

“太空出差三人组”要回家了

将采用快速返回技术着陆

为期 6 个月的太空之旅即将结束,“太空出差三人组”回家前搞起大扫除,并用影像记录下这段时光。

视频中叶光富拍下的王亚平跳着绳,逐渐“起飞”,王亚平实力演绎回家前高兴到起飞,逗乐了不少网友。

“太空出差”接近尾声,神十三乘组都在准备些什么?

整理“房间”

还记得 3 名航天员刚进空间站时,曾经十分费力地“拆快递”吗?

他们从货运飞船搬下来很多生活用品和实验设备,布置好了天上的“小家”。

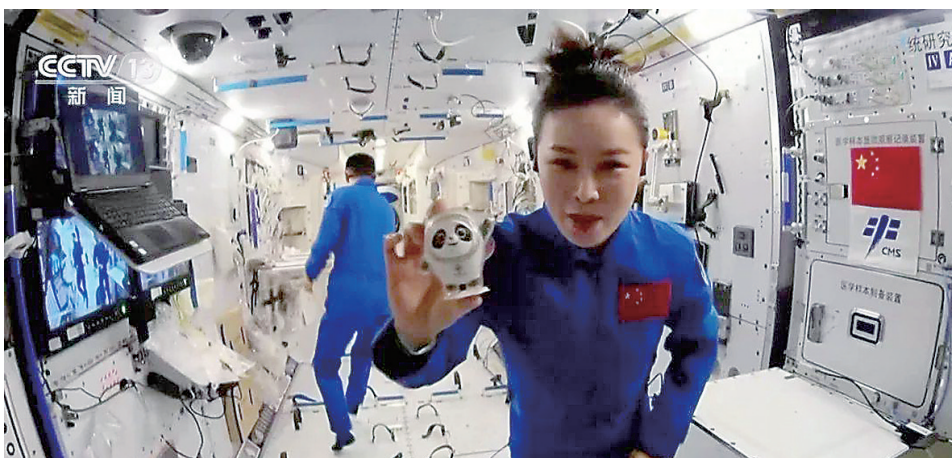
而在回家之前,他们 need 要把舱内环境尽量恢复原样。比如健身器材、实验用品、维修备件等都需要重新打包好,放回指定的位置。

另外,他们要对剩余的物资进行盘点和归类,以便未来神舟十四号飞船乘组“无缝切换”在轨生活。

收拾“行李”

回家之前,他们不仅要收拾“行李”,还要“搬运数据”。

“出差”半年,3 名航天员在天宫空间站内开展了多项实验,



这些实验数据、记录等都要从空间站核心舱“搬运”到神舟十三号飞船返回舱,早准备带回地面。

另外,空间站里近半年积累的垃圾也需要“随手带走”。航天员返回之前,需要对空间站来一次彻底“大扫除”,做好收集和整理工作。

锻炼身体

长期处于太空失重环境中,人的身体会产生肌肉萎缩、骨质流失等现象。为了缓解这些状况可能造成的危害,航天员每天都要在空间站里锻炼身体。

现在,他们需要进行强化锻炼,为返回地面提前做好适应性调整。航天员的每个动作都有科学的设计方案,航天员地面中心的失重生理效应防护团队会根据 3 位航天员的实时身体状况,提供“锻炼处方”。

目前,3 名航天员的身体状况和心理状态都优于预期,满足返回地球的条件需求。

“关灯锁门”

尽管技术成熟可靠,飞船返回舱重返地球的旅途仍然充满挑战。

航天员必须熟悉整个返回

过程中的必要操作和应急预案,还要认真检查飞船返回舱,确保各项系统正常工作。离开空间站之前,还需要做好临行状态设置,把电、水、气、通信等方面都设置到位。

临走之前,航天员要关闭空间站内各个舱门,再从核心舱返回神舟十三号飞船,安稳坐好后,系上安全带,并检查航天服的气密性及设备的完好度。一切准备就绪之后,他们就将踏上归途。

快速返回

从开始点火制动,到最终

在地面上安全着陆,神舟十二号用时 49 分钟。从飞船脱离空间站,到最后在地球上着陆,神舟十二号用了 28.3 小时。由此可见,想要加快返回的速度,关键是要缩短点火制动前的时间,尽快找到飞船着陆的时间窗口。

相比之下,俄罗斯航天局的联盟号载人飞船在脱离国际空间站后,只需绕地球转两圈左右,就能进行点火制动,整个过程只持续了 3 小时多一点。在点火制动后,联盟号用时大约 56 分钟降落在着陆场。从飞船脱离空间站,到最后在地球上着陆,联盟号只用了大约 4 小时,这就是快速返回技术。

经过前期的一系列技术验证,神舟十三号也将采用快速返回技术进行着陆。可以预见,在中国空间站将要飞过东风着陆场上空之前的几圈,神舟十三号将会脱离空间站,独自完成着陆前的最后几圈绕飞。

神舟十三号将会绕地球转 5 圈,耗时大约 7.5 小时。随后,飞船点火制动,脱离轨道,再入大气层,最终在东风着陆场降落,耗时也是大约 49 分钟左右。从脱离空间站,到最后在地球上着陆,神舟十三号预计将耗时 8.3 小时,这要比神舟十二号的返回时间缩短了 20 小时。

据澎湃新闻

多地现“变脸”诈骗案: 一段段逼真的视频竟是伪造的……

一段视频、一段语音未必是真人拍摄或者录制。在你不知道的手机 App 后台、支付界面、门禁闸机,或许有人正在盗刷你的脸……去年以来,多地发生“变脸”诈骗案。

记者调查发现,随着深度合成技术迅猛发展,落地场景激增,一些不法分子趁机牟利。音频、视频等合成技术滥用,对人脸、声纹、指纹等个人敏感信息保护形成挑战。

合成视频只需 2 元至 10 元,竟能注册手机卡、支付账户

近日,陈先生来到浙江省温州市公安局瓯海分局仙岩派出所报案,称自己被“好友”骗了近 5 万元。经过警方核实,骗子用了 AI 换脸技术,利用陈先生好友阿诚社交平台上发布的视频,截取了面部视频画面并进行了“换脸”,从而对陈先生进行了诈骗。

在警方抓捕现场,几名犯罪嫌疑人正用电脑将一张张静态照片制作为人脸动态视频。模拟制作出来的动态人物不仅能做点头、摇头等动作,还可完成眨眼、张嘴、皱眉等丰富表情,效果极为逼真。

在嫌疑人的电脑里,警方发现了十几个 G 的公民人脸数据,人脸照片和身份证照片分门别类存放在一个个文件夹里。“身

份证正反面照片、手持身份证照片、自拍照等,被称为一套。”民警介绍,成套照片被称为“料”,出售照片的人被称为“料商”,这些“料”在网上已转手多次,而“料”的主人却毫不知情。

犯罪嫌疑人马某交代,由于制作简单,一个视频价格仅为 2 元至 10 元,“客户”往往是成百上千购买,牟利空间巨大。

近年来,类似案件在浙江、江苏、河南等多地发生。浙江衢州中级人民法院的一份刑事裁定书披露:张某、余某等人运用技术手段骗过支付宝人脸识别认证,并使用公民个人信息注册支付宝账户,非法获利数万元。

网上“叫卖”合成软件教程

据合肥市公安局包河分局网安大队民警王祥瑞介绍,前述案件中 8 名犯罪嫌疑人多为社会闲散人员,有的连高中都没有读完。他们按照网购教程下载软件,花几个月便“自学成才”。

记者在网上一联系到一位售卖相关教程的卖家。卖家介绍,全套软件及教程售价有 400 元、800 元两档,800 元的为高阶版本,“过人脸成功率超高”。记者在演示视频中看到,照片上传至软件后,标注出五官位置,调整脚参数,一张脸便动了起来。“五官参数随教程送上,照抄即可。”据介绍,这些伪造视频不仅通过率高,人工审核都难辨真假。



“目前公众对照片等静态信息易被篡改已有所警惕,但对视频、声音等动态信息内容仍持有较高信任度。”清华大学人工智能研究院基础理论研究中心主任朱军说,深度合成技术飞速演进,让“眼见不再为实”,破解身份核验的难度会越来越低,耗时将越来越短。

专家担心,尽管针对深度合成技术的识别技术不断迭代、检测手段持续增强,但依然没能跑赢“伪造”技术升级的速度。浙江大学网络空间安全学院院长任奎说,随着合成技术应用门槛的进一步降低,合成内容已模糊真实与伪造的边界。

北京智源人工智能研究院安全创新中心执行主任田天认为,新型伪造方法层出不穷,网络传播环境日趋复杂,检测算法

存在漏洞缺陷等,反深伪检测难度越来越大。

法律规定相对滞后,也给不法分子留下可乘之机。中伦律师事务所合伙人陈际红说,目前法律规定,禁止利用信息技术手段伪造等方式侵害他人的肖像权,但技术如何使用算合理使用,哪些情形下应禁止使用等,没有具体规定;收集或收购个人声纹、照片,使用人脸、指纹、DNA、虹膜等个人生物信息等行为,在哪些范围内构成犯罪、将面临怎样的惩罚,需要司法裁判进一步给出明确指引。

别再让公众为“脸面”担忧

保护人脸、指纹、声纹等敏

感信息,不再担忧信息“裸奔”损害个人隐私、财产、名誉等,是公众的共同期待。

我国首个国家层面的科技伦理治理指导性文件《关于加强科技伦理治理的意见》近日印发,凸显技术伦理治理的重要性紧迫性。在今年的最高法工作报告中,包括人脸安全在内的个人信息安全等多次被提及。

陈际红表示,打击“变脸”诈骗犯罪,应从技术的合法使用边界、技术的安全评估程序、滥用技术的法律规制等方面予以规范,提高技术滥用的违法成本。

中国工程院院士、信息技术专家邬贺铨提出,针对深度合成技术滥用现象,应以技术规制技术,利用技术创新、技术对抗等方式,提升和迭代检测技术的能力。

技术规制之外,针对技术滥用暴露的风险治理应当体系化、完善化。“要构建数据集质量规范,根据应用场景对相关技术进行风险分级分类管理,明确设计开发单位、运维单位、数据提供方的责任。”国家工业信息安全发展研究中心副总工程师邱惠君说。

专家提醒,针对花样翻新的“变脸”诈骗,公众要提高防范意识,不轻易提供人脸、指纹等个人生物信息给他人,不过度公开或分享动图、视频等;网络转账前要通过电话、视频等多种沟通渠道核验对方身份。一旦发现风险,及时报警求助。

据新华社