以下案例均来自于互联网：

案例 1：网上泄密案例——歼十泄密案侦破记

1999 年 5 月 19 日，星期三。清晨，四川成都电子科技大学保卫部门的老李走进办公室，进入“西南教育网“网址，开始了每日例行的网上浏览。突然，一个醒目的标题赫然跃入眼帘。具有丰富保卫工作经验的老李仔细地阅读了题目下的正文，心不由得揪紧了。泄密，而且是泄露国家重要军工机密!他没有迟疑，马上接通了成都市国家安全局的电话。

成都市国家安全局董科长眉头紧锁起来，他当即说道：“此事非同小可，请马上下载该文，并通知你校网管中心立即将此文删除。“成都市国家安全局悬既将案情分别上报省国家安全厅和市委、市政府有关领导。

当日，成都市保密委和成都某公司保密委便对文章做出了专业密级鉴定，认为：该文严重泄露了我军工机密和中央领导的有关指示精神。成都市国家安全局对这起在国际互联网上泄露我军工机密案件的专项调查工作紧锣密鼓地开展起来。

5 月 19 日，成都市国家安全局通过在电子科大的调查发现，5 月 18 日 10 时 13 分 33 秒，一个名叫“GUN 枪王“的人在电子科大网址上粘贴了该泄密文章，而此人是通过成都理工学院一上网微机操作的。这是个令人兴奋的重要线索。第二天一早，****们就匆匆赶往成都理工学院调查，并很快将目光集中到一个姓赵的在校学生身上。据查：5 月 18 日 9 时 40 分至 11 时，赵某在该校信息教研室机房的联网微机上上网，其网上化名为“GUN 枪王“，与在电子科大网上张贴泄密文章的时间和署名相吻合。5 月 21 日，调查组****再次来到成都理工学院。下午 2 时，班主任将赵某带到了****面前。当****问起他的业余爱好时，赵某脱口而出：“上网和军事科技。“但当问到他在网上看到了什么军事方面的信息时，敏感的赵某似乎意识到了什么，只字不提有关泄密文章的情况。细心的****觉察到了赵某的顾虑，耐心地开导帮助他，终于使他放下了包袱，承认该文确是自己于 1999 年 5 月 15 日 10 时 23 分 21 秒存在其电子信箱中，并于 5 月 18 日上网时将其粘贴于电子科大网上，并当场从他本人的电子信箱中调出了该文。****们让他回亿该文的来源。“重庆邮电学院网站或者

华南理工学院网站“，赵某告诉了****们两个经常光顾的网站。然而，经过反复认真的查找，这两个网站均无泄密文章的原文。解铃还需系铃人，****们把赵某带到了拥有“西南教育网站总汇“之称的电子科大网站，让他上网回忆搜寻。一小时后，起

某从平时很少去的深圳邮电网 BBS(电子公告版)“一网情深“上找到了自己下载的文件。

****顺藤摸瓜，在电子科大有关专家的帮助下发现了深圳邮电网 BBS“一网情深“所 huode 获得的泄密文章是 5 月 13 日从深圳邮电网一台名为 Maxll-43 的微机上得到，进而发现该泄密文章在传递到此微机时已被修改。经进一步查证，发现深圳邮电网又是从一名为“北国开心天地“的网站中获得，而该网站是从东北大学所属东大阿尔派公司和辽宁邮电局共同组建的“北国数据公司“中的两台名为 ndc136 和网络地址为 202.118.112．224 的微机上最先有记载和发出的。该“站点及微机均设于东北育才学校内。追源工作在一步步展开，触角逐渐延伸到省外，难度亦越来越大。

与此同时，电子科大的王副书记和有关专家组成员通过连续 7 个小时的网上搜寻，查到泄密文章曾存在于“华南教育科研网“华南理工大学所设的“木锦站军事版“中，但已被版主删除。

5 月 22 日，四川省国家安全厅厅长陈文清等领导专程来到成都市国家安全局，与专案组****共同召开了案情分析会，当日，四川省国家安全厅即电告广东省国家安全厅，请求协查“木锦站军事版“5 月 15 日左右登载的有关泄密文章的情况。至此由深圳邮电网---东北育才学校和华南科研网---华南理工大学“木锦站军事版“两条线索齐头并进，追查密源的工作全面铺开。

5 月 25 日上午 9 时。四川省国家安全厅向成都市国家安全局通报了广东省国家安全厅回复的协查情况：经查，“华南教育科研网“近期确有一篇涉及我军工情况的文章，由一名为“阿安“的网民于 5 月 18 日 10 时 18 分从惠州 BBS 站转贴于“华南木棉站“上。然而，从文章内容看来，与那篇泄密文章大相径庭，不是所追密源。

随着一个又一个可能性被排除，追源线索愈来愈少。1999 年 5 月 26 日，一条新的线索出现了，上海复旦大学开设的“日月光华站“网站军事天地版中发现了泄密文章的原文。成都市国家安全局对此高度重视，迅速组织力量开展调查。调查发现，该文是一名叫“snake 小龙“的网民于 5 月 16 日 11 时 10 分 05 秒粘贴在该网站上的。

6 月 1 日，成都市国家安全局向上海市国家安全局发出专电，要求协查在“日月光华“网站军事天地版张贴泄密文章的署名为“snake 小龙“的详细情况。同日，成都市国家安全局请求辽宁省沈阳市国家安全局协查在“北国之春“网站上发布文章的王某的有关请况。6 月 3 日，上海市国家安全局回复协查结果，“snake 小龙“系复旦大学在校学生刘某，其于 5 月 16 日在自家电脑上粘贴该文至“日月光华站“军事天地版。6

月 4 日，成都市国家安全局请求福建省国家安全厅协查密源。6 月 8 日，沈阳市国家安全局回复协查结果：王的信息来源为其 5 月 8 日在所在某外贸公司上网浏览时，从深圳实达公司网站上下载，后转贴于“北国之春“网站上。6 月 11 日，福建省国家安全厅回复协查结果：泄密文章于 5 月 7 日 13 时 58 分 31 秒张贴于深圳实达公司网站“实达军事天地“版上。至此，泄密文章扩散的情况全面查清。

与此同时，内查工作亦在紧张有序地进行，结果显示，成都地区共涉及到 27 家单位，近十万人。****们将范围逐渐缩小，最终划定在某厂和某研究所内。****们详细调查了该厂和该所在 5 月 6 日至 18 日期间上网的所有人员，将其中具备泄密条件的上网人员纳入了重点视线范围，其中就有犯罪嫌疑人郭健。

根据成都市国家安全局提供的重点人员线索。成都市****局通过国家网上监控中心发现，5 月 7 日凌晨，粘贴在成都“威震四方“BBS 上署名为“netman“的泄密文章，是最早登上国际互联网的。由此展开调查，1999 年 6 月 11 日，终于抓获嫌疑人郭健。

至此，我国重大网上泄露军工机密案终于成功告破。

郭健 1992 年 7 月大学毕业分配到某研究所工作，任助理工程师，参加了我国某项军工项目的设计工作，并先后两次被公派出国培训。后因长期旷工被研究所于 1998 年 7 月开除。据郭健交代，1999 年 5 月 7 日零时 34 分 37 秒，他在家通过 169 拨号上网，于在线状态编写了那篇泄密文章，发表在“威震四方“栏目上。其目的是为了向网友显示自己掌握的国产某型先进战斗机的专业技术水准。根据郭健泄露国家军事秘密的犯罪事实，****局将其依法逮捕，后被判处有期徒刑八个月。

案例 2：博士研究生考试试题泄密案

2002 年 4 月的一天，湖南省某市正在进行着博士研究生的考试。可是开考不久，没有预料到的事情发生了，一位监考老师发现一名考生神色慌张，从衣袋里拿出事先准备好的纸条照着填写。监考老师们断定这位考生在作弊，立刻没收了他的试卷和纸条，取消了他的考试资格。然而事隔不久，在其他考场也相继发现有考生作弊。考试结束后，在某市的几个考场，当场发现的作弊考生达 6 人。这突如其来的多人作弊事件是从未发生过的，他们将没收的纸条进行仔细对照，惊惊讶地发现这些都是手抄答案，并且每份答案都完全相同。

省教委的领导得知情况后非常重视此事，立即派法纪处的同志进行调查。经过调查发现，这些答案是试卷泄露以后由其他人解答的，教委领导顿时感到问题的严重性。试卷是由理工大学研究生部招考办公室统一保管的，通过进一步调查，他们得知部分考生的答案是从某市个体户手里买来的。一起严重的试卷泄密事件立即反映到省、市党委和政府有关部门。各级领导给予高度重视，一方面，要求公安部门派出得力干警迅速侦破泄密案，另一方面，指示教育部门做好对作弊考生的清理工作，对异常试卷做好记录，查清泄密面，各项与试卷泄密案件有关的调查工作随即紧锣密鼓地展开了。这突如其来的试卷泄密的消息不胫而走，造成了不好的社会影响。

省保密局接到试卷泄密的报告后，立即派专人与相关部门取得联系，调查核实情况并提出查处意见和办法，随后市保密局也深入到教育部门协助调查此案。市公安局派出的侦破人员经过几天侦察，很快查清了试卷泄密的原由。

2002 年 4 月某单位职工家属李某到个体户张某家时，张某向李某夸口说自己能搞到博士研究生全国统一招考的试卷。李某就提出让张某搞一份英语试卷，张某马上答应下来。张某想到了与自己有几面之交的、在理工大学研究生部当主任的王某，于是就找到王某说明来意。王某对张某说：考试试卷是由专人严密管理，要想看一看都非常困难，拿一份出来，更是难上加难；万一试题泄密后被查出来，是要受到党纪、政纪处分的，严重的将受到法律的制裁。为了自己的前途，王某婉言谢绝了张某的要求。张某并不死心，死皮赖脸地缠着王某，并许诺：若弄到一份博士研究生全国统一招生英语试卷将以重金酬谢，并保证只给一人看。王某在利益面前，完全丧失了身为一名共产党员、国家工作人员应有的原则，答应了张某的无理要求。

试卷由研究生招考办公室统一保管，王某利用工作上的方便，在考试前一天上午 10 点左右，擅自到考试中心印卷现场，以"分管招生考试领导审核试卷"的名义，从研究生部招考办公室试卷监印工作人员手中拿走一份完整的博士研究生全国统一招考英语试卷。王某回到家里，立即电话通知张某试卷已到手中，张某放下电话急忙赶到王某家中，取走了这份试卷。当天下午 1 点左右，李某得知消息后，专程赶到张某家拿走试卷。李某回到家里，将试卷交给了儿子：王健。王健把试卷复印了两套后，以每套 2000 元的价格卖给孙某、伟东和伟杰三人。伟东和伟杰又以不等的价格将试卷多次转手，就这样这套考卷经过多次复印，泄露范围越来越大。

《教育工作中国家秘密及其密级具体范围的规定》第三条第一款规定：国家教育全国统一考试在启用之前的试题（包括副题）、参考答案和评分标准为绝密级事项。

第三条第二款规定：国家教育省级统一考试在启用之前的试题（包括副题）、参考答案和评分标准为机密级事项。

第三条第三款规定：国家教育地区（市）级统一考试在启用之前的试题（包括副题）、参考答案和评分标准为秘密级事项。

《中国共产党纪律处分条例》第六十七条规定：在考试、录取工作中，有泄露试题、考场舞弊、涂改考卷等违反有关规定行为的，给予警告或者严重警告处分；情节较重的，给予撤消党内职务或者留党察看处分；情节严重的，给予开除党籍处分.

案例 3：都是“winny”惹的祸

2006 年年初，最火的网络 BBS 上出现了“海上自卫队机密遭泄露”的贴子。这些“机密文件”将一艘名为“朝雪”驱逐舰使用的呼叫信号、密码使用表、紧急呼救电话，甚至训练和作战记录等细节。更可怕的是，在被公布的“极秘”（日本防卫厅按照文件重要程度把秘密文件分成三等：“机秘”、“极秘”、“秘”。）文件中，还有日本海上自卫队的非常用密码和密码文件的整理序号等内容。情报在网上传播一周后，日本防卫厅证实，这些秘密文件“属实”。这次情报泄露被军事专家称为“日本防卫史上”最大的泄密灾难。

无独有偶，“朝雪”泄密事件后一个月，日本陆上自卫队和航空自卫队的业务信息、冈山县和爱媛县警方的搜查信息再次泄露。此外，多家企业发生商定秘密泄露事件。

一系列的泄密事件，震惊日本上下。当时的日本首相小泉命令防卫厅：一定要彻查“朝雪”泄密的真相。经查，泄露秘密的罪魁是“朝雪”驱逐舰自卫队队员——41 岁的海曹长。作为电信官，他负责处理“朝雪”所有对外联络和通讯事务。电信室是舰艇上的机要重地，保密级别甚至高于“战斗指挥所”。电信官都是经过特别授权的保密人员。虽然日本防卫厅严禁队员移动存储与工作相关的数据，但就是这个重要涉密人员把工作中常用的文件制成 CD，擅自把秘密数据带回家，拷贝到互联网相连的个人电脑上。

随着调查的进展，调查人员发现，海曹长平时喜欢用日本最流行的下载交流软件“winny”下载歌曲和电影。而其他一系列信息泄露事件所涉及单位的内部工作人员也都曾经用装有“winny”软件的私人电脑处理公务。

“winny”软件于 2002 年 12 月问世，在日本广受欢迎的一款网络文件交换软件。用户可用它在网上检索感兴趣的电影、音乐和游戏等文件，如果在其他“winny”用户电脑的共享文件夹中找到了需要的文件，就可以随意下载。

但是，“winny”软件也是一些电脑病毒的温床。使用该软件下载的文件一旦隐藏“Antinny”等病毒，用户只要双击下载的文件图标，电脑就会感染病毒，这种病毒可随意将电脑中文件压缩后放置到共享文件夹中，一旦电脑联入互联网，就会导致信息泄露。此外，由于这种软件是基于自由网模式的点对点的网络文件交换软件，支持电脑间不经过服务器直接交换数据，且无法记录用户的 IP 地址，因此在一定程度上增加了保密监管的难度。由于电脑本身不会出现异常，用户往往直到被别了告知自己的个人信息泄露了，才意识到电脑感染了病毒。更为糟糕的是，流失的文件会被记录到许多电脑中，几乎不可能回收。

“朝雪”泄密事件后，日本防卫厅立即设立了“根治对策检讨会”，寻求防止再次发生同类事件的对策。“根治对策检讨会”给出的对策包括：对于“机密”“极秘”级别的秘密情报，一旦出现泄露，根据自卫队法对泄密人处以 5 年以下有期徒刑，即使是过失也要进行免职；对于 CD—ROM 等信息载体所保存的数据全部进行个别密码化，否则将以泄露情报“论处”。同时，日本政府要求金融、航空等和国民生活及社会经济活动密切相关的基础行业彻底采取防止泄密的措施。同时，日本各大公司纷纷针对“winny”开发了过滤软件。

据新华社报道，2006 年 12 月中旬，曾供职于东京大学研究生院、开发和散布“winny”软件的金子勇，被日本京都地方法院判处罚金 150 万日元（约合 1.28 万美元），原因是其违反了著作权法。

现在，就在日本各方都在采取紧急措施，以求堵住“winny”这扇泄密“天窗”的时候，在我国却还有许多软件下载网站提供“winny”软件的汉化版本，一些大型网站下载量甚至已达数万次。日本的泄密事件给我们敲响了警钟。一方面要做好对“winny”软件的防护工作。另一方面则要严格遵守涉密计算机不得连接国际互联网或其他公共网络、不在连接国际互联网的计算机上处理涉密信息等规定，从源头上防止泄密事件的发生。

案例 4：计算机网上泄密案

利用网络传递信息方便快捷，但利用互联网传递涉密信息，在方便自己的同时，也方便了境外的间谍机构。用涉密计算机上网浏览、传递涉密或不涉密信息都是十分危险的。别有用心的人不但可以通过网络获取涉密信息，还可以通过操作系统的漏洞侵入涉密计算机硬盘。也许当一些人津津有味地上网浏览时，间谍也正在津津有味地下载着我

们的国家秘密。

2002 年 3 月，某市某区教委为传达文件需要，竟将上级下发的涉密文件贴在与国际互联网相联的区教育信息网上。经鉴定，其中共 3 份属机密级国家秘密，2 份属于秘密级国家秘密。

2002 年 2 月，华北某学院教师刘某将涉密科研项目申请书（秘密级）在互联网上用电子邮件形式传递，造成泄密。6 月，该学院另一教师将 7 项涉密科研成果（秘密级）在互联网上用电子邮件传递，造成泄密。还是 6 月，该学院教师王某将两篇涉密文章在互联网上用电子邮件形式传递，造成泄密。案发后，学院给予三起泄密事件的责任人行政警告处分，并进行通报批评。

2002 年 9 月，某部委研究室工作人员张某违反计算机保密管理规定擅自在载有机密级文件的计算机上安装上网设施，从互联网上下载资料。致使计算机中有关统战工作的机密级文件被窃取，最后竟出现在某国的网站上，不仅给国家造成严重损失，而且在国际上也造成了很坏的影响。

2003 年国家保密局通过网络检查，查获了多起在互联网上发布秘密文件的泄密案件；这些文件大多是我们"自己人"贴上去的。有时工作人员为了工作方便将密级文件盖住密级和文件头后在内网传递，传来传去便传到了互联网上；而有时涉密文件是因在内网中没有标密，无知人员将其与非密文件统统放到外网上，导致文件泄密。同时这些泄密人员所在单位对计算机保密防范工作缺少应有的重视，没有完善的规章制度，不对本单位重点涉密人员进行保密知识教育，也是发生这些泄密事件的原因之一。

《计算机信息系统保密管理暂行规定》第十条规定：计算机信息系统存储、处理、传递、输出的涉密信息要有相应的密级标识，密级标识不能与正文分离。

第十一条规定：国家秘密信息不得在与国际网络联网的计算机信息系统中存储、处理、传递。

第二十二条规定：计算机信息系统的使用单位应根据系统所处理的信息涉密等级和重要性制订相应的管理制度。

第二十九条规定：违反本规定泄露国家秘密，依据《中华人民共和国保守国家秘密法》及其实施办法进行处理，并追究单位领导的责任。

案例 5 ： 文件泄密案

某市纺织工业总公司机械厂党委书记，1998 年 5 月 22 日在总公司开会期间，从总公司党办领取 3 份中央密级文件，因当日正值厂休，便将文件带回家中。次日上班后，没有按规定将文件交机要人员登记保管。6 月 17 日，纺织总公司按市委办公厅要求清退中央 1O 号原发件时，其才发现 3 份秘密文件全部丢失，后经多方查找，均无下落。

中国国际航空公司某分公司办公室主任，1998 年 5 月 14 日收到该公司党委办公室发的中央 10 号原发件。其在传阅和组织学习中，未能及时将文件收回归档。6 月 15 日，公司党办在发重印件，清退中央 10 号原发件时，发现丢失。

某市国家安全局秘书科 1998 年 5 月接到市委办公厅发来的中央 1O 号原发件后转局政治部，分发到处级单位。当时，机要干部病休，由该部干部陈某临时接管收发文件工作。因陈业务不熟，加之部办公室副主任张某又未将工作交待清楚，所以陈未在发文登记上标明分发文件的序号。6 月 24 日，局下发清退文件通知，张某负责清退，但未履行清退手续。后张调离，由另一干部接替其工作，张亦未严格履行交接手续。在清退文件过程中，负责收发文的干部因故再次易人，致使 1 份文件查无下落。

某市园林局所属一饭店，1998 年 5 月 19 日收到局分发的中央 10 号原发件，总经理办公室文秘李某(合同工，非党群众)将文件登记后送领导传阅，6 月 10 日，李提出辞职，办公室主任在与其交接文件时，发现此件不在卷内，便当即询问，李称正在领导处传阅。待该饭店接到局清退文件通知后，立即多方查找，发现文件丢失。

案件发生后，该市保密部门迅速展开调查，并对这几起文件丢失案件进行了通报，追究了责任人相关责任。

文件管理一直是保密工作的重点，造成上述丢失密级文件的原因，主要是：

一、对发至"县团级"的密级文件疏于管理是造成密级文件丢失的根本原因。

二、个别单位领导干部的保密观念淡薄，思想麻痹，违反保密规定，是造成密级文件丢失的主要原因之一。

三、保密制度不落实，有章不循，密级文件管理混乱，是造成密级文件丢失的又一重要原因。

四、个别单位发现密级文件失控后，没能积极组织力量查找，丧失了查找和补救的时机。

五、对涉密人员安排使用不合理，造成密级文件丢失。

各部门、各单位要加强领导，认真落实保密工作责任制，高度重视文件保密工作。

《保密法》第二十八条规定：任用经管秘密事项的专职人员，应当按照国家保密工作部门和人事部门的规定予以审查批准。

《中共中央保密委员会办公室、国家保密局关于国家秘密载体保密管理的规定》第十一条规定：收发秘密载体，应当履行清点、登记、编号、签收等手续。

第二十条规定：阅读和使用秘密载体，应当办理登记、签收手续，管理人员要随时掌握秘密载体的去向。

《中共中央保密委员会关于党政领导干部保密工作责任制的规定》第十条规定：对单位存在重大泄密隐患或发生泄密事件负有主要领导责任的党政领导干部，视情节轻重，按照干部的管理权限给予警告、严重警告、撤消党内职务、留党察看或者开除党籍处分。

《天津市关于实行保密工作领导责任追究制的暂行规定》第二条规定：实行保密工作领导责任追究制，应坚持"谁主管谁负责"、"业务工作管到哪里，保密工作也要管到哪里"，以及教育与惩处相结合的原则，明确责任、积极防范，切实将党政领导干部保密工作责任制落到实处。

第五条规定：对保密工作领导责任追究的形式：

（一） 通报批评；

（二） 责令作出书面检查；

（三） 党纪、政纪处分；

（四） 追究刑事责任。

前款所列形式可单独适用，也可视情况合并适用。

第七条第一款规定：单位一年内丢失 2 份以上（含 2 份）国家秘密载体的，在追究直接责任人责任的同时，责令分管党政领导作出书面检查。

第二款规定：连续两年丢失国家秘密载体的，在追究直接责任人责任的同时，责令分管党政领导作出书面检查。