高技术前沿

这是一个颇为矛盾、颇有争议的话题。一方面，受健身软件泄露军事基地位置影响，美国国防部正计划禁止相关人员使用智能手机；另一方面，考虑到智能手机出色的软件运算能力，美国国防部近期又决定为美军发放苹果手机，以便为单兵提供及时准确的战场信息。据悉，这也是美军构建“云作战”模式、保证战场数据信息共享的重要组成部分。

功能越来越丰富的智能手机，将在未来战场扮演指挥控制、通信导航、侦察监视等多种角色——

军用版智能手机离战场还有多远

■张玉民 许妍敏

研发战地智能手机成时尚

近年来，随着通信技术的快速发展和应用软件的不断丰富，智能手机性能日新月异，扩展功能愈发丰富。就在智能手机深刻影响日常生活的同时，美国军方也敏锐地捕捉到智能手机的潜在军事应用价值。

早在2009年，美国陆军一位高级将领就曾公开表态：“智能手机可以帮助美国陆军实现部队及装备的快速移动部署。”美国国防部用以代替黑莓手机的苹果智能手机，也将成为美军新一代通信设备，美军计划使其成为构建“云作战”模式、保证战场数据和信息顺畅传输的重要组成部分。

将高科技民用电子产品“改头换面”后推向信息化战场，美军一向把“拿来主义”发挥到极致。美国陆、海、空三军都制定了各自的军用智能手机发展规划，美国国防部打算使用超过60万部移动通信设备，其中包括已经配发航空部队使用的约4.1万部苹果智能手机。

智能手机成为美军的“战场神器”，还是近些年的事。2008年，美军曾为在阿富汗和伊拉克执行任务的部分官兵配发了iPad平板电脑。这些“制式”iPad电脑中详细储存了任务清单、当地人日常用语和地图等信息。利用平板电脑中储存的语音，美军官兵甚至可以直接与当地军民开展交流。美国雷神公司还曾研发过一款名为“雷神智能战术系统”的智能手机，能通过向官兵传输图片和视频的方式，有力提升单兵从信息枢纽中获取战场态势的能力。

近年来，美军对于研发战地智能手机的投入不断增加。2010年，美国国防部高级研究计划局开始对智能手机应用软件进行招标。美国陆军也通过“军队应用”挑战项目，进一步丰富智能手机的军事应用。此外，美国国防部高级研究计划局还专门立足“安卓”系统打造高安全保密性的战场军事通信终端，载体同样是智能手机。

在美军列装的“内特武士”单兵移动云通信指挥系统中，同样可见智能手机的身影。“内特武士”系统由一个酷似智能手机的触屏面板和无线电装置组成。安装在胸前或前臂的“智能手机终端”可用来发送短信和语音通话，还能显示周围地形、友军和目标位置。

那些“脑洞大开”的战场应用

近年来，智能手机在美军的军事行动中频繁“现身”。

在美国陆军举行的“远征勇士”演习中，无人机摄像头捕捉到对方设伏的情况后，美军士兵通过智能手机快速接收到从无人机传回的坐标。在美国国防部高级研究计划局开展的智能手机应用研究中，还出现了帮助狙击手计算射击数据、通过地图软件追踪目标、协助战地医疗诊断等“脑洞大开”的应用，有的应用早已被美军实地测试。目前，军用版苹果手机已经开始了多样化线上应用支持，最受士兵欢迎的应用软件包括用手机拍摄街道照片获取相关信息、嫌疑目标生物数据库比对等。

智能手机上战场的优势在于，它能驱散战场迷雾，成为战场态势感知的得力“参谋”。通过使用智能手机，作战人员可实时接收各种侦察系统获取的情报信息，形成综合、全面的战场态势感知。美军目前已具有通过智能手机获取2公里范围内所有卫星图像及空中、地面侦察情报的能力，甚至还能与战友实时共享战场态势，更好地协同作战。美国波音公司已经研发出战场嫌疑目标专用抓捕程序，只要打开手机拍下待抓捕人员的照片，就能将相关信息与战术作战中心和情报人员实时共享。未来，手握智能手机的士兵不但可以用短信报告战场周边环境，还能配合卫星导航进行“战场直播”，远在千里之外的指挥部可以据此完成对打击目标的匹配制导，从而开启战场远程打击的新模式。

其实，智能手机还是武器火控和射击瞄准的“掌中宝”。美军已经研制出将苹果智能手机与扳机控制系统融为一体的智能瞄准器，可在感知各项参数后修正射击诸元，甚至还能将射击弹道在屏幕上显示出来，让“人人都可以当神枪手”成为现实。同时，给智能手机安装专用软件后，还可以作为无人机、无人战车和机器人的遥控器。当你看到士兵在战场上“玩手机”，说不定他正在操控无人机作战。

此外，智能手机还可广泛应用于战时物资管理、战场装备抢修、战地卫生救护等领域。大量应用软件，可以让士兵在手机指导下进行体能锻炼、调整饮食和获取心理援助。

为智能手机戴上安全“紧箍咒”

智能手机虽好，并不意味着在战场上就可以高枕无忧地使用它。俄罗斯国防部之所以从今年3月1日起抛弃智能手机，要求军人只能使用简单的按键手机，就是智能手机泄密惹的祸。

喜欢自拍的俄罗斯士兵先后泄露了俄军进入乌克兰作战、“库兹涅佐夫”号航母机库内细节和俄军驻叙利亚赫梅明空军基地装备损坏等诸多秘密信息。帮了西方情报部门“大忙”的智能手机，自然被俄军拒之门外。无独有偶，热衷于上传健身数据的美军也在智能手机上栽过跟头。一款健身软件的“热力地图”竟然把美军的诸多海外秘密军事基地公之于众，对美国的海外军事基地安全产生了不小的影响。

智能手机上战场，就必须时刻为其戴好安全“紧箍咒”。智能手机的安全远不是终端用户所能决定的，真正的安全核心由无线服务供应商和操作系统发行商共同掌控，必须确保软件和数据传输的安全稳定。苹果手机之所以迟迟未能成为美军的“制式手机”，其中一个重要原因就是操作系统一度没有通过安全检测，无法正常连入军用网络。此前采购的近3000台iPad平板电脑之所以被美国空军特种行动部队“退货”，就是因为这款平板电脑中安装了由俄罗斯研制的阅读软件。美军对操作系统和软件安全的重视程度由此可见一斑。

为确保智能手机只有本人才能使用，美军已经开展了指纹或虹膜扫描等生物识别技术研究。除程序安全和使用安全外，美军还计划在智能手机中运用防破坏技术等安全手段，通过完全锁住装置和遥控数据归零等手段确保带入战场智能手机的安全。

战场上使用智能手机，更需要一个安全稳定的网络覆盖。战火纷飞的战场上，传统基站很难为手机提供稳定的信号。目前，美军已经研制出一种在手机上配置的天线触角，可提高接收地面基站或空中网络信号的能力。为确保能在恶劣战场环境下使用，参加实战的智能手机往往还需要进行防风沙、抗摔打等加固处理。军用智能手机离战场还有多远，还有待观察。

制图：徐 鹏

科技云

科技连着你我他

■本期观察：崔功荣 黄武星

植入“间谍”驱癌魔

如果把癌细胞比喻成不法分子，肿瘤就是不法分子拉帮结派组成的不法组织，它不仅能无限增长、危害生命，人体免疫系统和药物治疗还难以攻破其壁垒。目前对肿瘤的主要治疗手段副作用比较大，无论是化疗还是手术，都难免“伤敌一千自损八百”。如果能安插“间谍”携带药物打入“不法组织”内部，消灭肿瘤岂不轻松许多？

哈佛医学院的研究团队还真找到了“间谍”癌细胞的研制办法，并将研究成果发表在《科学转化医学》上。他们筛选出一种能与多种癌细胞表面特定受体结合且能诱导癌细胞死亡的配体分子作为武器，再寻找没有这种死亡受体的癌细胞作为“间谍”，将“武器”基因植入“间谍”基因序列中，一个释放致命“武器”的“间谍”癌细胞制作而成。由于癌细胞具有“归巢”特性，“间谍”癌细胞注射到体内，它将通过循环系统自动找寻肿瘤区域驻扎，释放配体分子将肿瘤消灭光。

植入到“间谍”癌细胞基因序列里的不仅有“武器”基因，还有自毁程序，一旦体内肿瘤清除，只要注入对应药物，“间谍”癌细胞便集体毁灭，以防二次致癌。

重新编码除“艾滋”

人类抗争艾滋病的几十年时间里，一直对这种新型病毒束手无策，艾滋病也成为真正意义上的绝症。不久前，美国《分子治疗》杂志刊登的一项研究成果给这场艰苦卓绝的抗争带来了希望。

科学家在长期研究中发现，艾滋病毒感染人体T细胞需要和T细胞产生的某种分子结合，如果将编码该分子的基因组进行修改，就相当于断了艾滋病的感染通道。于是，他们对造血干细胞进行基因改造，使其制造出的T细胞无法编码出该分子，让艾滋病毒面对改造后的T细胞无从下手，新型T细胞也就对艾滋病毒攻击产生了免疫，成为灭杀艾滋病毒的中坚力量。

在实验中，科学家发现改造后的造血干细胞能长期存活在骨髓中，并源源不断地制造具有艾滋病毒抗性的T细胞，并明显抑制了艾滋病毒在试验动物体内的发展。相信在不久的将来，这项技术将会不断完善，最终能彻底消灭人体内艾滋病毒。

让糖尿病“一贴没”

控制血糖不再打针吃药，只要一个小小的皮贴片就能解决！不久前，刊登在《自然通讯》的一项研究成果让这样美好的愿景可能成为现实。

他们以人体肾脏细胞为改造对象，通过加入不同功能的基因，得到一种能实时监控血糖含量并释放胰岛素的多功能细胞。该细胞对血液中的葡萄糖十分敏感，一旦监测到血糖异常升高或者超过阈值，就会立刻释放胰岛素，促使血糖含量恢复正常。为避免被人体免疫系统“错杀”，研究人员利用纳米多孔胶囊将这种细胞“捆”在一起，制成皮贴片植入病人皮肤。

这样检测和补偿“一条龙”服务的强大功能，可以与胰脏中的胰岛相媲美，甚至能完美地替换胰脏的部分功能。目前，皮贴片在人体内的有效时间约为三个星期，研究人员正努力延长有效时间，让患者生活更方便。

让科研生态风清气正

■范瑞洲 张宏烨

论 见

中央军委科学技术委员会日前发布《科研诚信倡议书》，在全军倡议科研诚信，不仅是对科研人员的一次思想洗礼，还是对科研工作的一次除污清流，必将产生深远影响。

强调科研诚信，本质是坚守科研的底线。科研的目的就是探索和揭示客观事物的内在本质和运动规律，其基本态度必须坚持实事求是、一切从客观实际出发，这是科研工作的逻辑起点。如果科研工作做不到诚信、做不到实事求是，不能一切从客观实际出发，那么也就失去了其存在和运行的内在逻辑，科研工作及其成果也便没有任何价值可言。只有坚守诚信底线，科研工作才具有科研行为的基本特征，才具有鲜活的生命力。

强调科研诚信，核心是科研人员要讲诚信。科研失信行为的背后，是科研工作者态度和思想上的模糊和认知偏差。要确保科研成果真实可信、科研行为干净可靠，关键还是要引导科研人员树立“科学最重、名利最轻”的正确职业道德观。只有科研人员思想诚实可信，科研行为才能实事求是，科研成果才能真实可靠。

强调科研诚信，关键是清除科研的“毒瘤”。科研诚信并不是新要求、高要求，而是对科研人员和科研工作的最基本要求。在全军范围内倡议科研诚信，说明科研失信行为在全军科研工作中在一定程度上仍然存在。强调科研诚信，就是要彻底根治科研人员思想浮躁化、功利化，科研工作商业化、表面化，科研成果虚假化、交易化等不良倾向，还原风清气正的科研生态。

科研是强军兴军的重大动力牵引，事关国防和军队全面建设，事关能打仗、打胜仗，容不得半点虚假。科研失信行为不仅败坏了科研风气，也容易挫伤科研人才的积极性，阻滞科研创新，甚至影响到强军兴军进程。强调科研诚信，根本目的就是要挤干科研成果的水分，保留和激励具有真才实学的科研人才，调动科研创新的积极性，夯实强军兴军的根基。

云计算：没那么容易

■林岩峰

热点追踪

云计算被看作继个人计算机变革、互联网变革之后的第三次信息技术浪潮，已成为全球信息产业关注的焦点。云计算的应用和发展将推动低成本、泛在、智能、便捷的信息服务体系建设。对云计算工作者来说，在实践中应认清以下五个特点。

大的数据中心还不是云数据中心。有人认为数据机房摆满各类服务器，拥有大量计算、存储设备就可以对外宣称是云数据中心，这是不了解其弹性、可计量、按需自助以及资源池化的特性。云数据中心融合数据中心和云计算技术的优点，可实现信息技术资源的高度虚拟化和各类服务管理程序自动化。如果只是一个大的数据中心，没有实现云计算基础架构，只能提供托管服务，就无法应对突然爆发的工作负载。

非云应用迁移至云端不是易事。将应用软件托管至数据中心，就好比一座雕像整体从A处搬到B处，相对来说比较简单；而迁移至云端，需要拆解组装，过程复杂得多。传统应用软件对硬件和软件平台有很强的依赖性，无法迁移至云端，进而享用云基础设施的好处。军队云数据中心初期不能全盘云化，要考虑到军队系统软件的实际情况。随着军队软件逐步推广云架构设计，同步推进云数据中心的全面云化工作。

云计算资源可以无偿使用但不能无限制。云计算资源通过网络以按需、易扩展的方式提供，像水、电资源一样能够被方便获取。地方云计算资源参照水、电的商业模式计价收费，但军队云数据中心只为军事单位服务，地方商业模式无法照搬。地方云数据中心能做到按需提供且不加限制，是因为用户会考虑成本因素，不会无节制申请。军队云数据中心在正式运转前一定要考虑清楚对外的运维模式，否则后患无穷。

云安全不是云数据中心单方的责任。在云计算发展早期，云计算被认为非常不安全，不少人拒绝考虑公有云，选择搭建自己的私有云。后来，人们认为云数据中心会为他们考虑所有的安全问题，便放心地将各种带有安全漏洞的软件部署在云中。云安全需要建立在好的软件设计基础上，如果有适当的软件安全架构，公有云比绝大多数本地数据中心更安全。各单位软件开发团队一开始就要对云安全有足够多的认识，多些未雨绸缪，少些亡羊补牢。

不能低估云计算推广难度。虽然人们普遍认识到云计算是信息技术发展的必然趋势，会给单位工作带来益处，希望云计算尽快落地。但云计算在推广过程中必然会带来工作流程、人员编制等多方面改变。组织的变革如果迟滞，将给云计算推进带来巨大阻力。特别是已有大量信息基础设施和维护人员的单位，云计算推广的难度更大，各项配套的法规制度、政策措施必须跟上。