“人脸识别破解术”成黑产业 护“脸”亟须查缺补漏

人脸识别作为一种易用性强的生物特征验证技术，目前在政务、安防、金融、生活消费等行业都有着广泛应用。不过，新华每日电讯记者调查发现，人脸识别技术存在明显的安全漏洞，对社会和财产安全存在重大隐患，亟须进行系统性的安全排查和堵漏。

▲人脸识别技术存在明显的安全漏洞（中新社资料图）

1 一起发票案牵出非法人脸识别案

记者从上海检察机关获悉，在近期上海市虹口区人民检察院公诉的一起特大虚开增值税普通发票案中，被告人通过破解人脸识别技术等方式，注册“皮包公司”用于虚开增值税普通发票。据悉，多名被告人为他人开具增值税普通发票价税合计超过5亿元。

案件中，犯罪嫌疑人首先通过相关政务平台完成注册“皮包公司”，过程中通过平台上注册人的人脸识别是注册成功的关键环节。

为达到目的，犯罪嫌疑人中专门从事人脸识别破解的成员表示，其一般先从他处以30元每个的价格购买他人的高清头像和身份证信息，之后利用“活照片”App对高清头像进行处理，让照片“动起来”，形成包括点头、摇头、眨眼、张嘴等动作视频。

“获取视频后，我们利用特殊处理的手机‘劫持’摄像头，在人脸认证环节时，手机摄像头不会启动，系统获取的是之前做好的视频。系统会认为是本人在摄像头前，最后通过认证。”犯罪嫌疑人说。

同时，该团伙还破解了某广泛用于管理电子营业执照App的人脸识别系统。犯罪嫌疑人下载电子营业执照后，会在App里添加办事员的身份信息。虚开发票团伙就以此通过办事员身份使用电子营业执照。

据犯罪嫌疑人交代，其破解的App类别非常广泛，涉及政务、安防、金融、支付、生活消费等用户量巨大的App。每单的破解价格从25元到300元不等。

2 15分钟破解19款手机的人脸识别系统

“15分钟破解19款手机的人脸识别系统。”据记者了解，依托清华大学人工智能研究院成立的团队瑞莱智慧近期披露了新的研究成果：研究人员根据一张照片，通过研究算法，制作一副特殊“眼镜”，就可以刷脸解锁他人手机或App身份认证。

研究人员向记者透露，其团队通过对抗样本攻击，戴上自制眼镜后，15分钟内破解了19款智能手机的人脸识别解锁系统。同样被破解的还包括十余款金融和政务服务类App。

研究人员表示，结合身份证号等个人信息，甚至可冒充机主完成线上银行开户。

3 “过脸识别技术”群里黑客成“贵客”

记者发现，网上存在大量提供破解人脸识别技术服务的群组，群名大多采用“过脸”“识别技术”等关键词逃避监管。群人数从100人到300人不等。

在一个名为“过脸识别技术”的群里，有人采取付费的方式邀约群内可以破解支付软件人脸识别审核的人士。黑客，成了人们追捧的“贵客”。

此外，有的群则是对破解技术进行资料、资源分享交流。一个名为“VX三色过脸”的群自称“破解人脸识别技术的扛把子”“适合想入行的新手和小白”，群内多达300人。

名为“蓝叶子”的用户给记者发来一段App人脸识别安防的破解视频，并表示可以出售一台特制的手机。通过导入自行制作的人脸动作视频后，所有在该手机上安装的应用软件，都可以自动跳过人脸认证的环节。每台手机的价格为1650元。

他还告诉记者，虚假的人脸动作视频可以使用“你我当年”“活照片”“轻松换脸”等App完成。

“我们了解到，有的公司上班考勤要进行人脸识别打卡，有员工委托黑客入侵打卡App，利用人脸识别漏洞来完成打卡，每月仅需付给黑客30元。”一位网络安防公司相关负责人向记者透露。

在上述虚开发票案中，犯罪嫌疑人除了利用破解技术从事虚开发票外，还会利用注册新账号从事骗取各类App补贴优惠等违法犯罪。

瑞莱智慧高级产品经理张旭东告诉记者，当前破解人脸识别技术主要是针对活体检测的假体攻击，但针对AI算法自身的对抗样本攻击威胁也逐步凸显。

“由于业界的人脸识别技术主要是固定几个方法，相似度很高。如果黑客提供一个专用于破解人脸识别的开源软件，并在互联网上广泛流传，犯罪分子利用漏洞进行各类App实施违法犯罪将犹如‘入无人之境’。”张旭东说。

在新华三集团安全专家曹亮看来，无论是对抗样本攻击还是针对活体检测的假体攻击，最终目的都是为了骗过“机器眼”。

“当前人脸识别算法大都是人脸上‘三点’‘五点’‘七点’的识别，通过对眼睛、鼻子、嘴、耳朵以及头部活动来实现认证。黑客完全可以通过了解机器内部验证机制和评判规则，再想办法绕过安全防护。”他说。

4 抓紧查缺补漏 还每一张脸“安全”

专家认为，应尽快排摸国内政务、安防、金融、支付、生活消费等领域的核心App应用存在的相关漏洞，并及时打上补丁，以防发生危害社会安全和财产安全的重大事件。

开展软硬件“对攻升级”。张旭东表示，当务之急应对涉及政务、安防、金融、消费等行业的人脸识别技术漏洞进行完善和升级。

“尤其是对于涉众、涉密、涉及公共利益的相关平台和技术服务提供商，需优先完成技术加固，对手机模拟器要做好防范和拒绝。同时，鼓励和引导更多手机厂商在手机升级时支持3D人脸识别技术。”张旭东说。

“手机厂商在写入手机系统时可内置安全模块，防止黑客绕过手机摄像头启动环节、对摄像头实现劫持，从源头上实现安全守护。”曹亮说。

制定落实人脸识别安全标准。曹亮表示，对核心领域使用人脸识别技术的产品，监管部门可制定并严格实施相关标准，保证产品符合安全技术要求。

“可依据人脸识别在公共或商业应用中对安全的差异化需求，制定分级别、多层次的国家安全标准及行业安全标准。”他说。

加强司法打击，保护每一张“脸”。“违法者可能涉嫌破坏计算机信息系统罪，执法和司法机关应当加强打击力度，形成威慑力。”北京格丰律师事务所合伙人郭玉涛律师说。他建议，当前各大政务、金融、电商等平台都搜集了大量的人脸数据，既存在重复建设的问题，更存在安全隐患和风险。国家和省级层面可建立统一的商用安防大数据中心，以此达到防止人脸信息的滥用、外泄等问题。

“可要求人脸识别算法供应商的模型须在大数据中心内进行训练，实现数据、模型物理上不出专网。算法供应商可租用大数据中心的数据和计算力进行算法模型的升级和更新。”他说。

（据新华每日电讯）

茶陵县工农兵政府：毛泽东亲手缔造的第一个“红色政权”

□ 株洲晚报融媒体记者 戴凛 通讯员 陈启浪

▲游客进入茶陵县工农兵政府旧址参观 记者 戴凛 摄

百年潮 株洲红 系列报道之⑬

市委宣传部 株洲日报社 市委党史研究室 联合推出

在茶陵县工农兵政府旧址的展厅里，有一幅连跨多个墙面的彩画。画面正中的两侧，群众吹号打鼓、欢天喜地。而在画面正中央，一名士兵正在为写着“茶陵县工农兵政府”的牌匾挂起红绸。

美国记者斯诺在他的《西行漫记》一书中，记载了毛泽东这样一段回忆：“在湖南的东南部的茶陵建立了全国第一个红色政权”。这里说的第一个红色政权，就是茶陵县工农兵政府。

九十多年后，记者站在工农兵政府成立的画像前，感觉那振奋人心的呼声仍在隐约传来。

工农兵政府成立 掀起“红色风暴”

茶陵县党史专家彭东明，指着如今恢复旧貌的县衙大厅说道：当年，接到毛泽东的指示后，宛希先向部队里的党员、团营干部和士兵委员会，向茶陵县委、县人民委员会等方面作了传达。随后，农会、工会、士兵委员会分别选出一名代表，组织工农兵代表会议，产生县工农兵政府主席。

工人代表谭震林，农民代表李炳荣，士兵代表陈士榘，相互谦让，宛希先便说：“‘工农兵政府’‘工’字带头。谭震林同志，你是工人代表，你就担任政府主席吧！”就这样，工农兵政府的主要领导人确定了。

11月28日，在旧县衙内，茶陵县工农兵政府成立。工农兵政府设立了民政、财经、青工、妇女等工作部门，任命农运、工运骨干及知识分子担任部门领导职务和政府秘书。

人民政府爱人民。茶陵县工农兵政府成立后，又派工作队分赴全县各地发动群众，建立区、乡工农兵政权，建立工农武装，惩治土豪劣绅，在茶陵大地掀起了“红色风暴”，也昭示着中国革命进入了劳动人民行使权力的新纪元。

为什么是茶陵？

毛泽东亲手缔造的第一个“红色政权”为什么会在茶陵？在来到茶陵县工农兵政府旧址前，记者也有这样的疑问。

茶陵历史悠久，古称茶乡，因地居“茶山之阴”和炎帝神农氏“崩葬于茶乡之尾”而得名。打开地形图不难发现，茶陵地处湘、赣、粤交通要津，可快捷东进江西，南下广东，犹如“三路襟喉”。同时，这里山地、丘陵占全县总面积的百分之九十，也为后来的游击战争提供了天然的战地优势。

毛泽东同志的《井冈山斗争》一书中还提到，“湖南方面，茶陵、酃县两县均有70%土地在地主手中。”面对苦难与压迫，茶陵人民没有屈服，而是奋起抗争。

1926年7月，中共茶陵支部成立，相继发展多名共产党员，并建立了4个党小组。1926年8月，小车乡又有了第一个乡农民协会，开展了农民运动试点，并取得胜利。1926年10月18日，茶陵还召开了县农民代表大会，并正式成立县农民协会。到了1927年，短短一年时间内，茶陵绝大部分地区都取得进步，成为红色苏区和游击区。茶陵社会各界的革命运动都蓬勃发展起来了。

秋收起义后，毛泽东开始“经营茶陵”

国共合作的第二次北伐战争，因国民党反动派的背叛惨遭失败。1927年5月长沙“马日事变”后，茶陵的反动派残酷镇压农民革命运动，制造了“鸡公石惨案”，共产党员和工农革命群众共108人惨遭杀害。茶陵县农会领导成员之一范桂嵘，被当地土豪劣绅杀害，年仅18岁。

“面对白色恐怖，茶陵共产党人愈发奋勇，顽强抗争。”据茶陵文史专家介绍，针对茶陵、攸县、酃县、安仁党组织均遭破坏的情况，1927年7月23日，中共湖南省委决定组建茶陵特委，辖茶陵、攸县、酃县、安仁四县，并由毛泽东在韶山革命活动时亲自培养的农民运动骨干之一——谭天民同志，任特委书记。

茶陵特委成立后，谭天民与茶陵共产党人取得联系，在省城求学的茶陵籍共产党人陈韶、谭趋新也悄然回县，与潜伏于民间的县内共产党人谭思聪等人在鸡公石会合。游击队成功组建，陈韶任队长，谭趋新任党代表，与敌人公开展开斗争。

▲展馆内的壁画，展示了茶陵县工农兵政府成立时的场景 记者 戴凛 摄

1927年9月，秋收起义如燎原星火迅速燃遍湘赣边界。而茶陵地处湘赣要地，自然条件良好，战略地位重要，又有较好的党的群众工作基础，因此毛泽东也首次有了“经营茶陵”的打算。

插曲：新政权“新瓶”却装了“旧酒”

1927年11月中旬，工农革命军进驻江西井冈山茨坪，在井冈山上安下家后，便将攻打茶陵作为向外发展的首选目标。

据茶陵党史记载，1927年11月16日清晨，按照毛泽东的安排部署，团长陈皓、政治部主任宛希先率领团部、一营和特务连500余人，从大垅出发向茶陵县城进发。18日清晨，部队攻克县城，占领了县署衙门。

然而，推翻了旧政权，新政权又该如何建立？

旧址解说员介绍，由于思想准备不足和实践经验缺乏，陈皓没有去做群众工作，也不顾毛泽东的叮嘱，而是绕开宛希先，成立了一个新政权，名为“县人民委员会”，并派谭梓生当了县长。但是谭梓生本人对于红色政权里的县长如何当心中无数，只好比照旧政府，升堂审案，纳税完粮。陈皓则因为旧军队的积习深重，不去打土豪、筹款子，没有经费就找商会要，或者搞摊派。结果人民群众对这个“新瓶装旧酒”式的政府极为不满。

听说“县人民委员会”如此作为，毛泽东提出尖锐批评。他号召彻底打碎旧政权，建立真正让人民当家做主的新政权，又立即给宛希先写信说到：“由部队派人当县长是不对的，不能按国民党那一套办。要成立工农兵政府。要保护商店，保护邮局，保护学校，保护医院。”

相关链接

旧址前身是州衙 始建于宋代中叶

茶陵县工农兵政府旧址坐落于茶陵县城关镇三角坪，占地面积18000多平方米。旧址的前身是南宋至清代的州衙，始建于宋代中叶，整个建筑属于徽派风格，中轴线上建有头门、仪门、牌坊、大堂、二堂、三堂、廨舍、内宅，自南向北沿中轴线依次排列形成七进院落。

2004年，按照修旧如旧的原则，茶陵县在原址上重新修复了工农兵政府旧址，2007年开馆。2017年底，茶陵县对旧址进行改造和重新布展。

▲扫码观看“百年潮 株洲红”系列报道之13视频