成泄密。保密法第三十一条、保密法实施条例第二十七条专门对涉密会议、活动的主办单位提出了应当采取的保密措施，要求制定保密方案，明确参会范围，落实场所、设施、设备保密管理规定，严格管理涉密载体，对参会人员提出明确保密要求。但是，从近年来有关涉密会议期间发生的泄密案件来看，一些管理措施没有落到实处，人员、载体、场所的管理依然是最容易出现问题的薄弱环节。同时，随着信息化的快速发展，由电视电话会议引发的泄密问题也应当引起高度重视。

案例分析

案例一：会议场所及人员管理不严

2018 年 1 月，某自治州无业人员蒋某以找工作为名进入某宾馆，误入该州委全会会议现场，并趁机窃取 2 份机密级会议文件。此后至 2019 年 8 月期间，蒋某冒充该州委、州政府工作人员，多次进入州委、州政府机关驻地会议室等场所，秘密窃取党政机关文件资料 300 余份和涉密文件 U 盘 1 个（存有机密级文件 5 份，秘密级文件 1 份）。2020 年 6 月，审判机关以非法获取国家秘密罪判处蒋某有期徒刑 1 年。

分析：按照保密法第三十一条规定要求，主办单位应根据会议涉密程度和工作需要，确定参会人员范围，审核参会人员资格，登记参会人员姓名、单位、职务等情况，并保存相关材料。本案中，蒋某初次误入会场时，工作人员没有第一时间审核其身份，导致 2 份机密文件被窃。此后，蒋某尝到甜头，长期冒充党委、政府工作人员出入、参与各种涉密会议直至被公安机关控制。在调查中经询问相关工作人员发现，涉密会议主办单位认为蒋某是承办单位工作人员，而承办单位认为其是主办单位工作人员，无人知晓蒋某到底是何方人士，同时也没有按要求进行审核、登记，这实质上是为蒋某的行为开了绿灯，致使其窃密行为屡屡得手。对此，机关单位应深刻吸取教训，在组织涉密会议时，特别是在会议进程中，扎扎实实做好保密审查这一基础性工作，避免出现风险隐患。

案例二：会议涉密载体管理不善

2019 年 8 月，某镇政府工作人员范某在参加县里召开的某涉密会议后，将涉密会议文件带回家中，其妻张某趁范不注意，使用手机对该涉密文件进行拍照，并对外予以扩散，最终导致泄密。事件发生后，该县纪委监委、县保密局联合对镇党委书记齐某进行约谈，责令其作出深刻检查；县纪委给予镇分管负责人、人大主席焦某党内警告处分；县监委给予范某降低岗位等级处分，并调离涉密工作岗位。

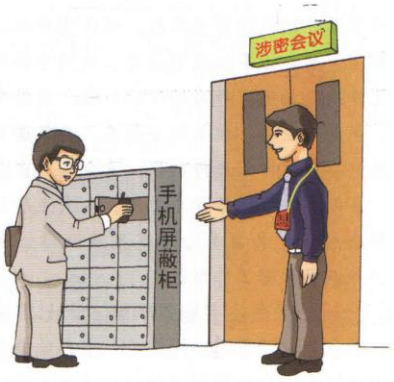
分析：保密法实施条例第二十七条规定要求，举办会议涉及国家秘密的，主办单位应当按照国家保密规定管理国家秘密载体。本案中，泄

密的主要原因在于范某违规将会议文件带至家中，为其妻接触涉密文件提供了条件。这种情况引发的泄密，也是老生常谈的一类问题。因此，机关单位应严格涉密会议使用或形成的涉密文件资料及其他涉密载体管理，在制作、分发、存放、回收、销毁等各个环节，落实保密管理措施。特别是在涉密会议开始前，应当指定专人负责会议涉密文件资料的发放、管理工作，并按要求及时登记、记录文件分发情况。会议进行中，文件负责人员应当紧盯文件动向，对中途离场人员予以重点关注，谨防涉密文件被违规带离会场。会议结束时，应当按规定第一时间清退、回收涉密文件材料，并妥善保管。同时，应加强对参会人员（含服务人员）的保密教育，要求其妥善管理涉密文件资料和其他涉密载体，不得擅自记录、录音、摄像和摘抄，不得擅自复印涉密文件资料等。

案例三：涉密视频会议违规接入互联网

2020年8月，某网站刊登某国有企业涉密文件。经查，该企业召开电视电话会议，传达上级机关涉密文件精神并就贯彻落实进行安排部署。会议期间，某分公司通过互联网音频会议软件接入，导致会议内容被网络窃取。案发后，会议召集人、该公司党委副书记黄某被给予党纪处分，并对公司年度绩效考核保密项进行扣分处理。

分析：保密法实施条例第二十七条规定要求，举办会议涉及国家秘密的，主办单位应当使用符合国家保密规定和标准的场所、设施、设备。本案中，造成泄密的主要原因在于使用了不符合保密规定的互联网渠道传达涉密文件精神。近年来，各地电视电话会议召开日益增多，客观上增加了泄密风险，机关单位应加强监管。在涉密会议召开前，主办单位应对会议场所设备进行严格检查，不得使用无线话筒、无线键盘、无线网络等无线设备或装置，不得使用不具备保密条件的电视电话会议系统。确需使用的扩音、录音等电子设备、设施应经安全保密检查检测，携带、使用录音、录像设备应经主办单位批准。



对策建议

以上3个案例仅为涉密会议泄密的具体表现。涉密会议特别是大型涉密会议，往往时间紧、任务重、环节多，主办单位限于人力等各方面因素，很难做到面面俱到，极易出现“跑风漏气”等问题，导致涉密会议泄密。结合对涉密会议泄密案例的具体分析，笔者认为，应从两方面做好涉密会议的保密管理工作。

一是明确各方责任，解决“谁来干”的问题。责任不清往往导致会议主办单位和承办单位之间形成衔接“漏洞”，甚至推诿扯皮。对此，涉密会议主办单位应制定保密工作方案，及时确定会议密级，对参会人员提出保密要求，明确专人负责督促落实。承办单位要按照主办单位要求，提供安全保密的环境、设施和设备，并对工作人员进行保密教育，明确工作人员的保密责任，要求其做好保密服务保障工作。

二是抓好制度落实，解决“怎么干”的问题。保密制度是长期以来保密工作经验和教训的总结提炼，凝聚了各方面的智慧和心血。机关单位应准确把握保密工作制度要求，重点围绕会议涉密人员、涉密场所、涉密设备、涉密载体、宣传报道等方面抓好落实，以慎之又慎、严之又严的作风做好相关工作，全力确保涉密会议不出任何问题。

责任编辑／徐 琛

（转自《保密观》）

（二）警示案例

网盘存密遭处分：切勿使国家秘密在互联网上“裸奔

近年来，网盘成为一种很常见的存储工具。不需要携带实体盘、存储空间大、随时随地上传下载，还可以分享文件给同事好友，诸多优点使得网盘很快受到个人和单位的青睐。这其中不乏一些机关单位工作人员使用网盘辅助办公的情况，随之而来的泄密事件也不在少数。

网盘存密：泄密案件时有发生

案例 1　违规存储国家秘密

某省直单位李某，利用自己的百度云盘私自保存涉密资料。经鉴定，该资料属于机密级国家秘密，该事件定性为在互联网上存储处理国家秘密泄密事件。李某受到组织处理。

案例 2　违规传递国家秘密

某县政协工作人员杨某为方便《地方志》撰写工作，在未经保密审查的情况下，擅自在单位将收集的 5000 余份文件资料（包括 1 份机密级、2 份秘密级国家秘密）上传到网盘，回家下载后使用。杨某受到行政警告处分。

云上存储：秘密信息安全难保

在网盘上存储处理涉密文件，就是让国家秘密在互联网上“裸奔”，其被泄露的风险极高。网盘遭受攻击几率高。国内外均出现过网盘遭到攻击泄密的安全事件。2019 年 1 月，国外云存储服务 MEGA 上超过 1.2 万个文件、包含 87GB 的数据遭到泄露。2020 年 4 月，网上出现了一款专为破解百度网盘的名为 Pandownload 的软件，该软件能够实现以非会员权限突破百度网盘官方设定，导致百度网盘中存储的文件泄露。该软件开发者被公安机关依法逮捕。

网盘安全保密系数低。之前网上曝光可通过第三方搜索软件查看网盘中存储的隐私文件。普通用户只需打开网页简单几步操作，就能看到大量设置了分享的网盘隐私内容。网盘的安全系数可见一斑。

严管严控：坚决杜绝网盘泄密

网盘泄密正在成为一种新的泄密方式，机关单位需要引起重视，严管严控。

一要把好“思想关”。要将网盘的安全保密隐患、使用网盘存储处理传输国家秘密的后果危害等，和涉密人员讲清楚、说明白，从思想上杜绝网盘存密这种低级错误的发生。

二要注重“检查关”。机关单位应定期有针对性地开展保密检查，重点关注涉密设备及系统保密管理要求是否落实，把好国家秘密在涉密设备和系统中的“出口关”，从源头上避免网盘存密行为的发生。

三要强化“技术关”。机关单位要采取必要的技术措施，及时发现、制止互联网上存储、处理国家秘密的错误行为。同时，采取技术手段加强监管，阻断、禁止网盘存密等具有泄密风险隐患的操作。

（转自《保密观》）

仔细查查！你的涉密计算机很可能违规外联

保密法第四十八条规定了 12 种严重违规行为，涉密计算机违规外联赫然在列。如今，保密法修订施行已十载有余，涉密计算机违规外联的低级错误为何仍屡屡发生？背后原因引人深思。

典型案例

案例 1：2019 年 9 月，有关部门在工作中发现，某单位 1 台涉密计算机多次违规外联。经查，该单位新入职人员王某因工作需要，申请 1 台非涉密计算机，设备管理员李某遂从库房调配了 1 台旧计算机给王某。但由于该计算机的设备标签脱落，二人均未发现该计算机原为涉密计算机，最终导致违规外联。

案例 2：2020 年 6 月，有关部门在工作中发现，某市属单位工作人员刘某使用的涉密笔记本电脑发生违规外联。经查，刘某因工作需要，将涉密笔记本电脑带入单位会议室使用，由于会议室中网线标识不清，着急开会的刘某误将涉密笔记本电脑接入互联网，触发违规外联报警。

案例 3：2020 年 9 月，有关部门在工作中发现，某县级单位 1 台涉密计算机多次发生违规外联。经查，该计算机为办公室工作人员孙某使用，孙某在使用过程中，看到某软件发生故障，就多次按照软件提示，尝试连接互联网进行自动修复，造成违规行为发生。

以上几种涉密计算机违规外联行为，令人防不胜防。仔细梳理，其成因无外乎以下 3 个方面：

1.保密意识淡薄、保密技能不强。如案例 1 中，设备管理员李某在设备标签脱落的情况下，未进一步核实就配发给使用人员，而使用人员也不闻不问，直接连接互联网。案例 2 中，刘某在网线涉密属性标识不清的情况下，不找管理员询问就着急连接使用。案例 3 中，孙某明知计算机的涉密属性还连接互联网

进行软件修复。而如果具有一定保密意识和技能，这些涉事人员应能够通过计算机运行的程序、线路墙插等对其是否涉密、是否联网进行初步判断，从而规避风险隐患。

2.设备管理混乱。比如，涉密设备与非涉密设备混放；涉密设备台账不清，设备的密级属性仅靠表面粘贴的设备标签识别；涉密设备清点维护不及时，标签脱落未能发现等。另外，人员交替中设备交接不清、管理人员违反规定将涉密计算机外送社会公司维修、将报废不用的涉密计算机硬盘拆下安装在非涉密计算机上使用等，也会导致失泄密事件的发生。

3.设备设施不完善。有的机关单位仅用普通胶水或透明胶带粘贴涉密设备标签，极易脱落；有的设备标签为手写，涂写随意；有的非涉密设备调整为涉密设备后，未及时更换标签，这些都容易导致误连接。

对策建议

那么，如何避免涉密计算机违规外联呢？需从人、物两方面加强保密管理。

相关人员要提高保密意识，加强技术学习，提高对失泄密风险隐患的自查自纠能力。要注意提高自己的保密技术水平，在接受保密教育培训后进行实战演练，将保密技能由理论落实到实践。

加强载体设备全生命周期和动态管理，不能因人员变更、位置变化、用途调整等因素导致脱管失控。另外，全生命周期管理还意味着动态监管，机关单位应采取实时技术监控、随机抽查、定期维护等手段，确保涉密设备始终可管可控。

（转自《保密观》）

（三）保密大视野

揭秘《绝密使命》背后的绝密往事

近日，国家广电总局“理想照耀中国——庆祝中国共产党成立 100 周年电视剧展播”作品之一《绝密使命》在央视一套圆满收官。

该剧首次真实再现了党的秘密交通线上完成的一次次惊心动魄的绝密使命，生动刻画了隐蔽战线上一批可歌可泣、大智大勇的英雄群像。其中有这样一段剧情让人印象深刻，我党的秘密交通员通过红色交通线护送一位代号为“上海爷叔”的重要人物，一路从上海出发，经过上千公里的艰难跋涉，终于平安抵达红都瑞金。

这是一段书写在保密史册上的真实历史，那么这位“上海爷叔”是谁？他又为何要从上海去往瑞金？这要从中央特科的成立讲起。

风云突变，中央特科应运而生

大革命失败后，1927 年 9 月底至 10 月上旬，中共中央机关从武汉迁回上海。当时的上海，军警宪特、租界巡捕、帮会势力和地痞流氓云集，地下斗争日益残酷。11 月，为保卫党中央的安全，周恩来筹建并领导了我党历史上第一个专业情报保卫机构“中央特科”。

我党隐蔽战线的创始人和领导者周恩来

中央特科的主要任务是，“保证中共中央领导机关的安全，收集掌握情报，镇压叛徒，营救被捕同志，建立秘密电台”，先后设立了一科（总务科）、二科（情报科）、三科（行动科，又称“红队”）、四科（通讯联络科）。

1931 年 4 月，中央特科遭遇了至暗时刻。特科负责人、兼任三科科长的顾顺章被捕叛变。千钧一发之际，我党潜伏在敌人“心脏”的钱壮飞及时送出绝密情报，力挽狂澜。中共中央机关在短时间内完成了一次史无前例的大转移，周恩来、瞿秋白、邓颖超、邓小平、陈云等中共中央领导人幸免于难。

龙潭三杰：李克农、钱壮飞、胡底

由于顾顺章掌握了我党大量核心机密，中央特科的一些“联络员”也是他一手挑选的，有些甚至只和他单线联系，再加上国民党开展大搜捕时，尚有一些同志还未来得及转移，中央特科数名队员被捕，遭敌人杀害，遭受重创。

保密护航，苏维埃血脉跳动不息

迫于上海严酷紧急的形势，党中央决定，派周恩来前往中央苏区担任苏区中央局书记。周恩来于 1931 年 12 月上旬出发，经由红色秘密交通线一路辗转、日夜兼程，于 12 月下旬到达永定，最终顺利抵达中央苏区。

这条成功护送周恩来同志的“华南交通线”，由上海经香港、汕头、潮安、大埔、永定直达江西瑞金，就是剧中所表现的交通线，被誉为“党的生命线”“苏维埃红色血脉”。据不完全统计，通过这条生命线进入中央苏区的领导同志和其他干部有 200 多人，运往苏区的物资超过 300 吨。

这条秘密交通线绵延 3000 公里，在险恶环境中一直能够顺利运转，得益于坚实可靠的保密护航。

时任中央交通局局长吴德峰在交通线建立之初就制定了《秘密工作条例》，包括不该问的人和事不问，不该看的文件不看，不该传播的不传播；不允许到群众斗争场合，不许照相；写过的复写纸、印过的蜡纸和有机密文字的纸屑要及时烧掉等，简明管用。

交通线上站点的设置也充分做到因地制宜，依据实际情况，以家庭、当铺、茶馆等多种形式做掩护，秘密开展工作。在交通员选拔方面，将对党忠诚、严守秘密放在

首位。此外，还需具备对敌斗争经验，熟悉多种方言土语，最好有一技之长便于掩藏身份等。

传递情报的方法也是巧妙多样，如用密写药水将文件写在衣服上、手绢背面等，运送金条、电台零件和药品等物资的方式也不能相同。

赤胆忠心的红色交通员加上系统扎实的保密工作，使得这条秘密交通线真正成为了“摧不垮、打不掉的地下航线”。

剑吼西风，保家卫国誓言无声

周恩来转移后，伤痕累累的中央特科在陈云的带领下，在上海开始了艰难的恢复重建工作，并继续坚持开展隐蔽斗争。

在腥风血雨的环境中，中央特科勇于向白色恐怖“亮剑”，前后八年里，在上海开展了大量卓有成效的工作，在我党历史上创造了多个“第一”：

组建了第一个打入敌人“心脏”的工作小组（“龙潭三杰”）；

发展了第一个反间谍关系（杨登瀛）；

开辟了第一条地下交通线（上海至中央苏区）；

研制了第一部无线电收发报机（同各地党组织取得电讯联系）；

编制了第一份密电码（“豪密”）；

设置了第一座中央级秘密档案库（中央文库）；

第一次公开镇压叛徒（何家兴、贺稚华夫妇）；

第一次协同保卫重要峰会（全国苏维埃区域代表大会）；

第一次成功转移党的机关（中共中央和江苏省委的机关）。

中央特科为保卫党中央的安全发挥了重大作用，并为抗日战争和解放战争时期党的隐蔽战线的发展奠定了坚实基础，在对敌斗争中立下了彪炳史册、光照千秋的不朽功勋。

(转自《保密观》)

（四）自测试题

· 判断题

1 保密法2010年修订后，涉密人员成为严格的法律概念，即涉密人员与涉密岗位直接相关，是否属于涉密人员取决于是否在涉密岗位工作，如果不在涉密岗位工作，即使了解掌握一些国家秘密，也不能确定为涉密人员。（　　）

2 保密要害部门部位中的岗位不能简单与涉密岗位画等号，这些部门部位中既有涉密岗位，也有非涉密岗位。（　　）

3 某中央机关下发1份秘密级文件，下发后不久即由新华社授权对外公布了部分内容，因此可视为该文件已解密。（　　）

4 机关单位对于已解除的不属于本机关单位产生的国家秘密，需要公开的，应经原定密机关单位同意。对于已解密的文件资料，在原定密机关单位尚未正式公开前，应作为内部资料加以保管，不能擅自公开。（　　）

· 选择题

5 【单选】2010年修订后的保密法取消了（　　）机关单位的定密权，取消了（　　）机关的绝密级定密权，改变了以往所有机关单位均可定密的做法。

A. 县级　　设区的市、自治州一级的　　B. 地市级　　设区的市、自治州一级的

C. 县级　　地市级

6 【单选】手机在下列哪种情况下存在泄密隐患？（　　）

①通话过程中　②待机状态　③关机

A. ①　　B. ①②　　C. ①②③

7 【多选】互联网及其他公共信息网络运营商、服务商应当配合（　　）对泄密案件进行调查，发现利用互联网及其他公共信息网络发布的信息涉及泄露国家秘密的，应当立即停止传输。

A. 公安机关　　B. 国家安全机关　　C. 检察机关

8 【多选】以下属于定密不当的情形的是（　　）。

A. 权限不当　　B. 依据不当　　C. 程序不当

责任编辑／武 薇