涉密会议频泄密，这些案例告诉你“跑风口”在哪里

原创：李宇斐 刘 阳保密观5月28日

近年来，涉密会议期间，时有微信泄密案发生，俨然成为一大“跑风口”。这些案例主要有以下3种类型。

案例1：违规使用微信处理涉密会议会务

2017年9月，为做好会务工作，某涉密会议服务人员展某，**将其负责的会务信息编辑后，发送到由8名会议服务人员组成的微信群，**被有关部门及时发现并补救处置，未发现造成泄密后果。案件发生后，有关部门**对展某进行了严厉批评，责令其作出深刻检查。**

案例2：违规使用微信传递涉密会议材料

2015年5月至6月，某党政机关负责人王某参加该省有关涉密会议期间，**通过微信将两份秘密级会议材料发送给家人，后被家人进一步转发。**此外，王某还将1份秘密级会议材料带回家，被家人拍照后通过微信发送给他人。案件发生后，**有关部门给予王某留党察看1年、行政撤职处分。**

案例3：违规使用微信传达涉密会议精神

2017年3月，某报社编务室人员任某在参加涉密会议时，**违规使用手机录音。会议结束后，任某将录音整理成会议记录，**报总编室主任王某。王某在报社总编辑彭某授意下，将会议记录上传到工作微信群。案件发生后，有关部门分别**给予任某、王某警告、记过处分，对彭某作出免职处理。**

微信缘何成为涉密会议的“跑风口”

第一，对微信泄密危害认识不足

一是认知偏差。如案例 1 中的展某，自作聪明地对会务信息进行编辑和替换，自以为将重要信息替换成字母代码，他人就看不懂。殊不知，这种小儿科式的“脱密”行为在明眼人眼中，可轻易推测出信息全貌。

二是心存侥幸。有的涉密人员明知保密禁令，也深知泄密后果，但仍抱有侥幸心理。如案例 2 中的王某，出于个人私心，通过微信将涉密会议材料发送给家人，以为在小范围内传播不会被发现。

三是贪图便利。有的涉密人员过度依赖微信，认为操作简单、交流及时、使用方便，头脑一热就将涉密会议相关信息发到微信中。如案例 3 中的彭某，未能认识到微信泄密的危害。

第二，涉密会议保密管理流于形式

一是未做好手机通讯设备的管理。涉密会议主办单位没有制定、实施有针对性的安保检查方案，导致有人将手机带入会场并录音，或拍摄会议材料。

二是未做好涉密会议保密提醒。微信是涉密会议期间发生泄密的主要途径，理应重点防范，但有的涉密会议主办单位没有汲取教训，未就手机、微信使用等提出专门要求，导致有人不知不会或心存侥幸。

三是未厘清涉密会议保密责任。发生泄密案的涉密会议，大多保密管理责任不明。会议既有主办单位人员，又有参会人员和服务人员，保密管理责任落实存在盲区，会前无人进行保密审查、会中不提保密要求、会后缺乏保密监管。

防范对策知多少

一要严格规范保密管理

会议召开前，应对场所内的电子设施、设备进行保密技术检测；为各工作组配备保密文件柜，为会场配置手机存放柜、手机和无线局域网干扰器等；禁止参会人员及工作人员携带手机、智能手表等进场，并通过电子屏、提示牌等设置明显的禁止带入提示。

会议期间，关闭会场区域移动通信信号和无线局域网接入设备，禁止对涉密文件、资料进行拍摄。

会议结束后，将需收回的涉密文件、资料全部清退、收回、核对登记，由指定部门统一销毁。

二要强化涉密会议召开前的保密教育

一是加强对会议工作人员的教育，由涉密会议主办及成员单位定期提醒；

二是对参会代表进行专题教育，强调管理要求，展示涉密会议微信泄密的典型案例；

三是对相关部门、人员进行针对性的提醒，特别是有可能接触到涉密会议材料的服务保障人员，杜绝利用手机拍照、摄录等行为。

三要狠抓涉密会议期间保密监管

就内部保密监管而言，涉密会议主办单位负有主体责任，要确保监管覆盖全员、全过程，发现问题及时纠正。

就外部管理而言，相关服务保障单位有巡逻责任，要根据自身职责权限牢牢把住涉密会议各环节，重点加强对计算机网络、移动通信网络的监管，发现问题及时补救处置。