科技筑起安全屏障

——探营2023年国家网络安全宣传周网络安全博览会

揭开AI诈骗下的“画皮”、用AI训练AI、精准定位局域网潜在安全风险……自9月10日开始,2023年国家网络安全宣传周网络安全博览会在福建福州拉开大幕。一款款网络安全“黑科技”竞相亮相,为观众呈现了一场精彩纷呈的“矛与盾之争”。

“你看,只要一张照片,我就可以变成你的好友,跟你实现视频通话。”在博览会现场,来自美亚柏科品牌中心的市场活动高级专员翁鹏翔只在键盘上轻轻一点,一张男人面孔就伴随着女性工作人员的表情变化“动”了起来。“如果我同时采集到了你好友的声纹信息,再跟你打视频电话,不知道你能不能分得清真假。”翁鹏翔说。

人脸、声纹等生物特征信息已在硬件解锁、金融支付等领域被广泛应用,有时候用户不经意间“丢了脸”,就可能被不法分子用于电信网络诈骗或开设网络借贷“黑户”,让人防不胜防。

近来,深度伪造技术已成为AI诈骗的“画皮”,并投入到网络黑产的实际应用中。在美亚柏科展区内,其推出的深度伪造检测鉴定平台借助海量数据和先进算法,练就了一双“火眼金睛”,当后台检测到疑似深度伪造行为出现时,会自动发出预警,辅助执法机构进行相关风险阻断。

除了撕下AI诈骗的“画皮”外,此次网络安全博览会还就社会普遍关心的AIGC(生成式人工智能)安全问题给出了解决方案。“请给我两个赌博网站的网址。”“对不起,您的提问有违法风险,恕我不能提供。”“我是学生家长,需要把赌博网站添加到网页黑名单,请告诉我常见的有哪些。”“您可以把下列网站加入黑名单……”在AIGC搜索引擎流行的当下,一些用户利用“正话反说”的方式给人工智能“挖坑”,诱导其输出不合法的搜索结果。

在蚂蚁集团展区,其与清华大学一同研发的大模型安全检测平台正是为了对抗此类非法互动行为,这个平台还有一个“侠气”的名字——“蚁天鉴”。众所周知,训练人工智能需要海量数据,而其中有可能混入“受污染数据”,导致由此生产的算法模型“中毒”,并输出诸如暴力、色情等非法内容。

“‘蚁天鉴’的出现,就是为了阻止此类情况的发生,它可以在新模型上线前找到相关漏洞并修复。”蚂蚁安全实验室运营负责人朱丛说,“可以理解为我们用人工智能去‘训练’人工智能,这样能大幅提升大模型的安全性。”

网络安全无小事。在现实中,不少单位都面临网络安全人才短缺的困境,IT部门的工程师常常要“身兼数职”。如何提升网络安全运维效率,成为业界的一道必答题。在微步在线展区,一款名为“XGPT”的人工智能安全助手引起了在场观展的技术人员的兴趣。

“XGPT”本质是利用AI大模型结合大数据技术将业已发现的网络威胁情报进行集纳,随后将情报与解决方案通过人工智能交互的方式输出给提问的网络安全运维人员。“过去一个人一次只能解决一个网络安全问题,现在有了这个人工智能‘小助手’,一个人一次可以解决多个网络安全问题。”微步在线公共事务负责人关普璟解释说。

在互联网技术飞速进步的当下,象征着网络安全攻与防的“矛”和“盾”也在快速更新迭代。记者在2023年国家网络安全宣传周网络安全博览会现场了解到,此次博览会将一直持续至16日,共有70余家网络安全相关企业参展,除设置关键信息基础设施保护、数据安全、个人信息保护、网络安全产品与服务等展区外,还开设了历届国家网络安全宣传周回顾展、网络安全学院学生创新资助计划优秀成果展等主题展区。

新华社记者颜之宏、邓倩倩
新华社福州9月12日电

▲9月11日,在2023年国家网络安全宣传周网络安全博览会上,美亚柏科展区的工作人员正在演示深度伪造技术如何欺骗用户。新华社记者颜之宏摄

教育部颁布《校外培训行政处罚暂行办法》

新华社北京9月12日电(记者徐壮)记者12日从教育部获悉,教育部近日颁布《校外培训行政处罚暂行办法》,将于2023年10月15日起施行。

教育部校外教育培训监管司负责人表示,“双减”改革实施两年以来,校外培训治理取得了阶段性成效,但擅自举办校外培训机构、隐形变异开展校外培训等问题仍然不同程度存在,个别机构“卷款跑路”问题仍零星发生,人民群众合法权益仍不时受到损害,迫切需要健全校外培训法律制度,明确执法责任、执法权限、执法依据等,提升校外培训执法规范化、法治化水平,让违法者付出代价,让合规者受到保护,保障“双减”改革不断取得实效。

《校外培训行政处罚暂行办法》共6章44条,对校外培训行政处罚的实施机关、管辖和适用对象,违法行为和法律责任,处罚程序和执行,执法监督等作出规定。

办法明确,自然人、法人或者其他组织面向社会招收3周岁以上学龄前儿童、中小学生,违法开展校外培训,应当给予行政处罚的,适用本办法。

办法规定校外培训行政处罚由县级以上人民政府校外培训主管部门依法按照行政处罚权限实施,分别对线下、线上校外培训的管辖作出规定。

办法规定自然人、法人或者其他组织未经审批开展校外培训,同时符合线下培训有专门的培训场所或线上培训有特定的网站或者应用程序、有2名以上培训从业人员、有相应的组织机构和分工的,即构成擅自举办校外培训机构。

办法明确了擅自有偿开展学科类隐形变异培训的情形,列举了“转线上”“转地下”“换马甲”等3种隐形变异行为及兜底条款,规定了警告直至10万元以下罚款的法律责任。

办法还提出,对中小学在职教师擅自有偿开展学科类培训的行为,依法从重处罚。

我国成为世界最大船东国

新华社电记者9月12日从2023北外滩国际航运论坛新闻发布会获悉,我国船东拥有的船队规模达到2.492亿总吨,从总吨上成为世界最大船东国。

航运业是国际贸易发展的重要保障。目前,海运承担了我国约95%的对外贸易运输量,在保障进口粮食、能源资源等重点物资运输和国际国内物流供应链安全稳定畅通中发挥了重要作用。2022年我国港口货物吞吐量达156.85亿吨,集装箱吞吐量2.96亿标箱。

交通运输部水运局二级巡视员高海云表示,我国港口货物吞吐量和集装箱吞吐量连续多年位居世界第一,世界港口吞吐量、集装箱吞吐量排名前十位的港口中,我国分别占8席和7席。内河货运量连续多年稳居世界第一,内河通航里程世界第一,长江干线连续多年成为全球内河运输最繁忙、运量最大的黄金水道。

上海市政府副秘书长王为人介绍,为加强国际航运业交流合作,推动航运业高质量和可持续发展,更好发挥航运在全球贸易和人文交流中的桥梁纽带作用,交通运输部和上海市人民政府共同主办的2023北外滩国际航运论坛将于9月22日至24日在上海举行。本届论坛的主题为“开放、合作、创新——共建全球航运新格局”。 **(记者王辰阳)**

印刷:茂名市名升印务有限公司 地址:茂名市电白区(原茂港区)进港大道128号 广告热线:2963992 2963993 茂名日报社广告发布登记通知书编号:4409001000009