

为赢得键盘战 给游戏“纠错”玩家屡次泄露军事机密



战争类游戏《战争雷霆》尽力提高各种道具的真实度，让骨灰级军迷们大呼过瘾。

英国“挑战者”坦克维护指南被公开

然而，这种事已经不是第一次发生了。几个月前的7月14日，一名英国军人玩家对《战争雷霆》的游戏设计师“没有”为英国现役的“挑战者二号”坦克正确建立模型感到不满。这名玩家声称自己是现实中“挑战者二号”坦克的指挥官和枪械指导员。他认为，游戏《战争雷霆》中的坦克建模是有误的，游戏设计师们没能把这款坦克“忠实地重现在游戏中”。

为了支撑他的言论，这名玩家上传了官方发行的《挑战者二号军队装备整理指南》——一本维护指南和手册。虽然他泄露的文件经过了部分删减，有一些内容被大片大片地涂黑掉，不过还能在文件中看到有着被叉掉的“英国机密”印章和“文件解禁”的印章。该玩家还表示，此文件来源于一辆驻扎于

英国威尔特郡基地的坦克中，该基地由使用“挑战者二号”皇家坦克团驻守。除了附上材料外，该玩家还详细解释了他认为应该如何修改以使坦克设计更逼真。

被告知“仍是机密”
面对这份材料被公开的情况，《战争雷霆》所在的公司及时联系了英国国防部，后者确认那名玩家分享的材料仍是机密。据报道，英国国防部的国防装备和支援分部已经阅读了上传的文件，并称其看起来像是“真实的原版文件”，“这很明显没有在自由信息计划中被公布，也没有考虑过删减。”

《战争雷霆》的开发公司并没有感谢这名玩家的贡献，而是把这些文件从论坛中删除，并因该玩家在网站上分享机密文件而对其予以处罚。

一名网站发言人称：“我们已经说清楚过，我们不会使用任何没有对公众开放、没有被完全地、合

法地解禁的文件。”“我们已经和英国国防部确认过这些文件仍然是机密文件。如果继续散发此文件，你将会违反在泄密文件首页中标明的《国家机密法案》。如果被逮捕，违法者可能会面临最高14年的监禁。你的每一次转发此文件，你把我们，特别是每一个英国公民，置于危险之中。”

英国国防部拒绝评论
更重要的是，“挑战者二号”坦克仍然是英国国防计划的重要组成部分。并且，英国陆军近期宣布了其将拨款八亿英镑来为挑战者坦克进行升级改装的计划。对此，一名英国国防部的女发言人说他们不对此事件发表任何评论。她接着说到：“我们十分重视所有的违规泄露机密的行为。如果适宜，本事件将会被评估并开展调查。相应措施将会部署到位，防止此类事件的再次发生。”

(上接p08版)

《战争雷霆》背后公司 痴迷“二战”场景游戏

《战争雷霆》诞生于2012年，是一款在线多人对战的战争类游戏，世界上成千上万来自各个国家的玩家可以同时操作战机、地面载具和战舰进行游戏。它由俄罗斯最大的游戏发行商Gaijin Entertainment开发，制作并发行。发展至今，这家俄罗斯游戏公司已成为一家非常欧洲化的公司，其总部设在匈牙利布达佩斯。除了俄罗斯之外，该公司在塞浦路斯、德国、拉脱维亚均设有办事处。

Gaijin Entertainment由来自俄罗斯的双胞胎兄弟安东·尤金采夫和基里尔·尤金采夫共同创建，安东担任总裁和首席执行官，基里尔当创意总监，这样的格局维持至今。团队中的许多人都对二战情有独钟，并具有多款二战游戏的开发经验。“战争是恐怖的，基本上没人愿意参战。然而，那些军事载具——飞机、坦克、战舰——真的非常动人，特别是对男性玩家而言，”安东如此解释制作二战游戏的愿景。当然，《战争雷霆》本质上是一款面向全世界的电子游戏，而非为军方开发的模拟游戏。后者会尽全力提高真实度，这让骨灰级军迷们大呼过瘾。



斯特拉瓦软件公布的运动轨迹泄露了军事基地的位置。

新闻链接

运动软件成为泄密工具

在任何一场战争中，情报工作都是打胜仗的前提条件。随着互联网的发展，情报获取方式也在不断更新换代，一款用于记录健身者运动轨迹的软件——斯特拉瓦，就向人们展示了一个获取情报的新途径。2017年11月，斯特拉瓦用2年时间积累的用户数据，制作发布了一幅“全球运动热力地图”。然而一名20岁的澳大利亚学生纳森·鲁泽研究这份热力图后，通过分析特定区域的一些运动轨迹，找到了美俄等国设在叙利亚、伊拉克和阿富汗等国的基地，有的从未向外界公布过。

暴露规模以及建筑物分布

据报道称，纳森·鲁泽公布他的“发现”后，越来越多的基地通过这种途径被“挖掘”出来，其中包括美国中情局在索马里摩加迪沙的基地、俄罗斯在叙利亚的赫梅米姆空军基地等。而且，从“热力地图”的轨迹中，能看到的不仅仅是基地的位置，基地内部的人员轨迹也清晰可见，专业人士可以从中研究出这些军事设施的运转方式。

一位名叫尼克·沃特斯的前英国军官，在这幅“全球运动热力地图”中找到了自己当年在阿富汗服役时驻扎过的基地。他气愤地指出，这是军队“在作战安全和人员安全方面的重大失败”，因为巡逻路线、基地位置及其他信息，“都可能被用作实施袭击的情报”。敏感军事设施的地理位置还不是唯一的风险，更重要的是军事人员的训练生活习惯以及部队的调动。不少士兵经常围着一些特定建筑或者路线慢跑，间接暴露了基地规模以及建筑物分布。安全分析师托拜厄斯·施耐德表示，这些数据可以为有意攻击美军的人提供便利。他还补充道，“这是很明显的安全威胁，因为你可以看出一个人的生活模式。”

轨迹信息泄露了军事机密

与传统获取情报方式相比，从斯特拉瓦运动软件的轨迹中获取这些信息，并没有使用任何隐蔽手段。据报道，“热力地图”上显示出的不少军事基地位置都没有在谷歌地图、苹果地图等其他商业地图应用上出现。另外，不仅在战区的军事基地得以显现，在美国本土的军事基地也可在“热力地图”上找到。斯特拉瓦公司说，他们制作的“热力地图”囊括了超过3000亿个独立数据点，10亿个用户锻炼数据，这些数据都是用户在锻炼时通过全球卫星定位系统上传的。

斯特拉瓦软件在设计之初就将数据分享作为它的核心功能之一，其相关产品被美国国防部采购并作为减肥器材下发部队。但没想到的是，软件的轨迹信息竟然泄露了军事机密。时任美国国防部长马蒂斯对此大为震怒，还考虑直接禁止美国士兵在军队中使用手机等电子设备，以免造成新的泄密事件。

分析人士认为，军方泄密一事，也与其移动设备管理条例存在漏洞有关。美国海军陆战队规定，个人可穿戴设备不能带有“电信通讯、无线网、拍照、摄像、麦克风和录音”等功能，并且“即便关闭上述功能，也不能使用具备这些功能的设备”。但是根据条例，可以使用具有蓝牙以及全球定位系统功能的设备，而斯特拉瓦公司正是通过全球定位系统获得数据的。

