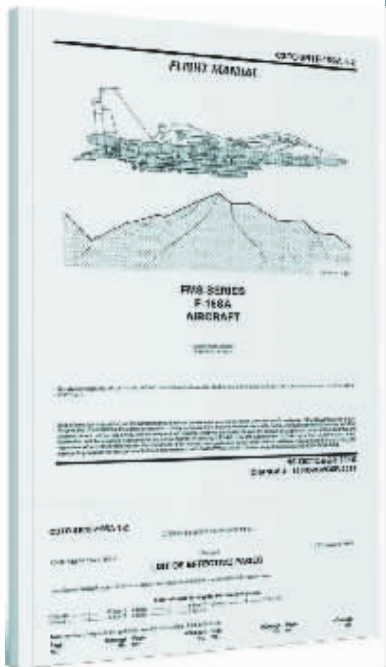


# 超250GB的美国军事装备数据在网上被公开发布 包括F-15、F-35战斗机以及多种无人机机密性能手册 美军被曝“史上最大规模泄密事件”

近日，“美军史上最大规模泄密事件”引起关注。一个名为“战斗轰炸机”的俄文账号在社交媒体上宣布：“一家美国公司主动提供了超过250GB的美国军事装备数据”，并公布了其中部分文件，包括F-15、F-35战斗机以及多种无人机在内的大批美军装备的机密性能手册。美国《技术时报》称，类似的泄密事件近年来多次发生，可能会暴露美军装备的真正弱点。



“杰达姆”精确制导炸弹。



美军战机性能手册。



美军F15战斗机。

## 超250GB机密数据 泄露的文件资料非常详细

据悉，泄露的文件包括F-35隐形战斗机的使用手册、F-15C/D和更先进的F-15SA战斗机的技术手册、“弹簧刀”无人机以及“杰达姆”精确制导炸弹等相关文件。

由于这些文件透露的信息非常详细，涉及的武器种类又多，因此它也被不少媒体形容为“美军史上最大规模泄密事件”。有人甚至开玩笑说，有了这些详细资料，“现在可以在车库里打造战机了”。其中最引人注目的是包含数百篇文档、详细介绍美国在2016年提供给沙特阿拉伯的美制F-15SA战斗机的文件，这份文件包括了配套的飞行手册、保养维修手册以及武器系统操作手册等。第一部分包括400多页，详细介绍了这种重型战斗机的各种系统。第二部分约40页，主要涉及F-15SA的基本飞行操作。第三部分有110页，包括F-15SA的应急操作，第四部分则是说明飞行员的职责，第五部分有50页，提到了战斗机的飞行速度、飞行高度等操作限制。

此外，泄露的文件还包括美国空军现役的AIM-120C先进中程空空导弹和AIM-9X红外格斗弹的详细资料。据悉，此前曾有类似美军文件遭泄露。2023年12月，某暗网数据交易平台有人宣称售卖一份“受到出口管制”的美国军用飞机手册。卖家称该文件总大小为5GB，标价为2万美元。

## 泄密事件频发 包括涉乌克兰“绝密”情报

实际上，这已不是美军第一次发生泄密事件。据美国《纽约时报》去年4月7日报道，推特等多家社交媒体出现一批疑似美军秘密文件，涉及俄乌冲突中乌克兰方面兵力及武器配置、战场地图、俄乌双方伤亡情况等情报，甚至包括标有“绝密”的情报。

据多家媒体报道，美国政府一度努力“删帖”，但网上仍有文件流传。《纽约时报》报道称，五角大楼对此感到震惊。有分析人士表示，此次文件的泄露规模可能已经超过100份。美国官员继而补充道，再加上文件本身的敏感性，此次泄密可能会造成巨大破坏。一位高级情报官员直言，此次泄密是共享情报的“五眼联盟的噩梦”。

随后，去年4月13日，美国联邦调查局（FBI）在马萨诸塞州逮捕了五角大楼军事文件泄密案嫌犯杰克·特谢拉。据美国有



美军F35战斗机。

线电视新闻网、福克斯新闻网等媒体披露的嫌疑人的背景信息显示，特谢拉时年21岁，于2019年进入马萨诸塞州空军国民警卫队，平时的工作包括保障军队“全球性大型通信网络”的正常运行。

美媒称，一封美国国防部内部邮件显示，特谢拉持有联邦政府授予的最高级别绝密信息安全许可。2022年7月，特谢拉被提拔为一等飞行员，他此前还曾荣获空军成就奖章。

据悉，遭泄露的文件除涉及俄乌冲突等多方面情报外，还包含韩国政府高层疑似遭美国情报部门监听的内容。美国官员曾表示，其中一些文件是真实的，这些文件暴露了美国对韩国、以色列和乌克兰等重要盟友的监听程度。

## 暴露信息安全漏洞 文件提供者或是美国军事公司

分析人士指出，“这些文件很详细，格式与先前在网上泄露的其他美国军事情报类似。严格来说，这些并不是蓝图或设计文件。”这也意味着，哪怕这些文件泄露出来，所能提供的技术价值也并不算大，至少想要依靠这些信息研制美军战斗机，显然是不可能的。

例如，F-15SA战斗机相关的技术文件虽然非常详细，但主要是用于维护人员和飞行员的简化介绍，而不是完整的设计文档，因此实际的技术参考价值不大。但美国《技术时报》也提到，“战斗轰炸机”账号宣称拥有250GB的美军装备文件，对外发布的只是其中很少部分，因此，可能没有公开的文件中还包括其他更多的美军机密信息，从中可以发现美军战斗机装备的弱点。

据介绍，这些资料中很多地方都标注有“禁止外传”或“机密信息”等标志，部分资料还经过大面积的涂黑处理，显示它们应该是属于美军的机密文件。

有媒体援引网络安全专家的分析称，提供这些文件的可能是美国军事公司，或是冒充它们的“第三方”，其中包含了从机密到公开的各种信息。文件显示，与F-35隐形战斗机相关的文件部分经过编辑，“这或许显示它们已经解密”。因为美国军方通常会在认为安全的情况下解密某些文件，这些文件虽然被公开，但关键信息常被打码或涂抹掉以保护敏感数据。这种公开的做法并不少见。例如，即使是涉及当前仍在服役的U-2侦察机这类敏感项目的文档，也可能在某种程度上被解密并

对外公开，前提是经过严格的审查和处理，确保不泄露关键的战略信息。

国际社会认为，更为关键的是，无论美军装备的这些机密数据是主动披露还是被动泄密，它们出现如此大规模的外泄情况，足以证明美军的信息安全出现了严重漏洞。

## 越来越多军事情报 能在游戏玩家论坛中轻易获得

报道称，这些外泄文件在全球军迷界引起轰动，有人甚至开玩笑说，有了这些详细资料，“现在可以在车库里打造战机了”。据介绍，这些资料在全球军迷范围内被广泛传播。

不过，有网络安全人员警告称，不要下载这些可疑的文件，因为黑客可能会利用热门事件传播病毒，下载恶意文件可能会导致用户设备被勒索软件或木马病毒感染。对于这次美军装备数据的大规模外泄事件，目前五角大楼保持沉默，而各方对于这些数据的真实性和严重程度说法不一。

据了解，除了美军的信息安全漏洞引发质疑，一些游戏玩家在某些游戏论坛上主动披露机密军事装备情报的现象也越来越多。去年1月就有玩家在著名军事模拟游戏《战争雷霆》论坛中发布了美国F-15和F-16战斗机的涉密信息。英国《卫报》报道称，各国玩家在《战争雷霆》可以同时操作战机、地面载具和战舰等进行“对决”。

因为玩家对武器装备性能的讨论，导致这款游戏自2020年以来至少发生了10起泄密事件。例如2021年7月，一名玩家因为游戏中英国“挑战者-2”主战坦克的装甲防护问题与他人发生争论。据《英国国防期刊》报道，为了证明自己很专业，这名玩家在游戏中讨论群组中上传了英国陆军装备保障出版物上的文档截图，以证明游戏开发人员建模错误。他还详细解释了设计人员错误地放置了哪些组件，并将其所在位置与出版物上的介绍进行比较，指出如何修改数据以使游戏更加逼真。英国国防部随后确认，这名玩家分享的材料真实且是机密的信息。

2021年10月，有多个玩家就游戏中法国“勒克莱尔”主战坦克的性能及参数发生过一次争执，一名法国陆军坦克组成员随即发布了该型主战坦克的部分机密手册信息。

据《法治日报》报道