奋进新征程 建功新时代·北京劳动者之歌

为网络强国建设保驾护航

——记北京奇虎科技有限公司“大数据+AI”安全协同创新团队

□本报记者 孙艳

数字化时代，人工智能成为新一轮科技革命和产业变革的核心驱动力，网络信息技术迭代升级加速，对网络安全保障提出了更高要求。作为人工智能应用最核心的载体，人工智能模型一旦被恶意攻击，将会影响数以千万计的开发者以及用户。“人工智能的安全问题渗透到各个领域、方方面面，已经成为当前急需解决的一个问题。对我们研究来说是一个新挑战、新机遇。”北京奇虎科技有限公司“大数据+AI”安全协同创新团队AI安全负责人邹权臣说，“这个时候，我们必须往前冲。”

探索与实践 赋能网络安全

勇于攻坚克难、做行业“领头羊”，是“大数据+AI”安全协同创新团队的一个传统。

团队在人工智能系统安全方面分成算法安全、漏洞挖掘两个小组，他们紧密配合、相互协作，对人工智能安全展开了深入研究。最新研制的人工智能系统安全检测平台，是国内首个支持系统化安全检测、支持提示注入风险检测的平台，覆盖图像识别、人脸识别、目标检测、生成式AI等多场景，可以通过系统监控和检测发现厂商AI漏洞，协助各厂商对漏洞进行修复，输出安全评分及分析报告，并提供相应的安全加固方案，保障了广大AI开发者和用户的安全以及行业的健康发展。经过孜孜不倦的研究努力，团队形成国际和国内多项领先成果，发现了谷歌、META、INTEL、华为和百度等厂商AI框架漏洞超过200余个，在谷歌AI框架Tensorflow漏洞发现方面质量和数量位列全球第一。

除了在AI安全领域遥遥领先，团队在数据安全治理方面的探索与实践也取得了累累硕果。团队面向数字经济时代的数据安全治理这一复杂问题展开研究，探索在促进数据流通共享与开发利用的场景下如何保障数据的全生命周期安全。在此过程中，团队创新提出了基于数据安全能力成熟度模型（DSMM）的数据安全治理体系。同时，聚焦大数据平台数据安全一体化管理、数据流通共享安全、大数据安全监测与监管3个方面的关键技术研究，创新突破了敏感数据自动识别、大数据安全监测与监管审计以及大数据滥用防范等关键技术，开发了DSMM测评支撑平台、数据分类分级系统和大数据安全监管审计平台等产品，全面提供数据安全咨询、测评、培训服务，面向政府、金融、电力和通信等行业领域，解决了数据在采集汇聚、流通共享与开发利用过程中的安全保护与监管审计问题，破解了企业或组织数据安全能力提升的共性难题。

利用“大数据+AI”更好地赋能网络安全，是团队的下一个技术攻坚方向。团队带头人钟力介绍，通过构建各行业领域互联互通的安全大数据基础库，打通安全运营数据，将会大幅提高我国应对APT攻击的能力，有效保障国家网络空间安全。

搭建平台 引领产业发展

搭建好平台，才能有效协同产学研等多方力量、打通并凝聚资源、做好技术创新和成果转化。2021年，国家发改委以服务国家重大战略任务和重点工程实施为目标，开始推进国家工程研究中心和国家工程实验室的优化整合工作。钟力率领团队克服种种困难，使实验室顺利通过验收并进入到了国家发改委新的国家工程研究中心序列。“纳入国家工程研究中心新序列仅仅是个开始，有了这个国家战略科技平台，我们可以以更广阔的视野开展科技创新，从产业的角度打通科研、技术突破和成果转化各环节。”

团队承担建设的另一个国家级平台，是科技部授牌的“安全大脑国家新一代人工智能开放创新平台”，这也是人工智能安全领域唯一的国家级平台。该技术平台实现了部分云端安全大脑的能力输出、安全大数据的赋能以及AI安全模型与训练数据集的开放共享，不仅为产业链和创新链上下游单位提供开放服务，还与高校和科研院所对接成果转化，促进人工智能安全生态体系建设。

为了给政府机构和企事业单位培养专业的数据安全人才，团队依托这两个国家级平台在国内率先推出了数据安全官和数据安全工程师的认证培训，从管理和技术两个层面系统提高组织人员对数据安全的认知能力。截至目前，团队已培训一千余名来自各行业领域的数据安全相关岗位人员，为政府、企事业单位的数据安全合规运营提供了人才保障。“仅2021年10月第一期培训，就有政府机构、电信运营商、金融等各个领域行业的90余名学员参加。”首期培训的场景，钟力还历历在目，“到现在我们的培训一直在有序开展，今年还成立了人才能力中心，开始全面培训数字安全人才。”

“责任在肩，必须创新向前。”钟力说，作为奋斗在国家数字安全最前线的数字安全人员，面对网络安全层出不穷的新挑战，他将继续与团队成员一起开拓创新、磨砺技术，全面筑牢国家数字安全防线，为网络强国建设保驾护航。

丰台公安分局右安门派出所社区民警傅天雷：

聚焦百姓身边事 提升群众安全感

□本报记者 余翠平

傅天雷（左）

有人说，琐碎是湮灭热情的研磨器。但从警以来，傅天雷却始终乐此不疲地“主动揽麻烦”，风险隐患、家长里短，都是他认真研究的课题。结合北京市公安局部署开展的“转作风、办实事、树形象”主题实践活动，他不断聚焦群众身边的“小案件、小纠纷、小事情”，提升人民群众的获得感、幸福感、安全感。

2017年，从部队转业后的傅天雷成为了丰台公安分局右安门派出所的社区民警，兼任丰台区右安门街道玉林里社区党委副书记。他积极推动社区党委向街道提出社区硬件设施申请，经过多方努力，5台高空坠物摄像机、18台治安摄像机、2105米架设线路建成使用，社区治安环境一下子有了突飞猛进的改变。

社区硬件设施建成后，傅天雷又开始着手“软件”建设。他带领社区干部通过上门走访、张贴宣传等方式，建立了社区居民“反诈微信群”，户入群率达92%。只要居民在群中反映问题，无论大小，他都会及时接收、积极协调、尽快答复。在傅天雷的组织协调下，社区干部、物业负责人、垃圾分类和负责接诉即办的工作人员积极入群，居民反映的很多诉求都快速得到解决。时间长了，“反诈微信群”就成了“有求必应群”，在化解矛盾纠纷、防范社区安全方面立下了汗马功劳。

傅天雷发现要想让社区整体水平再上一个台阶，就得让更多人发挥主人翁作用，参与社区共治。2020年，他依托社区党委倡导发起了“微光行动”志愿服务，汇聚社会各界爱心人士，传递党和政府的温暖。在他的动员下，佑安医院、北京考古遗址博物馆、首都医科大学国际学院等多家企事业单位都加入进来。截至目前，已有200多名志愿者参与到“微光行动”中，有14家单位成为了志愿服务的成员单位，团队还建立了“安全宣传、便民志愿、红色纽带、文化传承、环境美化、关爱帮扶、健康守护”7个小分队，队伍中还有来自20多个国家的50多名国际留学生。“微光团队”成立以来，走访慰问残疾人、鳏寡孤独家庭80多户，先后组织开展了春节系列慰问、迎新春联欢会、志愿巡河护河等活动。如今，“微光团队”已成为右安门地区一道亮丽的风景线，并成为北京市志愿组织中的一员。

此外，在傅天雷的积极推动下，社区党委开始筹划“最美玉林里居民”评选活动，充分调动广大居民的主人翁意识，让美好的道德情操在社区蔚然成风。

凭借出色表现，傅天雷曾获“全国特级优秀人民警察”“全国最美基层民警”等荣誉。