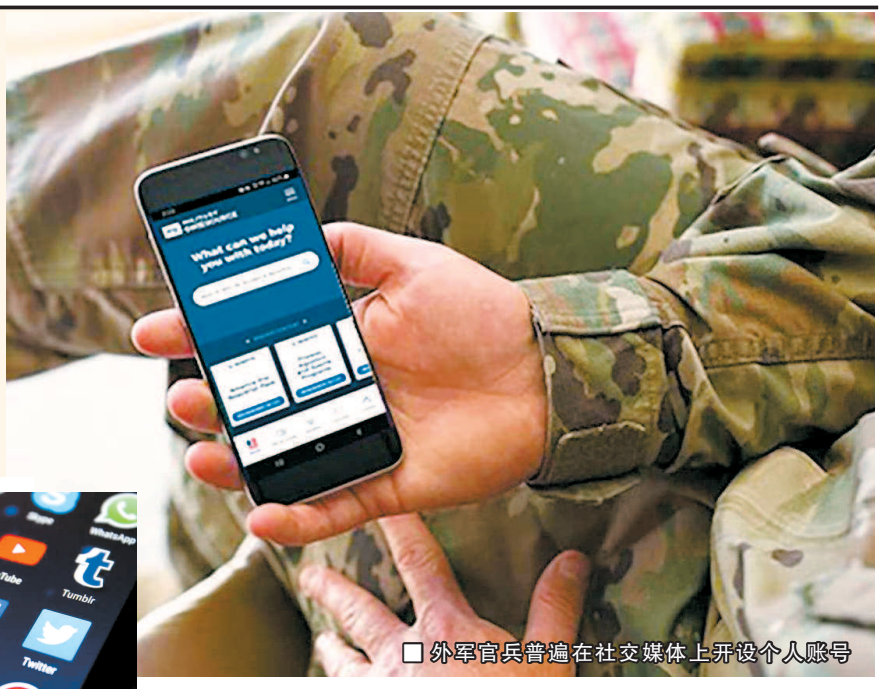

■ 各国军方对社交媒体“既爱又恨”



■ 外军官兵普遍在社交媒体上开设个人账号

『禁』还是『不禁』？

各国军界为网络社交媒体费心思

“三军之事，莫重于密。”随着网络社交媒体兴起，各国军队防间保密工作面临新的挑战。日前，美欧军队又发生多起社交媒体泄密事件，引发外界高度关注。

■ 俄军禁用智能手机的宣传画

一把“双刃剑”

对军队而言，社交媒体可谓“双刃剑”。如果利用得当，社交媒体不仅可以稳定军心士气、提高部队公共信息传播效率，还可以提升军队形象，加强征兵工作成效。例如“Z世代”（出生于1995年至2009年的人群）是美国军队征兵的主要对象，他们在分析决策时所依据的信息来源不再是传统媒体或谷歌、必应等传统互联网搜索引擎，而是依靠Tiktok等大量社交媒体用户发布的信息。在“Z世代”眼中，社交媒体上的内容要比其他来源更具可信度。因此，美军将社交媒体平台作为提高征兵工作有效性的重要途径，成为管理和宣传军队的一个有效途径和载体。

但由于社交媒体鼓励人们在线分享生活，用户的各种私人信息基本处于“不设防”状态，军事人员特别是“Z世代”士兵大量使用社交媒体给行动安全和情报安全带来了巨大压力。美军去年底的一项调查表明，军人每天在社交媒体上花费的时间要比平民更多。有“数字原住民”之称的“Z世代”士兵更是如此，他们从未经历过没有智能手机的日子，社交媒体不仅是他们的娱乐来源，更是他们的生活方式，是生活中不可或缺的组成部分。据美国情报部门统计，近年来，通过社交媒体获得的情报在各国情报部门开源情报中占比越来越高。2023年，20多岁的美国国民警卫队成员杰克·特谢拉在社交媒体Discord上泄露了大量美国国防部机密文件，2024年11月被联邦法院以“故意保留和传播国防信息”罪起诉，并获刑15年。在特谢拉“Discord泄密事件”之前，类似的事件时有发生，例如2022年“战争雷霆”（War Thunder）游戏社区就曾出现被英国国防部列为机密的挑战者-2坦克手册，还有一名自称法国军人的用户上传了法国勒克莱尔坦克的机密手册。

多个“风险源”

“Z世代”军人往往将他们入伍前的社交媒体习惯带入军旅生涯，因此除了密码遭破解、账号被盗的风险外，那些不经意间发布的信息本身也存在多种泄密“风险”。

一是敏感信息直接泄露风险。军队人员在社交媒体进行分享时如果警惕性不高，就可能无意之中泄露一些关于军事组织、战术或行动的敏感乃至机密信息。不久前，一名以色列士兵在更新社交媒体X上时写道，“周三我们将清洗Qatanah（靠近拉马拉市的一个村庄），如果一切顺利，周四就能回家了”，同时其账号个人资料中包含了所在战斗单位的名称，这样就泄露了以军突袭计划的时间和地点，最后导致行动临时取消。

二是地理位置间接暴露风险。即使所发布的照片或媒体看似“无害”，但其嵌入的隐藏元数据包含了照片或媒体的制作时间、使用设备，特别是位置（地理标记）信息。对普通人而言，这些信息可能毫无用处，但“有心人”可能从中获取某些设施、装备、人员的部署位置、隶属关系等敏感信息。此外，X等社交媒体程序本身就提供了地理位置定位服务，有些移动应用程序还会跟踪用户的活动轨迹。2018年，由于大量军人使用户外健身应用程序Strava并上传个人锻炼数据，导致美军驻阿富汗军事基地和秘密哨所的位置及人员配备情况“公之于众”，有人甚至称，根据上传的活动轨迹，“可以在美军最不经意的时候对其实施伏击”。

三是关联信息聚合风险。用户在社交媒体上往往会公开电话、地址、朋友圈、个人动态等信息，而且不同用户间会存在多种关联，因此在社交媒体上进行数据挖掘并非难事。通过把这些信息聚合汇总成“更大的图景”，有经验的分析员便能从大数据中“挖出”一些本难以获取或根本不可能获得的信息，如岗哨轮换、军事演习、部署变更等高价值军事情报，甚至通过进一步分析判断出社交媒体用户所在部队承担的任务、战备情况和作战能力。

此外，还存在成为“网络钓鱼”目标的风险。由于社交媒体上用户个人信息真假难辨，因此完全可以通过创建匿名或虚假身份来获取情报。几年前，北约战略通信卓越中心在演习期间进行了一项实验，通过社交媒体找到演习参与者，并引导其加入一个看似与该演习有正式关联的社交媒体X群组。最后，实验人员不仅获得参演士兵及其战友的联系方式、照片以及所属部队的准确位置，还成功说服一些士兵脱岗。据英国军情五处去年曾披露，过去5年中，敌对国家在LinkedIn平台上对超过万名英国涉密人员（通常拥有高级安全许可）实施“网络钓鱼”。印度军方也在社交平台发现了150多个冒充精神导师或美女并试图获取敏感信息的账号，2020年有11名印度海军士兵落入此类“桃色陷阱”，向那些用美女照片当头像的账号毫无保留地透露大量机密。


■ 社交媒体存在泄密风险


■ 印军砸毁收缴的军人智能手机

各有“过墙梯”

对于如何防止年轻官兵在社交媒体上失密泄密，世界各国军队的应对之法不尽相同。

有的以“封堵”为主，严格控制军人使用社交媒体。俄国防部要求军人不要使用网络社交媒体，2019年俄国家杜马还修订法律，规定除从事宣传工作的军人外，其他军人不得在互联网发布视频、照片等个人信息，同时还明确禁止军人在服役期间携带智能手机、平板电脑、电子手环等可接入互联网的电子设备。印军也于2019年要求所有人员在工作中不要使用WhatsApp，且不得加入类似社交平台的大型聊天群组，更不能在网上发布照片或透露军人身份，所有军官必须注销账号。2020年，印军还进一步“加码”，直接要求所有军人卸载89款手机应用软件，连一些网购、音乐甚至杀毒软件也不放过。更有甚者，印军还曾出现过为防止士兵使用社交媒体而“没收手机并当场砸烂”的例子。

有的则试图在运用社交媒体和保密之间找到平衡点。美军也一度禁止在军内使用个人社交媒体，但2010年美国国防部发布“负责并有效地运用基于互联网能力”备忘录，为社交媒体禁令画上句号。同时，为更好指导官兵正确、安全使用社交媒体，美军除了加强教育强调“虚拟世界不虚拟”，还发布了一系列操作性较强的规范性文件，如国防部发布《社交媒体官方使用标准化操作程序》，各军种也发布了各自的社交媒体使用规范和指导手册。以美国陆军为例，其39页的《陆军社交媒体手册》不仅涵盖社交媒体介绍、账号注册等使用说明，还列举了军事人员在使用社交媒体时的注意事项和风险提示，例如不要公开家庭地址、电话号码，不要提及出发和返回时间等行程安排，不要发布穿军装的照片，特别是在部署、训练或执勤时不要使用有定位功能的社交媒体应用程序，执行任务期间要关闭智能手机的GPS功能等。同时，美军还积极在社交媒体X、Youtube、Flicker等平台打造自己的社交媒体账号，并面向军内用户开设了Milblog、Milbook等军队社交媒体网站。此外，美军还建有军人社交媒体监控体系，如成立了“军事网络风险评估小组”，通过技术手段对军人使用社交媒体的情况进行监控，以便在发现泄密“苗头”时及时处理。

梁君 孙文静 李杰

军情揭秘

●国内邮发代号3-5/国外发行代号D694/全国各地邮局均可订阅/广告经营许可证号:3100020050030/社址:上海市威海路755号/邮编:200041/总机:021-22899999转各部
●本报印刷:上海报业集团印务中心等,在国内外6个印点同时开印/上海灵石、上海龙吴、上海界龙/北京、香港、美国洛杉矶
●本报在21个国家地区发行海外版/美国、澳大利亚、加拿大、西班牙、泰国、菲律宾、日本、法国、巴拿马、意大利、荷兰、新西兰、尼日利亚、印度尼西亚、英国、德国、希腊、葡萄牙、捷克、瑞典、奥地利等
24小时读者服务热线 962555
本报零售价 每份1.00元