切莫忽视指尖上的泄密

■张西成 刘金伟

近日，今日俄罗斯电视台网站报道称，俄罗斯国家杜马2月19日最终通过《军人地位法》修正案，禁止军人和参加军事训练的公民在媒体和互联网发布跟履职及军训相关的信息。

消息一出，关于信息化时代现代通信手段可能泄露国家和军事保密的问题再一次摆在世人眼前。当下由于信息技术的发展，尤其是自媒体时代的到来，每个用户可以随时随地发布消息、上传图片和影像，与他人分享信息。但凡事均优劣相间、利弊相伴。共享信息也是一把双刃剑，也许涉军的快门随手一按、涉密的指尖随意一点、涉战的言论随便一传，就为不法分子提供了可乘之机。数据显示，现在获取情报的渠道，有80%左右来源于公开信息，而这其中又有近一半来自互联网。

网络已成军事信息泄露的重要渠道，而大部分的泄露是“无意的”。有军事发烧友出于猎奇与炫耀心理，将一些部队现役装备车辆和演习场景拍照传至网络，引起大量的转发分享，有户外爱好者随手将涉足过的地方甚至是军事禁区拍照定位分享至网络，也有军人直播自己的生活区域。这些人认为自己不处在要害部位，不掌握核心机密，且网络安全是技术部门和专业人员的事情，因此主动防护的意识不强。殊不知，这些指尖上不经意的滑动，就很有可能将不法分子千方百计想要得到的信息“拱手相送”。

西方军事家若米尼认为，至少有一千种精神与物质的因素与战争直接相关。历史上，一张风景照、一幅导游图、一条新闻稿、一个通讯地址……这些日常生活中司空见惯的信息，却能在战争中发挥出奇的效果。

1983年10月，突然接到转向格林纳达执行登陆作战任务命令的美国第六舰队，虽然事先毫无准备，但凭借当地向游客出售的十分清晰和详细的导游图，顺利完成了登陆作战任务。格林纳达人为发展自己的旅游业而制作的精美旅游图，却成了引狼入室的向导、诱发战争灾难的“内奸”。

谋成于密而败于泄。军事秘密特别是核心机密，往往事关一个国家的底牌、命门，一旦失守将满盘皆输。从这个意义上讲，保密就是保安全、保打赢，绝不是一句戏言。

在由大向强阔步前行的征程上，我们需要一个和平安宁的国际国内环境。然而，我周边安全形势并不乐观。敌对势力对我军事机密的窥探、窃取一刻也没有停止过，并且花样不断翻新、手段不断升级。尽管我们远离了战场的厮杀，但随着网络社会化、社会网络化程度的日益加深，围绕军事信息夺取与反夺取、防护与反防护的对抗会更加激烈。面对严峻的挑战，我们的安全保密工作必须做到有备无患、万无一失。

机事不密则害成。传播精彩，谨防泄密。面对潜藏在信息之中的“潘多拉魔盒”，脑子里一定要绷紧保密这根弦。平时多一些保密意识、多一分防范责任，战时就少一些损失、多一分打赢胜算。互联网时代，严守用网保密规定，提高网络保密意识，应成为每一位公民义不容辞的责任和义务。

当心，潜伏在移动终端里的陷阱

■魏岳江 刘 鑫

近年来，随着信息化技术和通信技术的飞速发展，智能手机、平板电脑等移动终端走进了千家万户，走进了军营，为官兵获取信息、积累知识、沟通交流带来了诸多便利。5G通信技术的出现，又将给工作、生活、联系与沟通带来全新改变。

然而，移动终端是把双刃剑，其在提供智能化服务的同时，也在不知不觉中抓取使用者的位置、社交、账户等个人信息。因此，官兵在享受互联网红利的同时要清醒地看到存在的诸多泄密安全隐患，严格保守军事秘密，防患于未然，提高安全防范意识。

通讯录信息泄密不容小觑

移动存储设备使用日益便捷的今天，祝福信息正由贺卡等传统形式向文字、图片、视频结合的微信信息等多元化方式转变。军人在自编独具特色的祝福短信、利用网络编写电子贺卡或制作祝福视频时，有时会注明自己的单位、职务、姓名，甚至在其中泄露部队番号、军营驻地等信息。

部分官兵在手机通讯录或微信等社交平台上，将朋友、领导、同事的职务、单位、姓名等信息实名制存储标注，甚至备份至云端。存储在远程服务器上的数据，可能被不法分子非法浏览、拷贝或篡改，造成信息泄露。

此外，一些官兵聊天谈论涉军信息时，虽然用拼音、谐音代替敏感字段，但被稍微有一点军事常识的人读几遍就能知道大概内容，极易发生失泄密事件。

安全提示：

关闭或停用智能手机自带的上传云端功能，防止数据自动传输。

存储电话号码和备注社交平台好友信息时，尽量简化对方信息，或用仅自己理解的“密码”形式标记记录，降低通讯录泄露风险。

在网络上交流聊天中，不要谈论涉军信息和工作情况。

各单位建立的局部微信群，尽量使用单位编码、机构代码。

送节日祝福时，可在不涉及军事秘密的情况下，在祝福语言后面写上自己名字。

随手拍的照片不可小视

随着移动存储设备的普及，智能手机拍照、拍摄视频成为工作生活中的常态。殊不知，随手拍摄上传的照片、视频，就有可能被网络间谍盯住。

因为警惕性不高，擅自在社交平台上传身着军装或有军事装备武器背景的照片，更有甚者因其手机存贮空间不足，就把涉密照片放到网上加密文件夹，很可能被不法分子窃取利用。即使给文件加密或删除文件也容易被破解或恢复，不能保证信息绝对安全。

基于此，2月19日，俄罗斯国家杜马通过《军人地位法》修正案，要求不能传播与履行军人职责相关的照片、视频、地理位置等信息。《中华人民共和国军事设施保护法》也明确规定，除军事机关批准外，军事禁区等特殊地点和场合禁止拍照。

安全提示：

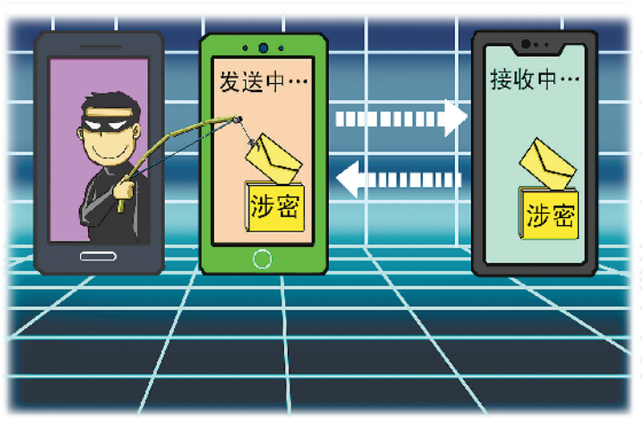
不要在工作地点、训练场所用手机拍照录像，不得对涉密资料进行摄像拍照。

不要将手机带入重要会议、涉密场所，如确需带入，要将手机电池取出，或者将手机统一暂时存放在远离会场的地方，防止手机被远程监控。

参加军事演习、执行涉密任务等特殊情况下，智能手机要实行统一保管，分发到个人时，手机摄像等功能要按规定关闭。

使用过的智能手机不可随意转让，必须经保密部门审查处理方可丢弃。

切勿让涉密文件“网上冲浪”



出于传送文件的便捷性，社交软件和电子邮件是现代人工作信息交流的重要媒介。殊不知，文件在网络中传送时会经过千千万万个节点，一旦被“黑客”利用服务器发起攻击，短时间内即能侵入移动终端获取文件信息。

2016年，美国民主党全国委员会网络被黑客组织入侵，近2万封电子邮件被维基解密披露，影响了美国大选局势。2017年6月，英国议会电子邮件系统遭到攻击，泄露至少90个由弱密码保护涉及国会议员及工作人员的电子邮件账户。

涉密文件历来是敌对势力利用恶意程序窥视和窃取的重点对象。即使文件上传后被立即删除，也可利用数据恢复技术复原。因此在使用社交平台和电子邮件进行工作交流时，涉及国家、军事机密的信息，决不能随意透漏。

安全提示：

涉密内容不通过微信群等社交平台和商业电子邮箱传送，尽量当面传达或使用保密电话。

不要打开陌生人发来的邮件和链接，防止感染木马病毒，导致手机或者电脑文件丢失甚至硬盘损坏。

要安装专业杀毒软件，及时升级，防止病毒侵入窃取邮箱密码。

切忌将手机电脑作为“U盘”存储涉密文件。

定时清理聊天中和邮件附件留下的图片、文件等临时文件，防止被非法截留、获取。

网络聊天小心误入钓鱼圈套

从目前侦破案件来看，被境外间谍情报机关通过网络勾连渗透策反的手段主要是以金钱为诱饵，对象是那些急需钱的人，途径是利用互联网聊天工具和社交媒体，伪装成军事爱好者、招聘猎头等身份，广泛活跃于各类军事论坛、社交、征婚、求职等网站，主动与网民聊天、帮助解决困难、提供就业机会等，逐渐拉近关系，一步步将网民拉下水。

基于此，许多发达国家和军队都相继建立健全社交媒体保密制度。美军颁布规范社交网络行为的6条基本准则中强烈建议不要加陌生人为好友。以军为防止社交媒体泄密发布命令，包括高级将领在内的所有以色列军人一律禁止使用社交软件，以防敌对势力渗透进以色列安全系统和国家机密被泄露。

安全提示：

安全设置微信个人头像，不使用着军装照片。

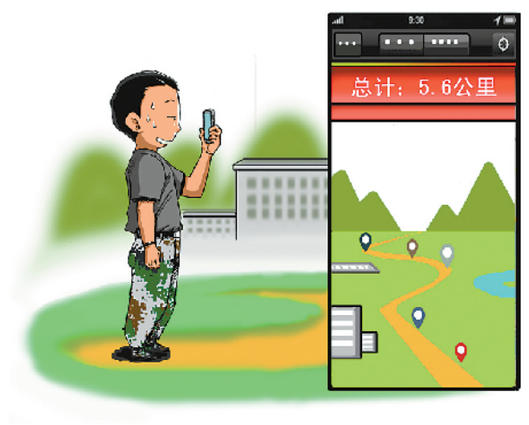
社交平台注册个人信息时，不使用军中术语，在地区设置上，选择范围广的地理位置信息，比如中国、美国等。

在社交平台添加好友时，设置要求对方需要验证，不要添加不知底细的陌生人为好友。停用“漂流瓶”“摇一摇”“附近的人”“允许陌生人查看十张照片”等功能，以防被不法分子翻看到重要信息并加以利用。

不要在招聘网站上以军人、军人家属或者子女身份发布求职信息，严禁暴露部队番号、单位驻地等详细简历及联系方式。

拒绝参加网上实名注册的各种抽奖、答题活动和非官方组织的有关政治、外交、军事等方面网上有奖征文等活动。

警惕定位软件泄露隐私信息



随着移动终端设备的普及，各类网络安全威胁也向移动终端转移，如不加识别就随意下载App，就可能成为网络间谍窃取用户个人隐私和信息的目标。

拿健身定位来说，由于用户在跑步锻炼时习惯打开健身定位，而在回家或到单位后将其关闭，在无意中就将自己住宅或单位的位置信息上传至软件后台。一家荷兰媒体就通过运动追踪器Polar准确找到了美国特工处特工、美国国家安全局特工、英国军情六处特工及众多国际秘密组织成员的确切动向和活动地点。

基于此，美国国防部发布禁令，禁止外派现役人员使用健身追踪器、智能手机和相关App的地理定位功能。俄罗斯国家杜马通过《军人地位法》修正案，军人在履职时禁止使用可联网的，可传送照片、视频、定位数据的电子产品。

安全提示：

通过官方渠道下载应用软件，禁止来源不明的软件安装请求，谨慎登记姓名、年龄、生日、手机号等信息，防止落入被间谍组织设置的钓鱼软件圈套。

不要在App或者网页端记录账号密码，养成定期修改密码的习惯，防止账号被盗。

及时升级更新移动终端系统，提升安全系数。

不要轻易打开诸如营销奖励、扫码送话费、寻人捐助等相关的链接和小程序。

严禁军人在驻地营院、健步走时打开移动终端的地理定位功能，防止被跟踪定位，暴露部队驻地位置信息。

授予应用软件程序权限时，注意严控访问个人隐私和网络的权限。

不用军队配发的保密手机连接互联网，做到办公专机专用。

莫让军事类自媒体沦为泄密号

在人人都是麦克风的时代，涌现出一大批军事类自媒体，筹办主体既有官方平台，也有不少退役军人、军事爱好者等。不可否认，这些新媒体为军队、军人发声等方面发挥了重要作用，取得了良好的社会效果。但同时，由于新媒体具有传播速度块、范围广的特点，一旦有涉密信息发布，即使及时撤回，网络上仍可找到蛛丝马迹。

2013年9月14日，美国《时代》杂志网站刊登了一篇文章，公布我国首艘航母辽宁舰的分析报告，这些资料完全来自中国网民公开发表的博文和图片。自媒体不经意间“揭秘”的文章照片，可能就把国家和军队秘密“拱手送人”。

安全提示：

个人和单位给相关自媒体投稿时，应严格按照有关要求把好审查关。

军事类自媒体从业人员应注重提升自身媒体道德素养，熟悉《中华人民共和国保守国家秘密法》《中国人民解放军保密条例》等保密规章制度，把握军事新闻报道的度。

军事类自媒体在报道相关内容时应严格把关，不得随意公开涉密的重大任务和军事活动图片，不得出现部队番号、编制、武器装备的性能、相关保密数据等，严防失泄密。

公众发现有泄露军事秘密危害国家安全的信息，可及时登录网络涉军违法犯罪和不良信息举报平台进行在线举报。

本版漫画：曹修武