武汉网络安全

WUHAN CYBER SECURITY

武汉市网络安全协会通讯
2025年第2期　总第6期

内部资料　电子样本

◎ **政策速递**

全国人民代表大会常务委员会关于修改《中华人民共和国网络安全法》的决定 /04P

武汉市生成式人工智能发展安全公约 /25P

◎ **党建引领**

武汉市网络安全协会党支部参加互联网行业党委“铭记历史，砥砺奋进”主题党日活动 /27P

◎ **国家网络安全宣传周专栏**

2025 年武汉市网络安全宣传周全城启动 /31P

◎ **黄鹤杯专栏**

聚智网安　筑梦黄鹤“黄鹤杯”大赛在汉收官 /39P

◎ **协会动态**

武汉市网络安全协会人工智能专业委员会第一次全体会议召开 /71P

第三届软件创新发展大会网络安全论坛在汉启幕 共探 AI 时代网安产业新路径 /73P

国家网安基地产业联盟在汉全面启动，助力打造网络安全产业高地 /80P

筑牢工业数据安全屏障 | 2025 中国 5G+ 工业互联网大会工业数据安全防护平行论坛在武汉成功举办 /98P

武汉市网络安全协会简介

INTRODUCTION TO WUHAN CYBER SECURITY ASSOCIATION

（中文简称：武网安协，英文简称：WHCSA）成立于 2018 年，是在中共武汉市委网络安全和信息化委员会办公室（武汉市互联网信息办公室）主管下，在民政部门依法登记成立的社会团体法人单位，也是唯一代表武汉网络安全产业的全市性、专业性、非营利性组织。

我会是民政部门认定的 AAAA 级社会组织；是中国网络社会组织联合会、中国网络空间安全协会和中国网络安全产业联盟正式成员单位，中国网络空间安全协会智能网联安全专业委员会发起单位，国家网络安全人才与创新基地产业联盟运营单位，全国基础软件安全可信行业产教融合共同体常务副理事长单位，武汉市互联网行业联合会副会长单位；具备全国团体标准信息平台团体标准发布资格，入选湖北省第一批优质团体标准制定主体重点培育名单；主办有全国首个“移动应用安全公益检测平台”，并与武汉东湖科技保险发展促进中心共建有“东湖网络安全保险服务中心”；是武汉市职称改革领导小组办公室授权的全市职称评审行业主管单位；成立了华中第一个智能汽车网络安全专业委员会、网络安全保险工作委员会、民办高校工作委员、人工智能专业委员会和医疗卫生与健康分会；拥有全市最大最全的网络安全高级专家智库，长期为各级主管部门提供智力支撑。

我会坚持带领成员单位积极主动对接国家互联网应急中心、全国信息安全标准化技术委员会、国家工业信息安全发展研究中心、工信部人才交流中心、工信部第五研究所等国家级平台资源；并与北京、上海、广东、重庆、四川、昆明等兄弟省市网络安全协会广泛开展交流合作；参与了省市网络安全领域各类的课题研究、政策咨询与制定工作；参与并组织历年省市“国家网络安全宣传周”系列宣传活动；主办承办了各类型专业性论坛、赛事、全市攻防演练等大型活动；协助主管部门遴选两年一度的“武汉市网络安全应急技术支撑单位”和每年的网络安全领域“武汉英才”计划培育支持专项等重要工作。

我会各项工作长期得到各级官方媒体的支持和关注，新华网、人民网、光明网、学习强国、中国新闻网、湖北日报（荆楚网）、长江日报（长江网）相继报道我会工作动态和成果。我会还在国内外重要学术期刊上发表十余篇科研论文，不少被 SCI、EI 收录检索。

我会的宗旨：遵守宪法、法律、法规和国家政策，践行社会主义核心价值观，遵守社会道德风尚；根据武汉市信息化建设发展的需要，贯彻执行国家的有关法律、法规和政策；以服务社会和服务会员为宗旨，发挥政府管理部门与信息系统用户之间的桥梁和纽带作用；协助管理机关规范和加强系统安全保护工作的管理，协助维护我市网络系统的安全和稳定；推动网络安全技术的发展，促进信息网络用户的法制观念和安全意识的提高，保障我市信息化建设的健康发展。

武汉，是全国首个拥有“国家网络安全人才与创新基地”的超大型国家中心城市，它还拥有着全国前三的高等教育资源、九省通衢的交通区位、上下游完整的产业基础、敢为人先的城市品格等诸多特色优势。《武汉市国民经济和社会发展第十四个五年规划和 2035 年远景目标纲要》明确提出，网络安全将成为武汉未来六大新兴产业，得到全市重点发展和布局。

相信未来，在全体武汉网安人的共同努力下，武汉网络安全产业和科技创新必将迎来更加快速、健康、持续的发展，共同为全国网络安全和信息化事业贡献“武汉网络安全”集体力量！

卷首语

岁聿云暮，冬意渐浓，《武汉网络安全》年末刊如期与各位读者见面。站在年度收官的时间节点回望，武汉市网络安全协会人工智能专业委员会（以下简称“专委会”）与业界同仁携手深耕的“AI+安全”沃土，已在江城结出丰硕果实。

这一年，专委会从无到有、由点及面筑牢生态根基：5 月正式成立后，迅速确立武汉人工智能研究院为主任单位、武汉大学人工智能学院、武汉理工大学计算机与人工智能学院、江汉大学人工智能学院等为副主任单位、黄鹤实验室为秘书长单位的核心架构，构建起覆盖 30 余家单位的“政产学研用”协作网络。6 月，我们召开首次全体委员会议明确技术研发、标准建设等五大方向，随即承办第三届软件创新发展大会网络安全论坛，发布《人工智能基础设施产品内生安全能力提升倡议书》，为行业协同立规定向。10 月在国家网安基地牵头举办的人工智能专场供需对接会更成为年度亮点，不仅发布《武汉市生成式人工智能发展安全公约》划定安全红线，更推动《生成式 AI 安全检测技术要求》标准立项，填补了领域规范空白。

AI 安全的发展始终伴随着模型可信、数据合规等挑战。作为专委会主任，我深知标准与协作是破局关键。新的一年，我们将持续推进检测标准落地，深化智能靶场、人才实训等场景创新，让技术攻关与行业共治形成合力。

道阻且长，行则将至。专委会将始终以“安全为基，智能为翼”，在武汉建设人工智能创新先导区的征程中，与各方共筑数字安全屏障！

武汉市网络安全协会人工智能专业委员会主任

武汉人工智能研究院副院长：

目 录

CATALOGUE

政策速递

04 全国人民代表大会常务委员会关于修改《中华人民共和国网络安全法》的决定
——附新修正《网络安全法》全文及历次审议报告法

07 中华人民共和国网络安全法

15 全国人民代表大会宪法和法律委员会关于《全国人民代表大会常务委员会关于修改（中华人民共和国网络安全法）的决定（草案）》修改意见的报告

16 全国人民代表大会宪法和法律委员会关于《中华人民共和国网络安全法（修正草案）》审议结果的报告

17 关于《中华人民共和国网络安全法（修正草案）》的说明

18 国家网络安全事件报告管理办法

20 网络安全事件分级指南

22 国家互联网信息办公室于《网络数据安全风险评估办法（征求意见稿）》公开征求意见的通知

25 武汉市生成式人工智能发展安全公约

党建引领

27 武汉市网络安全协会党支部参加互联网行业党委“铭记历史，砥砺奋进”主题党日活动

28 观阅兵 强信念 护网络 践初心 | 武汉市网络安全协会党支部组织开展九三阅兵观看活动

科普专栏

29 《安安说网安之科普小课堂》No.3 维护未成年人健康网络环境

30 《安安说网安之科普小课堂》No.4 维护未成年人健康网络环境

国家网络安全宣传周专栏

32 武汉市国家网络安全宣传周灯光秀绽放两江四岸

33 武汉网络安全号公交正式启航

34 网安嘉年华全城联动点亮武汉网红地标

37 网络安全宣传点亮相武汉、汉口火车站

黄鹤杯专栏

39 聚智网安 筑梦黄鹤 “黄鹤杯”大赛在汉收官

45 2025 年“黄鹤杯”网络安全人才创新大赛创新成果擂台赛圆满收官 聚焦落地转化赋能产业高质量发展

47 基于知识蒸馏的通用型车载网络入侵检测技术研究

50 面向演进的计算环境可信构建与分析关键技术研究
53 智能网联汽车网络安全检测技术规范研究
56 基于关键表征和无关表征解耦的人脸识别反欺诈方法
58 深度对抗技术在线上金融业务安全防护中的应用研究
60 基于人工智能的网络安全监测运营平台创新实践
62 基于 154N 体系驱动的超算中心纵深防御解决方案
65 “透视”加密黑盒：基于 AI 自学习的加密流量威胁检测实践
67 政务网络安全运营—数智护航江汉政务：AI+ 一体化网络安全运营体系建设

协会动态

70 武网安协发布推动武汉市“综合安全防护平台”（城市盾、行业盾）建设的倡议书
71 武汉市网络安全协会人工智能专业委员会第一次全体会议召开
73 第三届软件创新发展大会网络安全论坛在汉启幕 共探 AI 时代网安产业新路径
76 数链聚能 产业共融
——2025 年数据安全供需对接会成功举办
78 武汉市网络安全协会第二届第三次会员大会成功召开
80 国家网安基地产业联盟在汉全面启动，助力打造网络安全产业高地
81 武汉市网络安全协会医疗卫生与健康分会首次工作会议召开 开启医疗网安协同新征程
82 武汉市网络安全应用场景供需对接会金融保险专场顺利召开 全国首个风险量化标准发布
84 武汉市网络安全应用场景供需对接会智能网联汽车专场顺利召开 车联网安全标准落地助力产业合规发展
88 武汉市网络安全应用场景供需对接会人工智能专场顺利召开 公约与标准双轮驱动助力 AI 产业合规发展
91 网安基地招聘双选会火热启幕 助力国家网安基地人才高地建设
93 2025 年首场武汉市工业领域数据安全能力提升专题宣贯培训汉口片区活动成功举办
96 极智守护 驭见未来 第一届小米汽车守护活动圆满结束
98 筑牢工业数据安全屏障 | 2025 中国 5G+ 工业互联网大会工业数据安全防护平行论坛在武汉成功举办

102 武汉市网络安全协会服务指南

全国人民代表大会常务委员会关于修改《中华人民共和国网络安全法》的决定

——附新修正《网络安全法》全文及历次审议报告法

中华人民共和国主席令

第六十一号

《全国人民代表大会常务委员会关于修改＜中华人民共和国网络安全法＞的决定》已由中华人民共和国第十四届全国人民代表大会常务委员会第十八次会议于2025年10月28日通过，现予公布，自2026年1月1日起施行。

中华人民共和国主席　习近平

2025年10月28日

全国人民代表大会常务委员会关于修改《中华人民共和国网络安全法》的决定

第十四届全国人民代表大会常务委员会第十八次会议决定对《中华人民共和国网络安全法》作如下修改：

一、增加一条，作为第三条：“网络安全工作坚持中国共产党的领导，贯彻总体国家安全观，统筹发展和安全，推进网络强国建设。”

二、将第十八条改为第十九条，删去第二款。

三、增加一条，作为第二十条：“国家支持人工智能基础理论研究和算法等关键技术研发，推进训练数据资源、算力等基础设施建设，完善人工智能伦理规范，加强风险监测评估和安全监管，促进人工智能应用和健康发展。

“国家支持创新网络安全管理方式，运用人工智能等新技术，提升网络安全保护水平。”

四、将第四十条改为第四十二条，增加一款，作为第二款：“网络运营者处理个人信息，应当遵守本法和《中华人民共和国民法典》、《中华人民共和国个人信息保护法》等法律、行政法规的

规定。”

五、将第五十九条改为第六十一条，修改为：“网络运营者不履行本法第二十三条、第二十七条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告，可以处一万元以上五万元以下罚款；拒不改正或者导致危害网络安全等后果的，处五万元以上五十万元以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

“关键信息基础设施的运营者不履行本法第三十五条、第三十六条、第三十八条、第四十条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告，可以处五万元以上十万元以下罚款；拒不改正或者导致危害网络安全等后果的，处十万元以上一百万元以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

“有前两款行为，造成大量数据泄露、关键信息基础设施丧失局部功能等严重危害网络安全后果的，由有关主管部门处五十万元以上二百万元以下罚款，对直接负责的主管人员和其他直接责任人员处五万元以上二十万元以下罚款；造成关键信息基础设施丧失主要功能等特别严重危害网络安全后果的，处二百万元以上一千万元以下罚款，对直接负责的主管人员和其他直接责任人员处二十万元以上一百万元以下罚款。”

六、将第六十条改为第六十二条，增加一款，作为第二款：“有前款第一项、第二项行为，造成本法第六十一条第三款规定的后果的，依照该款规定处罚。”

七、增加一条，作为第六十三条：“违反本法第二十五条规定，销售或者提供未经安全认证、安全检测或者安全认证不合格、安全检测不符合要求的网络关键设备和网络安全专用产品的，由有关主管部门责令停止销售或者提供，给予警告，没收违法所得；没有违法所得或者违法所得不足十万元的，并处二万元以上十万元以下罚款；违法所得十万元以上的，并处违法所得一倍以上五倍以下罚款；情节严重的，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照。法律、行政法规另有规定的，依照其规定。”

八、将第六十一条改为第六十四条，其中的“并可以由有关主管部门责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照”修改为“并可以责令暂停相关业务、停业整顿、关闭网站或者应用程序、吊销相关业务许可证或者吊销营业执照”。

九、将第六十二条改为第六十五条，修改为：“违反本法第二十八条规定，开展网络安全认证、检测、风险评估等活动，或者向社会发布系统漏洞、计算机病毒、网络攻击、网络侵入等网络安全信息的，由有关主管部门责令改正，给予警告，可以处一万元以上十万元以下罚款；拒不改正或者情节严重的，处十万元以上一百万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站或者应用程序、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

“有前款行为，造成本法第六十一条第三款规定的后果的，依照该款规定处罚。”

十、将第六十五条改为第六十七条，修改为：

“关键信息基础设施的运营者违反本法第三十七条规定，使用未经安全审查或者安全审查未通过的网络产品或者服务的，由有关主管部门责令限期改正、停止使用、消除对国家安全的影响，处采购金额一倍以上十倍以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。”

十一、将第六十八条、第六十九条第一项合并，作为第六十九条，修改为：“网络运营者违反本法第四十九条规定，对法律、行政法规禁止发布或者传输的信息未停止传输、采取消除等处置措施、保存有关记录、向有关主管部门报告，或者违反本法第五十二条规定，不按照有关部门的要求对法律、行政法规禁止发布或者传输的信息停止传输、采取消除等处置措施、保存有关记录的，由有关主管部门责令改正，给予警告、予以通报，可以处五万元以上五十万元以下罚款；拒不改正或者情节严重的，处五十万元以上二百万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站或者应用程序、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处五万元以上二十万元以下罚款。

“有前款行为，造成特别严重影响、特别严重后果的，由有关主管部门处二百万元以上一千万元以下罚款，责令暂停相关业务、停业整顿、关闭网站或者应用程序、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处二十万元以上一百万元以下罚款。

“电子信息发送服务提供者、应用软件下载服务提供者，不履行本法第五十条第二款规定的安全管理义务的，依照前两款规定处罚。”

十二、将第六十四条、第六十六条、第七十条合并，作为第七十一条，修改为：“有下列行为之一的，依照有关法律、行政法规的规定处理、处罚：

（一）发布或者传输本法第十三条第二款和其他法律、行政法规禁止发布或者传输的信息的；

（二）违反本法第二十四条第三款、第四十三条至第四十五条规定，侵害个人信息权益的；

（三）违反本法第三十九条规定，关键信息基础设施的运营者在境外存储个人信息和重要数据，或者向境外提供个人信息和重要数据的。

“违反本法第四十六条规定，窃取或者以其他非法方式获取、非法出售或者非法向他人提供个人信息，尚不构成犯罪的，由公安机关依照有关法律、行政法规的规定处罚。”

十三、增加一条，作为第七十三条：“违反本法规定，但具有《中华人民共和国行政处罚法》规定的从轻、减轻或者不予处罚情形的，依照其规定从轻、减轻或者不予处罚。”

十四、将第七十五条改为第七十七条，修改为：“境外的机构、组织、个人从事危害中华人民共和国网络安全的活动的，依法追究法律责任；造成严重后果的，国务院公安部门和有关部门并可以决定对该机构、组织、个人采取冻结财产或者其他必要的制裁措施。”

本决定自 2026 年 1 月 1 日起施行。

《中华人民共和国网络安全法》根据本决定作相应修改并对条文顺序作相应调整，重新公布。

中华人民共和国网络安全法

（2016 年 11 月 7 日第十二届全国人民代表大会常务委员会第二十四次会议通过 根据 2025 年 10 月 28 日第十四届全国人民代表大会常务委员会第十八次会议《关于修改 < 中华人民共和国网络安全法 > 的决定》修正）

第一章　总则

第一条　为了保障网络安全，维护网络空间主权和国家安全、社会公共利益，保护公民、法人和其他组织的合法权益，促进经济社会信息化健康发展，制定本法。

第二条　在中华人民共和国境内建设、运营、维护和使用网络，以及网络安全的监督管理，适用本法。

第三条　网络安全工作坚持中国共产党的领导，贯彻总体国家安全观，统筹发展和安全，推进网络强国建设。

第四条　国家坚持网络安全与信息化发展并重，遵循积极利用、科学发展、依法管理、确保安全的方针，推进网络基础设施建设和互联互通，鼓励网络技术创新和应用，支持培养网络安全人才，建立健全网络安全保障体系，提高网络安全保护能力。

第五条　国家制定并不断完善网络安全战略，明确保障网络安全的基本要求和主要目标，提出重点领域的网络安全政策、工作任务和措施。

第六条　国家采取措施，监测、防御、处置来源于中华人民共和国境内外的网络安全风险和威胁，保护关键信息基础设施免受攻击、侵入、干扰和破坏，依法惩治网络违法犯罪活动，维护网络空间安全和秩序。

第七条　国家倡导诚实守信、健康文明的网络行为，推动传播社会主义核心价值观，采取措施提高全社会的网络安全意识和水平，形成全社会共同参与促进网络安全的良好环境。

第八条　国家积极开展网络空间治理、网络技术研发和标准制定、打击网络违法犯罪等方面的国际交流与合作，推动构建和平、安全、开放、合作的网络空间，建立多边、民主、透明的网络治理体系。

第九条　国家网信部门负责统筹协调网络安全工作和相关监督管理工作。国务院电信主管部门、公安部门和其他有关机关依照本法和有关法律、行政法规的规定，在各自职责范围内负责网络安全保护和监督管理工作。

县级以上地方人民政府有关部门的网络安全保护和监督管理职责，按照国家有关规定确定。

第十条　网络运营者开展经营和服务活动，必须遵守法律、行政法规，尊重社会公德，遵守商业道德，诚实信用，履行网络安全保护义务，接受政府和社会的监督，承担社会责任。

第十一条　建设、运营网络或者通过网络提供服务，应当依照法律、行政法规的规定和国家标准的强制性要求，采取技术措施和其他必要措施，保障网络安全、稳定运行，有效应对网络安全事件，防范网络违法犯罪活动，维护网络数据的完整性、保密性和可用性。

第十二条　网络相关行业组织按照章程，加强行业自律，制定网络安全行为规范，指导会员加强网络安全保护，提高网络安全保护水平，促进行业健康发展。

第十三条　国家保护公民、法人和其他组织依法使用网络的权利，促进网络接入普及，提升网络服务水平，为社会提供安全、便利的网络服务，保障网络信息依法有序自由流动。

任何个人和组织使用网络应当遵守宪法法律，

遵守公共秩序，尊重社会公德，不得危害网络安全，不得利用网络从事危害国家安全、荣誉和利益，煽动颠覆国家政权、推翻社会主义制度，煽动分裂国家、破坏国家统一，宣扬恐怖主义、极端主义，宣扬民族仇恨、民族歧视，传播暴力、淫秽色情信息，编造、传播虚假信息扰乱经济秩序和社会秩序，以及侵害他人名誉、隐私、知识产权和其他合法权益等活动。

第十四条 国家支持研究开发有利于未成年人健康成长的网络产品和服务，依法惩治利用网络从事危害未成年人身心健康的活动，为未成年人提供安全、健康的网络环境。

第十五条 任何个人和组织有权对危害网络安全的行为向网信、电信、公安等部门举报。收到举报的部门应当及时依法作出处理；不属于本部门职责的，应当及时移送有权处理的部门。

有关部门应当对举报人的相关信息予以保密，保护举报人的合法权益。

第二章 网络安全支持与促进

第十六条 国家建立和完善网络安全标准体系。国务院标准化行政主管部门和国务院其他有关部门根据各自的职责，组织制定并适时修订有关网络安全管理以及网络产品、服务和运行安全的国家标准、行业标准。

国家支持企业、研究机构、高等学校、网络相关行业组织参与网络安全国家标准、行业标准的制定。

第十七条 国务院和省、自治区、直辖市人民政府应当统筹规划，加大投入，扶持重点网络安全技术产业和项目，支持网络安全技术的研究开发和应用，推广安全可信的网络产品和服务，保护网络技术知识产权，支持企业、研究机构和高等学校等参与国家网络安全技术创新项目。

第十八条 国家推进网络安全社会化服务体系建设，鼓励有关企业、机构开展网络安全认证、检测和风险评估等安全服务。

第十九条 国家鼓励开发网络数据安全保护和利用技术，促进公共数据资源开放，推动技术创新和经济社会发展。

第二十条 国家支持人工智能基础理论研究和算法等关键技术研发，推进训练数据资源、算力等基础设施建设，完善人工智能伦理规范，加强风险监测评估和安全监管，促进人工智能应用和健康发展。

国家支持创新网络安全管理方式，运用人工智能等新技术，提升网络安全保护水平。

第二十一条 各级人民政府及其有关部门应当组织开展经常性的网络安全宣传教育，并指导、督促有关单位做好网络安全宣传教育工作。

大众传播媒介应当有针对性地面向社会进行网络安全宣传教育。

第二十二条 国家支持企业和高等学校、职业学校等教育培训机构开展网络安全相关教育与培训，采取多种方式培养网络安全人才，促进网络安全人才交流。

第三章 网络运行安全

第一节 一般规定

第二十三条 国家实行网络安全等级保护制度。网络运营者应当按照网络安全等级保护制度的要求，履行下列安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改：

（一）制定内部安全管理制度和操作规程，确定网络安全负责人，落实网络安全保护责任；

（二）采取防范计算机病毒和网络攻击、网络侵入等危害网络安全行为的技术措施；

（三）采取监测、记录网络运行状态、网络安全事件的技术措施，并按照规定留存相关的网络日志不少于六个月；

（四）采取数据分类、重要数据备份和加密等措施；

（五）法律、行政法规规定的其他义务。

第二十四条 网络产品、服务应当符合相关国家标准的强制性要求。网络产品、服务的提供者不得设置恶意程序；发现其网络产品、服务存在安全缺陷、漏洞等风险时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。

网络产品、服务的提供者应当为其产品、服务持续提供安全维护；在规定或者当事人约定的期限内，不得终止提供安全维护。

网络产品、服务具有收集用户信息功能的，其提供者应当向用户明示并取得同意；涉及用户个人信息的，还应当遵守本法和有关法律、行政法规关于个人信息保护的规定。

第二十五条 网络关键设备和网络安全专用产品应当按照相关国家标准的强制性要求，由具备资格的机构安全认证合格或者安全检测符合要求后，方可销售或者提供。国家网信部门会同国务院有关部门制定、公布网络关键设备和网络安全专用产品目录，并推动安全认证和安全检测结果互认，避免重复认证、检测。

第二十六条 网络运营者为用户办理网络接入、域名注册服务，办理固定电话、移动电话等入网手续，或者为用户提供信息发布、即时通讯等服务，在与用户签订协议或者确认提供服务时，应当要求用户提供真实身份信息。用户不提供真实身份信息的，网络运营者不得为其提供相关服务。

国家实施网络可信身份战略，支持研究开发安全、方便的电子身份认证技术，推动不同电子身份认证之间的互认。

第二十七条 网络运营者应当制定网络安全事件应急预案，及时处置系统漏洞、计算机病毒、网络攻击、网络侵入等安全风险；在发生危害网络安全的事件时，立即启动应急预案，采取相应的补救措施，并按照规定向有关主管部门报告。

第二十八条 开展网络安全认证、检测、风险评估等活动，向社会发布系统漏洞、计算机病毒、网络攻击、网络侵入等网络安全信息，应当遵守国家有关规定。

第二十九条 任何个人和组织不得从事非法侵入他人网络、干扰他人网络正常功能、窃取网络数据等危害网络安全的活动；不得提供专门用于从事侵入网络、干扰网络正常功能及防护措施、窃取网络数据等危害网络安全活动的程序、工具；明知他人从事危害网络安全的活动的，不得为其提供技术支持、广告推广、支付结算等帮助。

第三十条 网络运营者应当为公安机关、国家安全机关依法维护国家安全和侦查犯罪的活动提供技术支持和协助。

第三十一条 国家支持网络运营者之间在网络安全信息收集、分析、通报和应急处置等方面进行合作，提高网络运营者的安全保障能力。

有关行业组织建立健全本行业的网络安全保护规范和协作机制，加强对网络安全风险的分析评估，定期向会员进行风险警示，支持、协助会员应对网络安全风险。

第三十二条 网信部门和有关部门在履行网络安全保护职责中获取的信息，只能用于维护网络安全的需要，不得用于其他用途。

第二节 关键信息基础设施的运行安全

第三十三条 国家对公共通信和信息服务、能源、交通、水利、金融、公共服务、电子政务等重要行业和领域，以及其他一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益的关键信息基础设施，在网络安全等级保护制度的基础上，实行重点保护。关键信息基础设施的具体范围和安全保护办法由国务院制定。

国家鼓励关键信息基础设施以外的网络运营者自愿参与关键信息基础设施保护体系。

第三十四条 按照国务院规定的职责分工，负责关键信息基础设施安全保护工作的部门分别编制并组织实施本行业、本领域的关键信息基础设施安全规划，指导和监督关键信息基础设施运行安全保

护工作。

第三十五条 建设关键信息基础设施应当确保其具有支持业务稳定、持续运行的性能，并保证安全技术措施同步规划、同步建设、同步使用。

第三十六条 除本法第二十三条的规定外，关键信息基础设施的运营者还应当履行下列安全保护义务：

（一）设置专门安全管理机构和安全管理负责人，并对该负责人和关键岗位的人员进行安全背景审查；

（二）定期对从业人员进行网络安全教育、技术培训和技能考核；

（三）对重要系统和数据库进行容灾备份；

（四）制定网络安全事件应急预案，并定期进行演练；

（五）法律、行政法规规定的其他义务。

第三十七条 关键信息基础设施的运营者采购网络产品和服务，可能影响国家安全的，应当通过国家网信部门会同国务院有关部门组织的国家安全审查。

第三十八条 关键信息基础设施的运营者采购网络产品和服务，应当按照规定与提供者签订安全保密协议，明确安全和保密义务与责任。

第三十九条 关键信息基础设施的运营者在中华人民共和国境内运营中收集和产生的个人信息和重要数据应当在境内存储。因业务需要，确需向境外提供的，应当按照国家网信部门会同国务院有关部门制定的办法进行安全评估；法律、行政法规另有规定的，依照其规定。

第四十条 关键信息基础设施的运营者应当自行或者委托网络安全服务机构对其网络的安全性和可能存在的风险每年至少进行一次检测评估，并将检测评估情况和改进措施报送相关负责关键信息基础设施安全保护工作的部门。

第四十一条 国家网信部门应当统筹协调有关部门对关键信息基础设施的安全保护采取下列措施：

（一）对关键信息基础设施的安全风险进行抽查检测，提出改进措施，必要时可以委托网络安全服务机构对网络存在的安全风险进行检测评估；

（二）定期组织关键信息基础设施的运营者进行网络安全应急演练，提高应对网络安全事件的水平和协同配合能力；

（三）促进有关部门、关键信息基础设施的运营者以及有关研究机构、网络安全服务机构等之间的网络安全信息共享；

（四）对网络安全事件的应急处置与网络功能的恢复等，提供技术支持和协助。

第四章 网络信息安全

第四十二条 网络运营者应当对其收集的用户信息严格保密，并建立健全用户信息保护制度。

网络运营者处理个人信息，应当遵守本法和《中华人民共和国民法典》、《中华人民共和国个人信息保护法》等法律、行政法规的规定。

第四十三条 网络运营者收集、使用个人信息，应当遵循合法、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。

网络运营者不得收集与其提供的服务无关的个人信息，不得违反法律、行政法规的规定和双方的约定收集、使用个人信息，并应当依照法律、行政法规的规定和与用户的约定，处理其保存的个人信息。

第四十四条 网络运营者不得泄露、篡改、毁损其收集的个人信息；未经被收集者同意，不得向他人提供个人信息。但是，经过处理无法识别特定个人且不能复原的除外。

网络运营者应当采取技术措施和其他必要措施，确保其收集的个人信息安全，防止信息泄露、毁损、丢失。在发生或者可能发生个人信息泄露、毁损、丢失的情况时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。

第四十五条 个人发现网络运营者违反法律、

行政法规的规定或者双方的约定收集、使用其个人信息的，有权要求网络运营者删除其个人信息；发现网络运营者收集、存储的其个人信息有错误的，有权要求网络运营者予以更正。网络运营者应当采取措施予以删除或者更正。

第四十六条 任何个人和组织不得窃取或者以其他非法方式获取个人信息，不得非法出售或者非法向他人提供个人信息。

第四十七条 依法负有网络安全监督管理职责的部门及其工作人员，必须对在履行职责中知悉的个人信息、隐私和商业秘密严格保密，不得泄露、出售或者非法向他人提供。

第四十八条 任何个人和组织应当对其使用网络的行为负责，不得设立用于实施诈骗，传授犯罪方法，制作或者销售违禁物品、管制物品等违法犯罪活动的网站、通讯群组，不得利用网络发布涉及实施诈骗，制作或者销售违禁物品、管制物品以及其他违法犯罪活动的信息。

第四十九条 网络运营者应当加强对其用户发布的信息的管理，发现法律、行政法规禁止发布或者传输的信息的，应当立即停止传输该信息，采取消除等处置措施，防止信息扩散，保存有关记录，并向有关主管部门报告。

第五十条 任何个人和组织发送的电子信息、提供的应用软件，不得设置恶意程序，不得含有法律、行政法规禁止发布或者传输的信息。

电子信息发送服务提供者和应用软件下载服务提供者，应当履行安全管理义务，知道其用户有前款规定行为的，应当停止提供服务，采取消除等处置措施，保存有关记录，并向有关主管部门报告。

第五十一条 网络运营者应当建立网络信息安全投诉、举报制度，公布投诉、举报方式等信息，及时受理并处理有关网络信息安全的投诉和举报。

网络运营者对网信部门和有关部门依法实施的监督检查，应当予以配合。

第五十二条 国家网信部门和有关部门依法履行网络信息安全监督管理职责，发现法律、行政法规禁止发布或者传输的信息的，应当要求网络运营者停止传输，采取消除等处置措施，保存有关记录；对来源于中华人民共和国境外的上述信息，应当通知有关机构采取技术措施和其他必要措施阻断传播。

第五章 监测预警与应急处置

第五十三条 国家建立网络安全监测预警和信息通报制度。国家网信部门应当统筹协调有关部门加强网络安全信息收集、分析和通报工作，按照规定统一发布网络安全监测预警信息。

第五十四条 负责关键信息基础设施安全保护工作的部门，应当建立健全本行业、本领域的网络安全监测预警和信息通报制度，并按照规定报送网络安全监测预警信息。

第五十五条 国家网信部门协调有关部门建立健全网络安全风险评估和应急工作机制，制定网络安全事件应急预案，并定期组织演练。

负责关键信息基础设施安全保护工作的部门应当制定本行业、本领域的网络安全事件应急预案，并定期组织演练。

网络安全事件应急预案应当按照事件发生后的危害程度、影响范围等因素对网络安全事件进行分级，并规定相应的应急处置措施。

第五十六条 网络安全事件发生的风险增大时，省级以上人民政府有关部门应当按照规定的权限和程序，并根据网络安全风险的特点和可能造成的危害，采取下列措施：

（一）要求有关部门、机构和人员及时收集、报告有关信息，加强对网络安全风险的监测；

（二）组织有关部门、机构和专业人员，对网络安全风险信息进行分析评估，预测事件发生的可能性、影响范围和危害程度；

（三）向社会发布网络安全风险预警，发布避免、减轻危害的措施。

第五十七条 发生网络安全事件，应当立即启

动网络安全事件应急预案，对网络安全事件进行调查和评估，要求网络运营者采取技术措施和其他必要措施，消除安全隐患，防止危害扩大，并及时向社会发布与公众有关的警示信息。

第五十八条 省级以上人民政府有关部门在履行网络安全监督管理职责中，发现网络存在较大安全风险或者发生安全事件的，可以按照规定的权限和程序对该网络的运营者的法定代表人或者主要负责人进行约谈。网络运营者应当按照要求采取措施，进行整改，消除隐患。

第五十九条 因网络安全事件，发生突发事件或者生产安全事故的，应当依照《中华人民共和国突发事件应对法》、《中华人民共和国安全生产法》等有关法律、行政法规的规定处置。

第六十条 因维护国家安全和社会公共秩序，处置重大突发社会安全事件的需要，经国务院决定或者批准，可以在特定区域对网络通信采取限制等临时措施。

第六章 法律责任

第六十一条 网络运营者不履行本法第二十三条、第二十七条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告，可以处一万元以上五万元以下罚款；拒不改正或者导致危害网络安全等后果的，处五万元以上五十万元以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

关键信息基础设施的运营者不履行本法第三十五条、第三十六条、第三十八条、第四十条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告，可以处五万元以上十万元以下罚款；拒不改正或者导致危害网络安全等后果的，处十万元以上一百万元以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

有前两款行为，造成大量数据泄露、关键信息基础设施丧失局部功能等严重危害网络安全后果的，由有关主管部门处五十万元以上二百万元以下罚款，对直接负责的主管人员和其他直接责任人员处五万元以上二十万元以下罚款；造成关键信息基础设施丧失主要功能等特别严重危害网络安全后果的，处二百万元以上一千万元以下罚款，对直接负责的主管人员和其他直接责任人员处二十万元以上一百万元以下罚款。

第六十二条 违反本法第二十四条第一款、第二款和第五十条第一款规定，有下列行为之一的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处五万元以上五十万元以下罚款，对直接负责的主管人员处一万元以上十万元以下罚款：

（一）设置恶意程序的；

（二）对其产品、服务存在的安全缺陷、漏洞等风险未立即采取补救措施，或者未按照规定及时告知用户并向有关主管部门报告的；

（三）擅自终止为其产品、服务提供安全维护的。

有前款第一项、第二项行为，造成本法第六十一条第三款规定的后果的，依照该款规定处罚。

第六十三条 违反本法第二十五条规定，销售或者提供未经安全认证、安全检测或者安全认证不合格、安全检测不符合要求的网络关键设备和网络安全专用产品的，由有关主管部门责令停止销售或者提供，给予警告，没收违法所得；没有违法所得或者违法所得不足十万元的，并处二万元以上十万元以下罚款；违法所得十万元以上的，并处违法所得一倍以上五倍以下罚款；情节严重的，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照。法律、行政法规另有规定的，依照其规定。

第六十四条 网络运营者违反本法第二十六条第一款规定，未要求用户提供真实身份信息，或者对不提供真实身份信息的用户提供相关服务的，由有关主管部门责令改正；拒不改正或者情节严重的，处五万元以上五十万元以下罚款，并可以责令暂停

相关业务、停业整顿、关闭网站或者应用程序、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

第六十五条 违反本法第二十八条规定，开展网络安全认证、检测、风险评估等活动，或者向社会发布系统漏洞、计算机病毒、网络攻击、网络侵入等网络安全信息的，由有关主管部门责令改正，给予警告，可以处一万元以上十万元以下罚款；拒不改正或者情节严重的，处十万元以上一百万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站或者应用程序、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

有前款行为，造成本法第六十一条第三款规定的后果的，依照该款规定处罚。

第六十六条 违反本法第二十九条规定，从事危害网络安全的活动，或者提供专门用于从事危害网络安全活动的程序、工具，或者为他人从事危害网络安全的活动提供技术支持、广告推广、支付结算等帮助，尚不构成犯罪的，由公安机关没收违法所得，处五日以下拘留，可以并处五万元以上五十万元以下罚款；情节较重的，处五日以上十五日以下拘留，可以并处十万元以上一百万元以下罚款。

单位有前款行为的，由公安机关没收违法所得，处十万元以上一百万元以下罚款，并对直接负责的主管人员和其他直接责任人员依照前款规定处罚。

违反本法第二十九条规定，受到治安管理处罚的人员，五年内不得从事网络安全管理和网络运营关键岗位的工作；受到刑事处罚的人员，终身不得从事网络安全管理和网络运营关键岗位的工作。

第六十七条 关键信息基础设施的运营者违反本法第三十七条规定，使用未经安全审查或者安全审查未通过的网络产品或者服务的，由有关主管部门责令限期改正、停止使用、消除对国家安全的影响，处采购金额一倍以上十倍以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款。

第六十八条 违反本法第四十八条规定，设立用于实施违法犯罪活动的网站、通讯群组，或者利用网络发布涉及实施违法犯罪活动的信息，尚不构成犯罪的，由公安机关处五日以下拘留，可以并处一万元以上十万元以下罚款；情节较重的，处五日以上十五日以下拘留，可以并处五万元以上五十万元以下罚款。关闭用于实施违法犯罪活动的网站、通讯群组。

单位有前款行为的，由公安机关处十万元以上五十万元以下罚款，并对直接负责的主管人员和其他直接责任人员依照前款规定处罚。

第六十九条 网络运营者违反本法第四十九条规定，对法律、行政法规禁止发布或者传输的信息未停止传输、采取消除等处置措施、保存有关记录、向有关主管部门报告，或者违反本法第五十二条规定，不按照有关部门的要求对法律、行政法规禁止发布或者传输的信息停止传输、采取消除等处置措施、保存有关记录的，由有关主管部门责令改正，给予警告、予以通报，可以处五万元以上五十万元以下罚款；拒不改正或者情节严重的，处五十万元以上二百万元以下罚款，并可以责令暂停相关业务、停业整顿、关闭网站或者应用程序、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处五万元以上二十万元以下罚款。

有前款行为，造成特别严重影响、特别严重后果的，由有关主管部门处二百万元以上一千万元以下罚款，责令暂停相关业务、停业整顿、关闭网站或者应用程序、吊销相关业务许可证或者吊销营业执照，对直接负责的主管人员和其他直接责任人员处二十万元以上一百万元以下罚款。

电子信息发送服务提供者、应用软件下载服务提供者，不履行本法第五十条第二款规定的安全管

理义务的，依照前两款规定处罚。

第七十条 网络运营者违反本法规定，有下列行为之一的，由有关主管部门责令改正；拒不改正或者情节严重的，处五万元以上五十万元以下罚款，对直接负责的主管人员和其他直接责任人员，处一万元以上十万元以下罚款：

（一）拒绝、阻碍有关部门依法实施的监督检查的；

（二）拒不向公安机关、国家安全机关提供技术支持和协助的。

第七十一条 有下列行为之一的，依照有关法律、行政法规的规定处理、处罚：

（一）发布或者传输本法第十三条第二款和其他法律、行政法规禁止发布或者传输的信息的；

（二）违反本法第二十四条第三款、第四十三条至第四十五条规定，侵害个人信息权益的；

（三）违反本法第三十九条规定，关键信息基础设施的运营者在境外存储个人信息和重要数据，或者向境外提供个人信息和重要数据的。

违反本法第四十六条规定，窃取或者以其他非法方式获取、非法出售或者非法向他人提供个人信息，尚不构成犯罪的，由公安机关依照有关法律、行政法规的规定处罚。

第七十二条 有本法规定的违法行为的，依照有关法律、行政法规的规定记入信用档案，并予以公示。

第七十三条 违反本法规定，但具有《中华人民共和国行政处罚法》规定的从轻、减轻或者不予处罚情形的，依照其规定从轻、减轻或者不予处罚。

第七十四条 国家机关政务网络的运营者不履行本法规定的网络安全保护义务的，由其上级机关或者有关机关责令改正；对直接负责的主管人员和其他直接责任人员依法给予处分。

第七十五条 网信部门和有关部门违反本法第三十二条规定，将在履行网络安全保护职责中获取的信息用于其他用途的，对直接负责的主管人员和其他直接责任人员依法给予处分。

网信部门和有关部门的工作人员玩忽职守、滥用职权、徇私舞弊，尚不构成犯罪的，依法给予处分。

第七十六条 违反本法规定，给他人造成损害的，依法承担民事责任。

违反本法规定，构成违反治安管理行为的，依法给予治安管理处罚；构成犯罪的，依法追究刑事责任。

第七十七条 境外的机构、组织、个人从事危害中华人民共和国网络安全的活动的，依法追究法律责任；造成严重后果的，国务院公安部门和有关部门并可以决定对该机构、组织、个人采取冻结财产或者其他必要的制裁措施。

第七章 附则

第七十八条 本法下列用语的含义：

（一）网络，是指由计算机或者其他信息终端及相关设备组成的按照一定的规则和程序对信息进行收集、存储、传输、交换、处理的系统。

（二）网络安全，是指通过采取必要措施，防范对网络的攻击、侵入、干扰、破坏和非法使用以及意外事故，使网络处于稳定可靠运行的状态，以及保障网络数据的完整性、保密性、可用性的能力。

（三）网络运营者，是指网络的所有者、管理者和网络服务提供者。

（四）网络数据，是指通过网络收集、存储、传输、处理和产生的各种电子数据。

（五）个人信息，是指以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等。

第七十九条 存储、处理涉及国家秘密信息的网络的运行安全保护，除应当遵守本法外，还应当遵守保密法律、行政法规的规定。

第八十条 军事网络的安全保护，由中央军事委员会另行规定。

第八十一条 本法自 2017 年 6 月 1 日起施行。

全国人民代表大会宪法和法律委员会关于《全国人民代表大会常务委员会关于修改〈中华人民共和国网络安全法〉的决定（草案）》修改意见的报告

全国人民代表大会常务委员会：

本次常委会会议于 10 月 25 日下午对关于修改网络安全法的决定草案进行了分组审议。普遍认为，修改决定草案已经比较成熟，建议进一步修改后，提请本次常委会会议表决通过。同时，有些常委会组成人员和列席人员还提出了一些修改意见和建议。宪法和法律委员会于 10 月 25 日晚召开会议，逐条研究了常委会组成人员和列席人员的审议意见，对修改决定草案进行统一审议。中央网络安全和信息化委员会办公室、国家互联网信息办公室有关负责同志列席了会议。宪法和法律委员会认为，修改决定草案是可行的，同时，提出以下修改意见：

一、修改决定草案第二条对人工智能安全和发展作了规定。有的常委委员建议，增加促进人工智能应用、运用人工智能提升网络安全保护水平等内容。宪法和法律委员会经研究，建议采纳这一意见，在这一条中增加促进人工智能应用的内容，并增加一款规定：国家支持创新网络安全管理方式，运用人工智能等新技术，提升网络安全保护水平；同时，删去现行法第十八条第二款。

二、有的常委委员建议，对现行法第七十五条作出修改，扩大本法的域外适用情形。宪法和法律委员会经研究，建议将这一条修改为：“境外的机构、组织、个人从事危害中华人民共和国网络安全的活动的，依法追究法律责任；造成严重后果的，国务院公安部门和有关部门并可以决定对该机构、组织、个人采取冻结财产或者其他必要的制裁措施。”

在审议中，有些常委会组成人员还对加强网络安全工作等提出了一些意见建议。宪法和法律委员会经研究，建议有关方面认真研究常委会组成人员的审议意见，进一步总结网络安全法实施经验，加强新技术新应用风险监测评估，推进构建更加完备的网络安全制度体系，提升网络安全保障能力和水平，切实维护国家网络空间主权、安全、发展利益。

经与有关部门研究，建议将本决定的施行时间确定为 2026 年 1 月 1 日。

此外，根据常委会组成人员的审议意见，还对修改决定草案作了个别文字修改。

修改决定草案修改稿已按上述意见作了修改，宪法和法律委员会建议提请本次常委会会议审议通过。

修改决定草案修改稿和以上报告是否妥当，请审议。

全国人民代表大会宪法和法律委员会

2025 年 10 月 27 日

全国人民代表大会宪法和法律委员会关于《中华人民共和国网络安全法（修正草案）》审议结果的报告

全国人民代表大会常务委员会：

常委会第十七次会议对网络安全法修正草案进行了初次审议。会后，法制工作委员会将修正草案印发各省（区、市）人大、中央有关部门、部分全国人大代表、基层立法联系点和研究机构等征求意见；在中国人大网全文公布修正草案，征求社会公众意见。宪法和法律委员会、法制工作委员会到北京调研，听取地方意见；并就修正草案的有关问题与有关方面交换意见，共同研究。宪法和法律委员会于 9 月 28 日召开会议，根据常委会组成人员的审议意见和各方面的意见，对修正草案进行了逐条审议。中央网络安全和信息化委员会办公室、国家互联网信息办公室有关负责同志列席了会议。10 月 15 日，宪法和法律委员会召开会议，再次进行了审议。宪法和法律委员会认为，为贯彻落实党中央决策部署，适应网络安全新形势新要求，加强法律之间的衔接，完善法律责任制度，对网络安全法作出修改是必要的，修正草案经过审议修改，已经比较成熟。同时，提出以下主要修改意见：

一、有的常委委员建议，贯彻习近平总书记关于网络强国的重要思想，充实网络安全工作指导原则的内容。宪法和法律委员会经研究，建议增加一条规定：网络安全工作坚持中国共产党的领导，贯彻总体国家安全观，统筹发展和安全，推进网络强国建设。

二、有的常委委员和地方、社会公众提出，当前人工智能技术快速发展应用，建议在本法中予以积极回应，支持人工智能技术创新，加强基础设施建设和风险防范，促进人工智能健康发展。宪法和法律委员会经研究，建议增加一条规定：国家支持人工智能基础理论研究和算法等关键技术研发，推进人工智能训练数据资源、算力等基础设施建设，完善人工智能伦理规范，加强安全风险监测评估，创新并加强人工智能安全监管，促进人工智能健康发展。

三、有的常委委员建议，在个人信息保护方面进一步做好与民法典、个人信息保护法等法律的衔接。宪法和法律委员会经研究，建议增加规定：网络运营者处理个人信息，应当遵守本法和《中华人民共和国民法典》、《中华人民共和国个人信息保护法》等法律、行政法规的规定。

四、有的常委委员和部门、社会公众建议，进一步完善相关处罚规定，加大对部分违法行为的处罚力度，并做好有关条款之间的衔接。宪法和法律委员会经研究，建议对修正草案作以下修改：一是，对违法销售或者提供网络关键设备、网络安全专用产品的行为，提高罚款标准，并增加规定：情节严重的，并可以责令暂停相关业务、停业整顿、吊销相关业务许可证或者吊销营业执照；二是，删去第七条第二款规定的“并可以责令暂停相关业务、停业整顿、关闭网站或者应用程序、吊销相关业务许可证或者吊销营业执照”中的“可以”；三是，进一步明确，窃取或者以其他非法方式获取、非法出售或者非法向他人提供个人信息，尚不构成犯罪的，由公安机关依照有关法律、行政法规的规定处罚。

此外，还对修正草案作了一些文字修改。

宪法和法律委员会已按上述意见提出了全国人民代表大会常务委员会关于修改《中华人民共和国网络安全法》的决定（草案），建议提请本次常委会会议审议通过。

修改决定草案和以上报告是否妥当，请审议。

全国人民代表大会宪法和法律委员会

2025 年 10 月 24 日

关于《中华人民共和国网络安全法（修正草案）》的说明

一、关于修改的背景和工作情况

党中央高度重视网络安全工作。习近平总书记强调：没有网络安全就没有国家安全，就没有经济社会稳定运行，广大人民群众利益也难以得到保障。网络安全法是网络安全领域的基础性法律，自 2017 年 6 月 1 日施行以来，对于维护国家网络空间主权、安全和发展利益，保护各方主体在网络空间的合法权益，促进经济社会信息化健康发展发挥了重要作用。

近年来，信息技术日新月异，网络应用更加普及，日益融入社会生产生活，与此同时，网络安全风险进一步凸显，利用网络从事网络入侵、网络攻击、传播违法信息等违法行为屡有发生。2021 年以来，全国人大常委会持续推进网络领域相关立法，数据安全法、个人信息保护法等相继制定实施。贯彻落实党的二十届三中全会关于加强网络空间法治建设的重要部署，适应网络安全新形势新要求，加强与网络领域相关立法的衔接协调，对网络安全法法律责任制度作出修改完善，加大对部分违法行为的处罚力度，推动形成良好网络生态是必要的。

网络安全法（修改）列入了十四届全国人大常委会立法规划和年度立法工作计划。中央网信办会同全国人大常委会法工委深入开展调研，广泛听取有关部门、企业、行业组织和专家学者等各方面意见，两次向社会公开征求意见，在此基础上形成网络安全法修正草案。

二、关于修改的总体思路

此次网络安全法修改主要把握以下四点：一是坚持以习近平新时代中国特色社会主义思想为指导，深入贯彻习近平法治思想和习近平总书记关于网络强国的重要思想。二是坚持问题导向，重点强化网络安全法律责任，加大对违法行为处罚力度。三是坚持体系化衔接，加强与数据安全法、个人信息保护法、行政处罚法等相关法律有机衔接，在行政处罚的种类、范围、幅度等方面作出合理安排。四是坚持分类施策，科学设置网络运行安全、网络信息安全等不同类型违法行为的法律责任。

三、关于修正草案的主要内容

修正草案共 9 条，主要内容包括：

（一）完善不依法履行网络运行安全保护义务行为的法律责任。一是，区分造成大量数据泄露、关键信息基础设施丧失局部功能等严重情形，以及造成关键信息基础设施丧失主要功能等特别严重情形，参照数据安全法有关规定，提高罚款幅度（修正草案第一条、第五条）；二是，对销售或者提供未经安全认证、安全检测或者安全认证不合格、安全检测不符合要求的网络关键设备和网络安全专用产品的行为，增加规定法律责任（修正草案第二条）；三是，对违反规定开展网络安全认证、检测、风险评估等活动或者向社会发布网络安全信息的行为，完善处置处罚措施（修正草案第四条）；四是，对关键信息基础设施运营者使用未经安全审查或者安全审查未通过的网络产品或者服务的行为，完善处置处罚措施（修正草案第六条）。

（二）完善不依法履行违法信息处置义务行为的法律责任。结合近年来网络信息内容违法行为执法实践，对网络运营者发现网络违法信息未依法采取相应处置措施，或者不按照有关部门的要求采取相应处置措施的行为，完善处置处罚措施；对造成特别严重影响、特别严重后果的违法情形，加大处罚力度。（修正草案第七条）

（三）做好侵害个人信息权益等行为法律责任的衔接。个人信息保护法规定了侵害个人信息权益行为的法律责任，数据安全法规定了违法向境外提供重要数据行为的法律责任。据此，将上述两种情形的法律责任改为衔接性规定，即适用个人信息保护法、数据安全法等法律、行政法规的规定予以处理、处罚。（修正草案第八条）

（四）增加从轻、减轻或者不予行政处罚的规定。根据 2021 年修订的行政处罚法，增加衔接性规定，明确网络运营者存在主动消除或者减轻违法行为危害后果、违法行为轻微并及时改正且没有造成危害后果、初次违法且危害后果轻微并及时改正或者有证据足以证明没有主观过错等情形的，依法从轻、减轻或者不予行政处罚。（修正草案第九条）

国家网络安全事件报告管理办法

（2025 年 9 月 11 日 国家互联网信息办公室）

第一条 为规范网络安全事件报告管理，及时控制网络安全事件造成的损失和危害，根据《中华人民共和国网络安全法》、《中华人民共和国数据安全法》、《中华人民共和国个人信息保护法》、《关键信息基础设施安全保护条例》等法律法规，制定本办法。

第二条 在中华人民共和国境内建设、运营网络或者通过网络提供服务的网络运营者，在发生网络安全事件时，应当按照本办法的规定进行报告。

第三条 国家网信部门负责统筹协调全国网络安全事件报告管理工作。省级网信部门负责统筹协调本行政区域内网络安全事件报告管理工作。

第四条 网络运营者在发现或获知涉及本单位的网络安全事件时，应当按照《网络安全事件分级指南》（见附件）进行研判，属于较大以上网络安全事件的，按以下程序报告：

涉及关键信息基础设施的，网络运营者应当第一时间向保护工作部门、公安机关报告，最迟不得超过 1 小时。属于重大、特别重大网络安全事件的，保护工作部门在收到报告后，应当第一时间向国家网信部门、国务院公安部门报告，最迟不得超过半小时。

网络运营者属于中央和国家机关各部门及其直属单位的，应当及时向本部门网信工作机构报告，最迟不得超过 2 小时。属于重大、特别重大网络安全事件的，各部门网信工作机构在收到报告后，应当第一时间向国家网信部门报告，最迟不得超过 1 小时。国家网信部门收到报告后及时向有关部门通报。

其他网络运营者应当及时向属地省级网信部门报告，最迟不得超过 4 小时。属于重大、特别重大网络安全事件的，省级网信部门在收到报告后，应当第一时间向国家网信部门报告，最迟不得超过 1 小时，并同时向同级有关部门通报。

本行业领域有专门规定的，网络运营者还应当按照行业主管监管部门要求报告。

涉嫌违法犯罪的，网络运营者应当及时向公安机关报案。

第五条 网络运营者应当以合同等形式要求为其提供网络安全、系统运维等服务的组织或个人，及时向其报告监测发现的网络安全事件，并协助其按照本办法规定报告网络安全事件。

第六条 鼓励社会组织和个人报告所获悉的较大以上网络安全事件。

第七条 报告网络安全事件时，应当包括下列内容：

（一）涉事单位名称及涉事系统或设施基本

情况；

（二）网络安全事件发现或发生的时间、地点、类型、级别，以及已造成的影响和危害，已采取的措施及效果；对勒索软件攻击事件，还应当包括要求支付赎金的金额、方式、日期等；

（三）事态发展趋势及可能造成的进一步影响和危害；

（四）网络安全事件原因初步分析意见；

（五）溯源调查工作线索，包括但不限于可能的攻击者信息、攻击路径、存在的漏洞等；

（六）拟进一步采取的应对措施以及请求支援事项；

（七）网络安全事件现场保护情况；

（八）其他应当报告的情况。

对于规定时间内不能判定事发原因、影响或发展趋势等网络安全事件情况的，可先报告第一项、第二项内容，其他情况及时补报。

网络安全事件报告后出现新的重要情况或调查工作取得阶段性进展的，涉事单位应当及时报告。

第八条 网络安全事件处置工作结束后，网络运营者应当于 30 日内对相关事件发生原因、应急处置措施、造成的危害、责任追究、完善整改情况、教训等进行全面分析总结，形成事件处置总结报告按照原渠道上报。

第九条 网信部门建设 12387 网络安全事件报告热线电话和网站、邮箱、传真等方式，统一接收网络安全事件报告。

第十条 网络运营者未按照本办法规定报告网络安全事件的，有关主管部门按照有关法律、行政法规的规定进行处罚。

因网络运营者迟报、漏报、谎报或者瞒报网络安全事件，造成重大危害后果的，对网络运营者及有关责任人依法从重处罚。

承担网络安全事件报告的部门未按照本办法规定报告网络安全事件的，依据有关法律、行政法规和网络安全工作责任制追究相关单位和人员责任。

第十一条 发生网络安全事件时，网络运营者已采取合理必要的防护措施，按照应急预案进行处置、有效降低网络安全事件影响和危害，并按照本办法规定及时报告的，可视情从轻或不予追究相关单位和人员责任。

第十二条 本办法所指网络安全事件是指由于人为原因、网络遭受攻击、网络存在漏洞隐患、软硬件缺陷或故障、不可抗力等因素，对网络和信息系统或其中的数据和业务应用造成危害，对国家、社会、经济造成负面影响的事件。

本办法所指网络运营者是指网络的所有者、管理者和网络服务提供者。

本办法所指《网络安全事件分级指南》参照《信息安全技术 网络安全事件分类分级指南》国家标准（GB/T 20986-2023）制定，以有限枚举的方式给出相关事件的分级定量指标。

第十三条 涉及国家秘密的网络安全事件报告，按照有关部门规定执行。

第十四条 本办法自 2025 年 11 月 1 日起施行。

附件

网络安全事件分级指南

一、特别重大网络安全事件

符合下列情形之一的，为特别重大网络安全事件：

1. 重要网络和信息系统遭受特别严重的系统损失，造成系统大面积瘫痪，丧失业务处理能力。

2. 核心数据、重要数据、海量公民个人信息丢失或被窃取、篡改、假冒，对国家安全和社会稳定构成特别严重威胁。

3. 其他对国家安全、社会秩序、经济建设和公众利益构成特别严重威胁、造成特别严重影响的网络安全事件。

通常情况下，满足下列条件之一的，可判别为特别重大网络安全事件：

1. 省级以上党政机关门户网站、中央重点新闻网站因攻击、故障，导致 24 小时以上不能访问。

2. 关键信息基础设施整体中断运行 6 小时以上或主要功能中断运行 24 小时以上。

3. 影响一个或多个省级行政区 50% 以上人口，或者 1000 万人以上用水、用电、用气、用油、取暖、交通出行、就医、购物等工作、生活。

4. 核心数据、重要数据泄露或被窃取、篡改、假冒，对国家安全和社会稳定构成特别严重威胁。

5. 泄露 1 亿人以上公民个人信息。

6. 省级以上党政机关门户网站、中央重点新闻网站、超大型网络平台等被攻击篡改，导致违法有害信息特大范围传播。以下情况之一，可认定为“特大范围”：

（1）在主页上出现并持续 6 小时以上，或在其他页面出现并持续 24 小时以上；

（2）通过社交平台转发 10 万次以上；

（3）浏览或点击次数 100 万以上；

（4）省级以上网信部门、公安机关认定为是“特大范围传播”的。

7. 造成 1 亿元以上的直接经济损失。

8. 其他对国家安全、社会秩序、经济建设和公众利益构成特别严重威胁、造成特别严重影响的网络安全事件。

二、重大网络安全事件

符合下列情形之一且未达到特别重大网络安全事件的，为重大网络安全事件：

1. 重要网络和信息系统遭受严重的系统损失，造成系统长时间中断或局部瘫痪，业务处理能力受到极大影响。

2. 核心数据、重要数据、大量公民个人信息丢失或被窃取、篡改、假冒，对国家安全和社会稳定构成严重威胁。

3. 其他对国家安全、社会秩序、经济建设和公众利益构成严重威胁、造成严重影响的网络安全事件。

通常情况下，满足下列条件之一的，可判别为重大网络安全事件：

1. 地市级以上党政机关、企事业单位门户网站，省级以上重点新闻网站因攻击、故障，导致 6 小时以上不能访问。

2. 关键信息基础设施整体中断运行 1 小时以

上或主要功能中断运行 3 小时以上。

3. 影响一个或多个地市级行政区 50% 以上人口，或者 100 万人以上用水、用电、用气、用油、取暖、交通出行、就医、购物等的工作、生活。

4. 核心数据、重要数据泄露或被窃取、篡改、仿冒，对国家安全和社会稳定构成严重威胁。

5. 泄露 1000 万人以上公民个人信息。

6. 地市级以上党政机关、企事业单位门户网站，省级以上重点新闻网站，大型以上网络平台等被攻击篡改，导致违法有害信息大范围传播。以下情况之一，可认定为“大范围”：

（1）在主页上出现并持续 2 小时以上，或在其他页面出现并持续 12 小时以上；

（2）通过社交平台转发 1 万次以上；

（3）浏览或点击次数 10 万以上；

（4）省级以上网信部门、公安机关认定为是“大范围传播”的。

7. 造成 2000 万元以上的直接经济损失。

8. 其他对国家安全、社会秩序、经济建设和公众利益构成严重威胁、造成严重影响的网络安全事件。

三、较大网络安全事件

符合下列情形之一且未达到重大网络安全事件的，为较大网络安全事件：

1. 重要网络和信息系统遭受较大的系统损失，造成系统中断，明显影响系统效率，业务处理能力受到影响。

2. 重要数据、较大量公民个人信息丢失或被窃取、篡改、假冒，对国家安全和社会稳定构成较严重威胁。

3. 其他对国家安全、社会秩序、经济建设和公众利益构成较严重威胁、造成较严重影响的网络安全事件。

通常情况下，满足下列条件之一的，可判别为较大网络安全事件：

1. 地市级以上党政机关、企事业单位门户网站，省级以上重点新闻网站因攻击、故障，导致 2 小时以上不能访问。

2. 关键信息基础设施整体中断运行 10 分钟以上或主要功能中断运行 30 分钟以上。

3. 影响一个或多个地市级行政区 30% 以上人口，或者 10 万人以上用水、用电、用气、用油、取暖、交通出行、就医、购物等工作、生活。

4. 重要数据泄露或被窃取，对国家安全和社会稳定构成较严重威胁。

5. 泄露 100 万人以上公民个人信息。

6. 党政机关、企事业单位门户网站，重点新闻网站，网络平台等被攻击篡改，导致违法有害信息较大范围传播。以下情况之一，可认定为“较大范围”：

（1）在主页上出现并持续 30 分钟以上，或在其他页面出现并持续 2 小时以上；

（2）通过社交平台转发 1000 次以上；

（3）浏览或点击次数 1 万以上；

（4）省级以上网信部门、公安机关认定为是“较大范围传播”的。

7. 造成 500 万元以上的直接经济损失。

8. 其他对国家安全、社会秩序、经济建设和公众利益构成较严重威胁、造成较严重影响的网络安全事件。

四、一般网络安全事件

除上述网络安全事件外，对国家安全、社会秩序、经济建设和公众利益构成一定威胁、造成一定影响的网络安全事件。

国家互联网信息办公室于《网络数据安全风险评估办法（征求意见稿）》公开征求意见的通知

为规范网络数据安全风险评估活动，保障网络数据安全，促进网络数据依法合理有效利用，根据《中华人民共和国数据安全法》《网络数据安全管理条例》等法律法规，国家互联网信息办公室起草了《网络数据安全风险评估办法（征求意见稿）》，现向社会公开征求意见。公众可以通过以下途径和方式提出反馈意见：

1. 登录中国网信网（www.cac.gov.cn），进入首页“网信要闻”查看文稿。

2. 通过电子邮件方式发送至：shujuju@cac.gov.cn。

3. 通过信函方式将意见寄至：北京市海淀区阜成路 15 号国家互联网信息办公室网络数据管理局，邮编 100048，并在信封上注明“网络数据安全风险评估办法征求意见”。

意见反馈截止时间为 2026 年 1 月 5 日。

附件：网络数据安全风险评估办法（征求意见稿）

国家互联网信息办公室

2025 年 12 月 6 日

网络数据安全风险评估办法

（征求意见稿）

第一条 为了规范网络数据安全风险评估活动，保障网络数据安全，促进网络数据依法合理有效利用，根据《中华人民共和国数据安全法》、《中华人民共和国网络安全法》、《网络数据安全管理条例》等法律法规，制定本办法。

第二条 在中华人民共和国境内开展网络数据安全风险评估，应当遵守本办法。法律、行政法规、部门规章另有规定的，依照其规定。

本办法所称网络数据安全风险评估（以下简称风险评估），是指对网络数据和网络数据处理活动安全进行的风险识别、风险分析和风险评价等活动。

第三条 国家网信部门在国家数据安全工作协调机制指导下，统筹各地区、各部门开展风险评估，加强工作协调、信息共享。

第四条 各有关主管部门应当按照“谁管业务、谁管业务数据、谁管数据安全”的原则，定期组织开展本行业、本领域风险评估，可以根据工作需要对本行业、本领域的重要数据处理者开展风险评估

情况进行检查，并于每年 1 月底前向国家网信部门报送年度风险评估及检查计划。

省级网信部门统筹省级有关部门制定本行政区域年度风险评估及检查计划，按照前款要求报送国家网信部门。

第五条 国家网信部门在国家数据安全工作协调机制指导下，统筹有关主管部门和省级网信部门报送的年度风险评估及检查计划，避免重复评估、重复检查。

各有关部门开展检查不得向被检查的网络数据处理者收取费用。

第六条 处理重要数据的网络数据处理者（以下简称重要数据处理者）应当每年度对其网络数据处理活动开展风险评估。重要数据安全状态发生重大变化可能对数据安全造成不利影响的，应及时对发生变化及其影响的部分开展风险评估。

鼓励处理一般数据的网络数据处理者（以下简称一般数据处理者）至少每 3 年开展一次风险评估。

第七条 风险评估工作应当按照《网络数据安全管理条例》有关要求和《数据安全技术 数据安全风险评估方法》（GB/T 45577）等有关国家标准开展。有关主管部门对本行业、本领域风险评估工作另有规定的，从其规定。

第八条 网络数据处理者可以自行或者委托第三方评估机构（以下简称评估机构）开展风险评估。

网络数据处理者自行开展风险评估，应当指定专人负责。网络数据处理者委托评估机构开展风险评估，应当优先选择通过认证的评估机构，并通过订立合同或者其他具有法律效力的文件等方式明确双方的权利、责任和保密义务等。

第九条 经国务院认证认可监督管理部门依法批准的具有数据安全服务认证资质的认证机构，可按照《数据安全技术 数据安全评估机构能力要求》（GB/T 45389）等有关国家标准、行业标准对评估机构开展认证。

第十条 评估机构开展风险评估应当遵守法律法规，公正客观地作出风险判断，并对所出具的风险评估报告真实性、有效性、完整性负责，不得再委托其他机构开展风险评估。

第十一条 同一评估机构及其关联机构不得连续 3 次以上对同一网络数据处理者开展风险评估。

第十二条 评估机构在风险评估过程中发现网络数据处理活动存在重大数据安全风险的，应当及时通报网络数据处理者，并按照有关规定向省级以上网信部门、有关主管部门报告。

评估机构及其工作人员应当对在风险评估过程中获得的数据、商业秘密、保密商务信息等依法予以保密，不得泄露或者非法向他人提供，在风险评估工作结束后及时删除相关信息。

第十三条 重要数据处理者开展年度风险评估应当按照本办法附件模板编制评估报告，一般数据处理者可以参照本办法附件模板编制评估报告。有关主管部门对风险评估报告模板另有规定的，从其规定。

风险评估报告至少保存 3 年。

第十四条 重要数据处理者应当在年度风险评估完成后的 10 个工作日内按照有关主管部门要求报送评估报告。主管部门不明确的，向省级网信部门或者国家网信部门报送。

有关主管部门应当公开评估报告报送渠道和联系方式，及时接收重要数据处理者报送的评估报告，自收到评估报告之日起的 10 个工作日内将报告通报同级网信部门。国家网信部门汇总相关报告并报送国家数据安全工作协调机制。

省级以上网信部门和有关部门可对网络数据处理者的评估报告真实性、准确性进行抽查核验，网

络数据处理者应当配合开展抽查核验。

第十五条 省级以上网信部门和有关部门在风险评估报告核验、监督检查等工作中发现网络数据处理者有以下情形之一的，应当要求其委托通过认证的评估机构开展风险评估：

（一）网络数据处理活动存在较大安全风险的；

（二）发生网络数据安全事件，导致重要数据或者大规模个人信息泄露、被窃取的；

（三）网络数据处理活动可能危害国家安全、公共利益的；

（四）国家网信部门或者有关部门规定的其他情形。

对同一网络数据安全事件或者风险，不得重复要求网络数据处理者委托评估机构开展风险评估。

第十六条 网络数据处理者按照有关部门要求委托评估机构开展风险评估的，应当履行下列义务：

（一）为评估机构开展风险评估工作提供必要支持，包括为风险评估人员提供访问网络数据设施、网络数据、系统及操作日志记录权限等；

（二）在限定时间内完成风险评估，承担评估费用，情况复杂的，报有关部门批准后可以适当延长；

（三）在完成风险评估后将评估机构出具的评估报告报送有关部门，评估报告应当由评估机构主要负责人、风险评估负责人签字并加盖机构公章；

（四）按照有关部门要求对风险评估中发现的问题进行整改，在整改完成后 15 个工作日内，向有关部门报送整改情况报告。

网络数据处理者不得以任何方式要求或者示意评估机构出具不实或者不当的评估报告。

第十七条 有关部门在组织风险评估工作中发现存在可能危害国家安全、公共利益的网络数据处理活动，应当责令网络数据处理者进行整改；对整改不到位、拒不整改的网络数据处理者，可以采取要求其停止处理重要数据等措施。

第十八条 各地区、各部门应当加强风险信息共享和协同处置，及时处置风险评估工作中发现的安全风险和问题，并按照有关规定及时报告。

省级网信部门统筹协调本行政区域内风险信息共享和协同处置工作，于每年 3 月底前向国家网信部门报送上一年度风险信息处置情况，国家网信部门汇总相关情况报送国家数据安全工作协调机制。

第十九条 任何组织、个人有权对风险评估中的违法违规活动向有关部门进行投诉、举报，收到投诉、举报的部门应当依法及时处理。

第二十条 省级以上网信部门和有关部门发现网络数据处理者未按规定开展风险评估的，应当依据《中华人民共和国数据安全法》等法律法规予以处置处罚。

发现评估机构违反本办法开展风险评估的，省级以上网信部门和有关部门应当责令其进行整改；情节严重的，可以限制或者禁止其开展风险评估活动，追究相关人员责任，并予公布；构成犯罪的，依法追究刑事责任。

第二十一条 风险评估、网络安全等级保护测评、数据安全管理认证、个人信息保护合规审计、商用密码应用安全性评估等内容重合的，相关结果可以互相采信，避免重复评估、审计、认证。

第二十二条 重要数据处理者提供、委托处理、共同处理重要数据前进行风险评估，可以参照本办法有关规定执行。

第二十三条 核心数据处理者的风险评估，按照国家有关规定执行。

第二十四条 开展涉及国家秘密、工作秘密的风险评估活动，按照《中华人民共和国保守国家秘密法》等法律、行政法规及国家保密规定执行。

第二十五条 本办法自 年 月 日起生效。

武汉市生成式人工智能发展安全公约

为规范全市范围内生成式人工智能的研发、部署、使用和管理等活动，确保健康、有序、可持续发展，特制定本公约。

一、总则

1. 适用范围

本公约适用于在本市行政区域内，从事生成式人工智能相关业务的企事业单位、科研机构、高校以及其他社会组织和个人。包括但不限于利用生成式人工智能进行内容创作（如文本、图像、音频、视频等）、智能决策辅助、自动化服务提供等活动的所有参与者。

2. 基本原则

合法合规原则。严格遵守国家法律法规，落实国家互联网信息办公室发布的《生成式人工智能服务管理暂行办法》等各项行业管理规定，确保所有涉及生成式人工智能的行为均有法可依、有章可循。

安全可靠原则。将安全作为生成式人工智能技术发展与应用的首要前提，确保技术全生命周期的可控性，防范技术失控带来的安全风险。

伦理道德原则。遵循社会公认的伦理准则和道德规范，确保 生成式人工智能技术应用符合社会主义核心价值观，尊重人权、保护隐私、避免歧视，防止技术被用于不良目的或产生有害影响。

数据合规原则。严格遵守数据保护法律法规，规范数据收集、存储、使用、共享等环节，保障数据安全与个人隐私。

创新发展原则。鼓励生成式人工智能技术创新，推动技术与城市发展深度融合，提升城市治理现代化水平，促进经济社会高质量发展。

二、安全与风险管理

1. 强化网络安全防护。研发和应用生成式人工智能系统应具备高可靠性和稳定性，具备故障检测、预警与自动修复能力，防止系统崩溃或异常运行导致的安全事故。采取先进的网络安全技术，防范网络攻击、数据泄露、恶意篡改等安全威胁，确保系统网络安全。

2. 确保算法合理性。具有舆论属性或者社会动员能力的深度合成服务提供者，应当按照《互联网信息服务算法推荐管理规定》履行备案和变

更、注销备案手续。对生成式人工智能算法进行定期审查与评估，防止算法偏见、歧视、误导性输出等问题，确保算法公平、公正、透明。

三、数据与隐私管理

1. 严防数据泄露。坚持“最小必要”与“全生命周期安全”原则，强化数据采集、传输、存储、处理、销毁等各环节的防护措施，完善访问控制与审计机制，防止个人信息及敏感数据泄露。

2. 防范污染滥用。严格核验训练与应用数据来源，防止引入带有恶意、偏见或错误的信息。建立数据污染检测与清理机制，保障训练数据的合法性、准确性与健康性，防止模型输出受污染影响。

3. 加强隐私保护。严格遵守个人信息保护法律法规，对涉及个人信息的数据进行特殊保护，采取匿名化、去标识化等技术手段，防止个人信息泄露与滥用。建立健全隐私投诉处理机制，保障数据主体的合法权益。

四、内容审核与知识产权保护

1. 内容生成规范性。利用生成式人工智能生成的内容应当符合社会主义核心价值观和社会公序良俗，不得包含违法、淫秽、暴力、恐怖、煽动仇恨等不良信息。建立完善的内容过滤机制，对生成的内容进行实时监测和筛选，维护真实、可信、清朗的网络信息环境。引导用户正确使用生成式人工智能工具，培养健康的创作习惯和文化氛围。

2. 版权归属明确性。尊重生成内容的知识产权，明确生成内容的知识产权归属，鼓励对原创性生成内容进行版权登记与保护。加强对生成式人工智能技术应用中知识产权的管理，防止侵犯他人知识产权，如未经授权使用受版权保护的数据进行训练等行为。

五、构建共治生态

1. 提升公众人工智能素养。在追求技术突破与市场发展的同时，同步投入安全建设与风险防控。推动人工智能基础知识与安全意识的公众普及，提升社会整体对生成式人工智能的理解与理性使用能力。

2. 强化合作与交流。积极参与国内外人工智能安全治理合作与标准体系建设，推动形成透明、包容、公正的全球治理框架，助力生成式人工智能朝着更加安全、可靠、可持续的方向发展。

六、附则

1. 公约修订。本公约将根据国家法律法规调整、技术发展趋势以及本市生成式人工智能技术应用实际情况，适时进行修订完善。

2. 生效日期。本公约自发布之日起生效。

武汉市网络安全协会党支部参加互联网行业党委“铭记历史，砥砺奋进”主题党日活动

为纪念中国人民抗日战争暨世界反法西斯战争胜利 80 周年，进一步加强行业党员理想信念教育，激发爱国情怀。近日，互联网行业党委组织开展＂铭记历史，砥砺奋进＂主题党日活动，武汉市网络安全协会党支部多名党员代表参加此次活动。

活动中，全体人员共同观看了历史题材电影《南京照相馆》。该片取材于真实历史事件，以南京大屠杀为历史背景，通过艺术化手法再现了 1937 年南京城破后，一群素不相识的普通人在＂吉祥照相馆＂中守护日军暴行底片的故事。

观影结束后，武汉市网络安全协会党员代表何溪山结合自身工作畅谈感悟。他表示：＂影片中暗房里缓缓显影的不仅是胶片，更是民族记忆的觉醒。故事主角用生命守护的相册，与我们今天守护的网络空间安全

本质相通，都是对正义与真相的捍卫。作为网络安全从业者，我们要像守护底片的先辈一样，筑牢数字防线，让历史真相在信息时代永不褪色。＂

此次主题党日活动的开展，进一步激发了党员的历史责任感和使命感。大家纷纷表示，将把观影感悟转化为工作动力，立足岗位、担当作为，以实际行动传承红色基因，践行初心使命。

观阅兵 强信念 护网络 践初心 | 武汉市网络安全协会党支部组织开展九三阅兵观看活动

9 月 3 日，武汉市网络安全协会党支部及秘书处全体成员，集中观看纪念中国人民抗日战争暨世界反法西斯战争胜利 80 周年阅兵仪式直播，以庄重仪式感传承红色基因、凝聚行业力量。

上午 9 时许，阅兵仪式准时开始，全体成员起立肃立，伴随激昂的国歌旋律致敬祖国。当徒步方队迈着铿锵步伐通过检阅台、现代化装备方阵依次亮相。新组建的军事航天部队、网络空间部队、信息支援部队首次受阅，作为网络安全从业者，协会全体党员及员工眼中满是自豪与振奋。

观看结束后，协会还组织简短交流。成员们纷纷表示，阅兵式展现的国家实力与军人风貌令人心潮澎湃，作为网络安全工作者，更深刻认识到“网络空间是国家安全的重要组成部分”。未来将以“筑牢网络安全防线”为己任，在关键信息基础设施保护、网络和数据安全治理、促进行业发展等领域主动作为，为维护国家网络空间主权、安全和发展利益贡献自己的力量。

《安安说网安之科普小课堂》

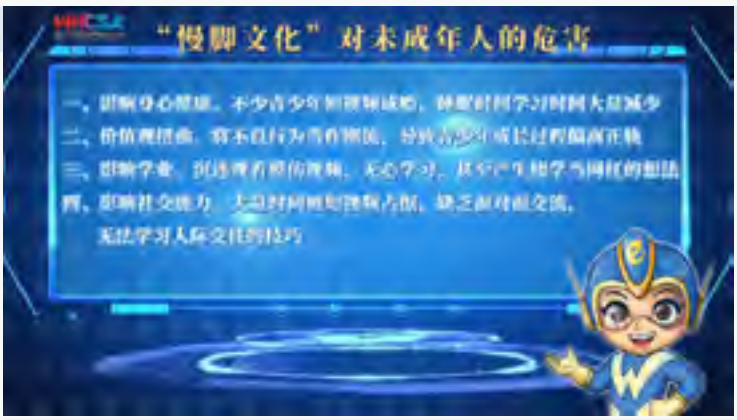
No.3 维护未成年人健康网络环境

本期主要内容

01 典型案例报道

“慢脚文化”在网络上侵害未成年人的典型案例

02 详细说明危害



“慢脚文化”对未成年人的危害

03 科普法律法规

安安科普相关法规

《安安说网安之科普小课堂》

No.4 维护未成年人健康网络环境

本期主要内容

01 典型案例报道

网络诈骗的典型案例

02 详细说明危害

安安介绍防诈小妙招

03 科普法律法规

安安科普相关法规

2025

武汉市国家网络安全宣传周

网络安全为人民
网络安全靠人民

武汉市国家网络安全宣传周灯光秀绽放两江四岸

2025 年 9 月 15 日至 21 日是国家网络安全宣传周，今年活动主题为“网络安全为人民、网络安全靠人民”——以高水平安全守护高质量发展武汉市积极响应并举办一系列宣传活动下面请欣赏网络安全主题长江灯光秀

武汉龟山电视塔

汉口江滩建筑群

武汉长江二桥

武汉网络安全号公交正式启航

2025 年武汉市国家网络安全宣传周正火热进行中（9.15-9.21），今年主题“网络安全为人民，网络安全靠人民”，在武汉有了超接地气的打开方式！

“网安专车”巡游全城，安全感一路随行

武汉市打造的“网安专车”正式启航！主题车身醒目亮眼，成为街头流动的“网络安全宣传站”。乘车途中，不仅能沉浸式感受网安氛围，还有专业人员随车讲解 —— 从防范电信诈骗到保护个人信息，从识别钓鱼链接到守护支付安全，干货满满的知识搭配趣味互动体验，让市民在通勤路上轻松 get 网安技能，真正实现“坐一趟车，学一套防护招”！

网安嘉年华全城联动点亮武汉网红地标

武汉市国家网络安全宣传周期间，以“网络安全为人民，网络安全靠人民”为主题的一场场别开生面的“武汉网络安全 City Walk”打卡分享活动，在火车站、机场、各大网红地标开展。在武汉市各大热门地点构建起 " 行走的网络安全课堂 "，实现了专业知识与城市空间的有机融合。

部分地区活动采用“集章打卡”的游园会形式，巧妙设置了知识科普区、趣味游戏区、互动打卡区和礼品兑换区四个区域，吸引了众多市民的目光，大家纷纷踊跃参与，为国家网络安全宣传周增添了一抹亮丽的色彩。

黄鹤楼打卡点

在知识科普区，网络安全案例展板前人头攒动。工作人员通过“快问快答”的互动方式，将网络安全知识以生动有趣的形式呈现给市民。市民们积极思考、踊跃回答，答对问题即可获得一枚印章。这种轻松愉快的学习方式，让市民们在不知不觉中加深了对网络安全知识的理解和记忆。趣味游戏区更是热闹非凡，“净网沙包”“安全套圈”“防火墙拆塔”等游戏，将网络安全知识巧妙地融入其中。市民们在尽情玩耍的同时，也

昙华林打卡点

杨泗港大桥打卡点

东湖绿道打卡点

黎黄陂路巴公房子打卡点

提升了自身的网络安全意识和防护技能。

在各大热门地点，互动打卡区的网络安全主题创意背景板成为了市民们的热门打卡点，大家纷纷拍照留念，并分享至朋友圈，向更多人宣传网络安全的重要性。

此次＂文旅＋科普＂的网安宣传模式，为武汉网络安全知识普及提供了可复制、可推广的新路径。市民可持续关注＂武汉网络安全＂官方账号，获取最新网安防护指南、参与线上互动学习，将打卡活动中习得的知识转化为日常数字生活的防护习惯，共同为构建安全、健康的数字环境注入持久动力。

武汉天河机场打卡点

网络安全宣传点亮相武汉、汉口火车站

2025年9月15日至21日，国家网络安全宣传周期间，武汉市网络安全宣传点，亮相武汉、汉口火车站，开展以“网络安全为人民，网络安全靠人民”为主题的2025国家网络安全宣传周活动。

“谨防新型AI诈骗，遇到熟人借款等情形，尽量通过多种方式确认对方是否为本人！”活动期间，民警和志愿者通过发放宣传资料、现场讲解互动问答等形式，向旅客普及网络安全知识，本次活动得到了武汉铁路公安处的大力支持，让“网络安全为人民，网络安全靠人民”的理念深入人心有效提升旅客的网络安全意识和防范能力。

黄鹤杯专栏

一、大赛介绍

2016 年以来，武汉市每年在国家网络安全与人才创新基地组织举办“黄鹤杯”网络安全人才创新大赛，目前该赛事已发展为具有广泛影响力的国家级网络安全品牌赛事。2025 年“黄鹤杯”以“聚智网安·筑梦黄鹤”为主题，重磅推出职工技能专项赛、江城校园新星赛、实景攻防沙场赛及创新成果擂台赛四大赛道，大赛设置丰厚奖励。聚力发掘实战型网安人才，加速创新成果转化落地，为加快推动国家网络安全人才与创新基地建设发展，促进网络安全产业高质量发展注入人才和创新动能。

二、组织机构

主办单位：武汉市委网信办、武汉市总工会、武汉网络安全大学（筹）、国家网络安全人才与创新基地

承办单位：武汉市网络安全协会

三、赛事介绍

职工技能专项赛

聚焦在职人员的实战技能，采用线上 CTF 与线下 AWD 攻防对抗的赛制，赛题直指工作痛点以锤炼真实能力。赛事汇聚各行业精英同场较量，其突出的职业激励在于，优秀选手有机会获得“武汉市五一劳动奖章”这一重磅荣誉，为职业发展提供强力背书。

面向各领域在职职工（含企事业单位、社会组织等），不限职业背景，具备网络安全相关技能或从业经验的个人均可报名。

创新成果擂台赛

它不仅是赛事，更是连接人才与产业的“超级连接器”。赛事采用“理论创新”与“实践创新”双轨并行模式，完整覆盖从基础研究到产业应用的全链条，并严格强调成果的原创性与解决行业实际问题的实用价值。

面向企业、高校院所（含学生团队）、独立开发者等的网络安全创新团队或个人。

实景攻防沙场赛

顶级白帽子的实战盛会，其核心亮点在于突破虚拟环境，在线下决赛中直接对真实的智能网联汽车进行实景渗透攻击，挖掘能影响行车安全的高危漏洞。赛事旨在“以攻促防”，选手发现的漏洞及修复方案将直接推动车企安全升级，实现技术价值向产业防线的快速转化。

面向国内相关专业机构从业人员、国内相关技术爱好者、持有合法白帽子资质（如 CNVD/CNNVD 认证）的网络安全技术个人。

江城校园新星赛

专为高校学子设立，高度聚焦实战能力培养。赛事采用风靡全球的 CTF 及 AWD 攻防形式，让学生在贴近真实的对抗中将理论知识转化为实战技能。它为不同层次院校的学生提供了公平的全国性竞技舞台，优胜者不仅能获得奖励，还有机会赢得网络安全头部企业的实习机会，为职业生涯奠定坚实基础。

面向全国高校在读学生（含专科、本科、研究生），以 3 人团队形式参赛，重点面向在汉高校相关专业学生。

聚智网安 筑梦黄鹤
“黄鹤杯”大赛在汉收官

2025 年“黄鹤杯”网络安全人才创新大赛于 10 月下旬在国家网络安全人才与创新基地成功举办。本届大赛以“聚智网安·筑梦黄鹤”为主题，设置职工技能专项赛、创新成果擂台赛、实景攻防沙场赛、江城校园新星赛四大赛道，吸引全国千余名选手参与，涌现出一批优秀人才与创新成果，全面展现了我国网络安全领域的实践水平与技术潜力。

本届大赛由武汉市委网信办、武汉市总工会、国家网络安全人才与创新基地共同主办，武汉市网络安全协会、国家网络安全人才与创新基地产业联盟联合承办，并得到东风汽车集团研发总院、小米安全中心、攀升等单位的支持。

职工技能专项赛：立足实战，锤炼行业尖兵

职工技能专项赛面向各行业在职人员，采用“线上 CTF ＋线下 AWD”双模式综合考核选手在漏洞挖掘、系统防护等方面的实战能力。来自交通银行湖北省分行的程子丘荣获一等奖，武汉市中心医院瞿朗、招联消费金融公司的何卓仟与李忠明分获二等奖。获奖选手覆盖金融、医疗、通信、公安等领域，凸显网络安全在多行业深度融合与广泛需求。

创新成果擂台赛：推动理论实践融合，助力技术落地

理论创新赛道中，武汉大学国家网络安全学院“珞珈山堆栈小分队”凭借“羽盾轻链——基于向量承诺

聚合技术的数字货币交易验证系统”获得一等奖。该系统在区块链交易验证领域实现重要突破，吞吐量达2.9KTPS，为同类系统的1.8至4.9倍。

实践创新赛道方面，武汉江民网安科技有限公司研发的“完全自主可控恶意代码监测系统”斩获一等奖。该系统已在全国电网超1000家电厂部署，并参与多项国家级重大活动安保任务，展现出国产安全技术的成熟应用能力。

实景攻防沙场赛：聚焦智能网联，强化实战能力

作为本届赛事亮点，实景攻防赛聚焦智能网联汽车安全，依托东风汽车集团研发总院提供的真实智能网联车辆和靶场平台，构建“远程渗透+本地实战”双模式对抗环境。北京天融信网络安全技术有限公司李泉荣获一等奖，大连工业大学谷明轩、武汉科技大学李瑞琛、武汉汉融通数智科技有限公司李振瑞等选手分获二等奖。本赛道有效推动车联网安全技术从研究走向实践，为行业培养具备实景攻防能力的专业人才。

江城校园新星赛：培育青年力量，夯实人才基础

面向全国高校的江城校园新星赛共吸引125所高校255支队伍参赛。经过CTF初赛与AWD决赛的激烈角逐，许昌学院“RedBean”战队荣获一等奖，湖北大学“HUBUSHFY”、平顶山学院“彳亍不彳亍”、郑州警察学院“彩虹七号”等团队分获二等奖，湖北汽车工业学院“PokerFace5”等5个个团队获三等奖。青年学子在实战中提升技能、展现潜力，为我国网络安全事业储备了坚实后备力量。

打造网安赛事品牌，构筑人才技术产业生态

“黄鹤杯”大赛持续推动“以赛促学、以赛促创、以赛聚才”，逐步构建起“人才—技术—产业”良性生态，已成为武汉贯彻落实网络强国战略、加快打造“中国网谷”的重要平台。

武汉市委网信办相关负责人表示，未来将继续深化政产学研用协同，推动创新成果转化与应用，为我国网络安全事业高质量发展持续贡献“武汉力量”。

2025年“黄鹤杯”职工技能专项赛获奖名单

一等奖

程子丘	交通银行股份有限公司湖北省分行
瞿　朗	武汉市中心医院

二等奖

何卓仟	招联消费金融股份有限公司
李忠明	招联消费金融股份有限公司
席　晨	中国移动通信集团湖北有限公司
李志彬	中国建设银行股份有限公司湖北省分行

三等奖

向思豪	中国电信股份有限公司湖北分公司
罗宗斌	江西机电职业技术学院
黄思源	武汉网络安全技术有限公司

优胜奖

薛道威	中国联合网络通信有限公司湖北省分公司
常　磊	招联消费金融股份有限公司
范　涛	中国联合网络通信有限公司湖北省分公司
胡　曦	武汉市公安局汉阳区分局
吴佳骅	武汉城市职业学院
王晓琪	北京天下信安技术有限公司
汪俊峰	中国移动通信集团湖北有限公司武汉分公司全

2025 年“黄鹤杯”
实景攻防沙场赛获奖名单

一等奖

李　泉	北京天融信网络安全技术有限公司

二等奖

谷明轩	大连工业大学艺术与信息工程学院
李瑞琛	武汉科技大学
李振瑞	武汉汉融通数智科技有限公司

三等奖

姚广政	奇安信网神信息技术(北京)股份有限公司
赵昱杰	常州信息职业技术学院
吴启明	广东海洋大学
蔡维嘉	奇安信网神信息技术(北京)股份有限公司
唐　铮	湖北东方网盾信息安全技术有限公司

优胜奖

汤　仟	奇安信网神信息技术(北京)股份有限公司
冷和博	奇安信网神信息技术(北京)股份有限公司
邓　轩	湖北东方网盾信息安全技术有限公司
钟悦康	武汉交通职业学院
吴　伟	联通(湖北)产业互联网有限公司
王　健	联通(湖北)产业互联网有限公司

2025 年“黄鹤杯”
江城校园新星赛获奖名单

一等奖

RedBean	许昌学院

二等奖

UBUSHFY	湖北大学
彳亍不彳 于	平顶山学院
彩虹七号	郑州警察学院

三等奖

PokerFace	湖北汽车工业学院
西柚的那就这个	中国人民警察大学
贪生pass	郑州警察学院
mo0n1ight	河南警察学院
havefun	武汉工程大学

优胜奖

T3st3r	郑州轻工业大学
私立键等学院	湖北民族大学
子怡说随便	河南警察学院
什么都不队	湖北汽车工业学院
做梦到flag	武汉城市职业学院
胡椒神话	湖北交通职业技术学院

2025 年“黄鹤杯”
创新成果擂台赛获奖名单

理论创新赛道

一等奖	武汉大学国家网络安全学院(珞珈山堆栈小分队)	羽盾轻链--基于向量承诺聚合技术的数字货币交易验证系统
二等奖	武汉大学国家网络安全学院ASAP课题组 严飞、王鹃、张立强、朱强	基于知识蒸馏的通用型车载网络入侵检测技术研究 面向演进的计算环境可信构建与分析关键技术研究
三等奖	湖北天融信网络安全技术有限公司及标准起草单位 湖北松颢科技有限公司 张帆，古天龙，刘小丽，郝峰锐，罗良逸，孙平	T/WHCSA008-2025智能网联汽车网络安全检测技术要求 网之追风电力安全检测综合可视化软件 基于关键表征和无关表征解耦的人脸识别反欺诈方法
优胜奖	网络安全技术学院(杨豪，刘志亮，郑卓闻汪文静，黄波，马金金，詹泽怡) 陈丽蓉 元启智境团队(湖北大学、武汉凌泽网安科技有限公司) 武汉安恒信息科技有限公司	面向可信数据交换的量子密钥分发与协商的机理研究 基于大模型的网络空间语义安全防御关键技术研究 基于安全大模型与语义代码知识图谱的多模态源代码认知 与智能分析研究 T/WHCSA 006-2024《数据要素场内流通安全评估规范》

实践创新赛道

一等奖	武汉江民网安科技有限公司	完全自主可控的恶意代码监测系统
二等奖	武汉众邦银行股份有限公司 深圳万物安全科技有限公司	线上金融业务安全深度对抗平台 AIOT孪生安全智能体(智能物联网李生安全智能体)
三等奖	国网湖北省电力有限公司武汉供电公司信息通信分公司 中金数据(武汉)超算技术有限公司 北京神州绿盟科技有限公司	基于人工智能技术的网络安全监测运营平台 中金数据(武汉)超算技术有限公司网络安全解决方案 "透视”加密黑盒:基于AI自学习的加密流量威胁检测实践
优胜奖	武汉市卫生健康信息中心(武汉市人口信息监测站) 湖北航天信息技术有限公司 联通(湖北)产业互联网有限公司 华中师范大学、武汉凌泽网安科技有限公司、北京神州绿盟科技有限公司	区域医疗大模型数据安全解决方案 武汉市智慧城市基础平台(一期)项目建设及服务安全体系解决方案 江汉区政务网络一体化安全运营应用案例 沉浸式攻防实训智能教学靶场络

2025 年“黄鹤杯”网络安全人才创新大赛创新成果擂台赛圆满收官 聚焦落地转化赋能产业高质量发展

2025 年 10 月 17 日，国家网络安全人才与创新基地培训中心内网安精英人才汇聚，2025 年“黄鹤杯”网络安全人才创新大赛创新成果擂台赛决赛在此圆满落幕。作为赛事四大赛道中唯一以“成果落地”为核心导向的竞赛单元，本届大赛以“聚智网安 · 筑梦黄鹤”为主题，秉持“理论筑基、实践强基”的核心理念，历经初赛严格筛选，最终从众多参赛项目中遴选出 24 项优质创新成果同台竞技，为网络安全行业呈现了一场融合学术前沿与实战价值的高端智慧交流盛宴。

一、专业赛事架构搭建公平竞技舞台

本届大赛由武汉市委网信办、武汉市总工会、国家网络安全人才与创新基地联合主办，武汉市网络安全协会、国家网络安全人才与创新基地产业联盟承办，小米安全中心、武汉攀升鼎承科技有限公司提供支持，自启动以来便以“高标准、严要求、重实效”为原则构建完善赛事体系。

决赛延续双赛道并行的模式，理论赛道聚焦网络安全前沿理论创新，实践赛道侧重技术方案的实战应

用与产业适配。各参赛团队需通过“15 分钟成果路演 +5 分钟评委答辩”的严苛环节接受检验，评审组则由两大赛道各 5 位行业权威专家组成，从创新性、科学性、技术水平、学术价值、应用价值五个维度进行量化评审，全方位保障评审结果的公平、公正与专业。

二、双赛道巅峰对决彰显网安创新实力

决赛现场，各参赛团队全力以赴展开激烈角逐，路演与答辩环节亮点纷呈，充分展现了我国网络安全领域的创新活力与人才实力。

理论赛道集中呈现了网络安全前沿技术的创新突破与标准引领作用。武汉大学珞珈山堆栈小分队的向量承诺聚合技术，为数字货币交易验证提供了新颖解

决方案；ASAP 课题组的知识蒸馏研究，推动了车载网络入侵检测技术的进步。在基础理论研究方面，严飞团队的计算环境可信构建研究，为系统安全奠定了理论基础；湖北天融信牵头制定的智能网联汽车检测标准，助力汽车产业信息安全规范发展。创新技术应用上，湖北松颢科技的电力安全检测软件实现可视化运维；张帆团队的人脸识别反欺诈方法，通过表征解耦提升生物识别安全性。在前沿探索领域，网络安全技术学院的量子密钥分发研究开辟了安全通信新路径；陈丽蓉的大模型语义安全防御研究，应对人工智能新兴威胁。元启智境团队的安全大模型与代码知识图谱、武汉安恒的数据流通安全评估规范、武汉数智云的数据分类分级指南，共同构建了从理论创新到标准落地的完整研究体系，为网络安全可持续发展提供了重要支撑。

实践赛道成果展现了网络安全技术在关键行业的深度应用与创新突破。武汉江民网安的完全自主可控恶意代码监测系统，体现了国产化安全能力的提升；众邦银行的线上金融业务安全对抗平台，为数字金融构建了主动防御体系；深圳万物安全的 AIOT 孪生安全智能体，创新性地将数字孪生技术应用于物联网安全领域。在关键基础设施方面，国网湖北电力的人工智能安全监测平台实现了电网网络的智能化运营；中金数据的网络安全解决方案为算力基础设施提供可靠保障。技术应用层面，北京神州绿盟的加密流量威胁检测项目，运用 AI 自学习技术破解加密流量分析难题；武汉市卫生健康信息中心的区域医疗数据安全方案，为医疗大模型应用筑牢安全基座。湖北航天信息的智慧城市安全体系、联通产业互联网的政务网络一体化运营案例、华中师范大学等单位的沉浸式攻防实训靶场、东湖高新集团的智慧园区主动防御体系，以及交通银行团队的 API 数据安全治理方案，共同展现了网络安全从传统防护向智能化、场景化、体系化发展的新趋势。

答辩环节中，评委们针对理论成果的转化路径、实践方案的市场推广潜力等关键问题展开深度问询，参赛选手从容应答，充分展现出扎实的专业功底与清晰的成果落地思考，赢得现场一致认可。

三、以赛促创搭建成果转化桥梁 赋能网安产业高质量发展

本届“黄鹤杯”网络安全创新成果赛以“理论 + 实践”双赛道及四大领域的覆盖，构建了高水平交流平台。大赛汇聚政策、技术、学术与投资领域的多元评委，实现了评审维度的全覆盖，保障了公平公正。通过特邀投资机构加入，赛事有力打通了“前沿研究 - 技术落地 - 金融赋能”的关键链路，为网络安全创新与产业融合注入了强劲动力。

大赛组委会相关负责人表示，后续将持续跟进参赛成果的发展动态，为符合市场需求的优质项目提供“场景对接、资源匹配”等全方位支持，切实发挥赛事“以赛选优、以赛促用”的核心作用。此次赛事的成功举办，不仅加速了网络安全创新成果的转化应用，更凝聚了行业创新力量，为网络安全产业高质量发展注入强劲动力。

创新成果擂台赛优秀成果展示（部分）

基于知识蒸馏的通用型车载网络入侵检测技术研究

■ 李思帆[1]、魏高达[1]、方泊璎[1]、曹越[1]
（1. 武汉大学国家网络安全学院，湖北 武汉 430072）

摘要：随着智能交通系统的发展，车载网络（IVNs）已成为车辆内部与外部通信的关键载体，但数据流量的复杂性和多样性给异常流量检测带来巨大挑战。同时，新技术的引入使车载网络面临更多安全漏洞，严重影响入侵检测系统（IDS）的准确性。为此，提出一种基于知识蒸馏技术的轻量化高效异常检测方法（KDBC），将双向编码器表征法（BERT）模型的深层语义知识迁移至轻量化卷积神经网络 - 双向长短期记忆神经网络组合模型（CNN-BiLSTM）架构，在不显著降低检测性能的前提下，大幅减少计算开销和存储需求。实验结果表明，KDBC 模型在汽车以太网、CAN 总线等多协议车载网络数据中均表现出优异的异常检测能力，在真实车载网关环境中验证的准确率和 F1 分数均超过 0.98，兼具安全性与通用性。

关键词：车载网络；入侵检测；知识蒸馏；BERT；CNN-BiLSTM

1、引言

智能交通系统的快速发展推动车载网络（IVNs）成为智能车辆的核心组成部分，实现电子控制单元（ECUs）间及与交通信号灯、路侧单元等外部设施的通信。车载网络主要包含汽车以太网、控制器局域网（CAN）和时间敏感网络（TSN），分别满足高带宽传输、低成本控制和实时性需求。然而，网络复杂性的提升和多协议融合使车载网络易受多种攻击，如 CAN 总线的拒绝服务（DoS）攻击、以太网的帧注入攻击及 TSN 的时间同步攻击，严重威胁行车安全。

现有入侵检测方法多针对单一协议场景，难以适配多协议融合的现代车载网络架构。同时，BERT 等深度学习模型虽检测精度较高，但计算开销大，无法部署于资源受限的车载环境；而 CNN-BiLSTM 等轻量化模型虽资源需求低，但通用性不足。为此，本文提出 KDBC 方法，通过知识蒸馏融合两类模型优势，实现多协议场景下的高效入侵检测，并在真实车载网关环境中验证其有效性。

2、基于知识蒸馏的入侵检测模型

2.1 系统模型

车载网络由汽车以太网、CAN 总线和 TSN 构成异

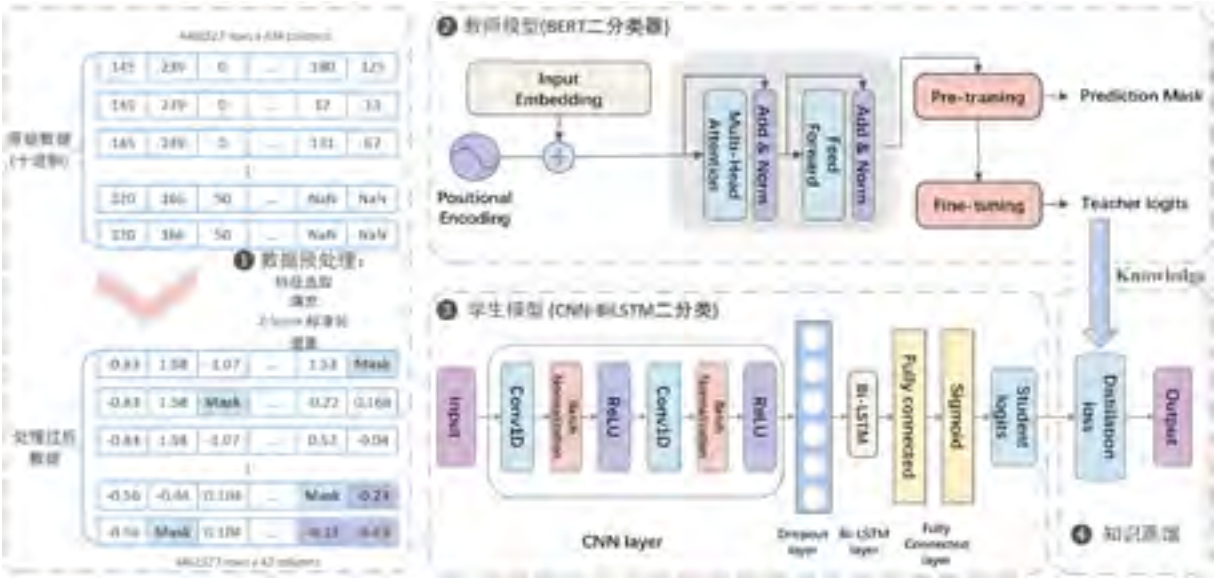


图 1：KDBC 框架流程示意图

构通信架构，中央网关作为数据交互核心，需同时防护多类型攻击。汽车以太网支持高级驾驶辅助（ADAS）等系统的高带宽数据传输；CAN 总线凭借可靠性和低成本成为控制通信主流；TSN 通过确定性传输满足自动驾驶等实时性需求。针对三类网络的攻击类型包括帧注入、MAC 泛洪、拒绝服务（DoS）、重放、模糊攻击等，KDBC 采用二分类设计，通过流量分析识别正常与异常状态。

2.2 KDBC 框架设计

如图 1 所示，KDBC 框架包含数据预处理、教师模型（BERT）、学生模型（CNN-BiLSTM）及知识蒸馏四大模块，形成从原始车载网络流量到精准异常检测的完整技术链路，各模块既独立发挥功能，又通过数据与知识流转形成闭环。

数据预处理针对多协议数据异构问题优化输入：通过互信息筛选 42 个关键特征，零填充统一 CAN 总线与以太网 / TSN 数据长度至 42 字节，Z-Score 归一化消除量级差异，再以 10% 概率进行随机掩码增强（70% 特征设为掩码、20% 替换为随机值、10% 不变），提升模型鲁棒性。

BERT 教师模型负责深层语义提取：输入嵌入层将流量转为“令牌 + 段 + 位置”三维向量，12 层 Transformer 编码器通过多头自注意力捕捉特征关联，微调阶段适配二分类任务，生成含攻击语义的高维特征。

CNN-BiLSTM 学生模型主打轻量化：两层卷积层提取局部空间特征，Dropout 抑制过拟合，双向长短时记忆网络（BiLSTM）捕捉时序依赖，全连接层输出结果，参数仅 26.4 万，远低于 BERT 的 1.09 亿，适配车载资源约束场景。

知识蒸馏采用响应式策略：以 BERT 预测为软标签，用 KL 散度损失引导学生学习；以真实标签为硬标签，用交叉熵损失保障精度，权重 0.5 融合双损失，实现“轻量化 + 高性能”平衡。

2.3 实验验证

实验采用 TOW-IDS（以太网 /TSN 数据）和 can-train-and-test（CAN 总线数据）数据集，硬件环境为 NVIDIA RTX 4090 GPU 和 AMD Ryzen Threadripper PRO 5995WX CPU，软件基于 PyTorch 框架开发。评价指标包括准确率、F1 分数及模型资源开销。

单一 TOW-IDS 数据集测试中，KDBC 准确率达 0.9966，F1 分数 0.9935，较原始 CNN-BiLSTM 分别提升 3.66 个百分点和 0.0534；混合数据集测试中，准确率和 F1 分数均超过 0.9996，接近 BERT 模型性能。资源开销方面，KDBC 模型大小仅 1.01MB，参数 26.4 万，远低于 BERT 的 417.64MB 和 1.09 亿参数。

真实车载网关测试（东风猛士 817）中，KDBC 在包含嗅探、扫描等未知攻击的场景下，准确率仍达 0.9842，F1 分数 0.9816，且模型大小仅为同类高性能模型的 1% 以下，满足车载环境部署需求。

3、结论

本文提出的 KDBC 方法通过知识蒸馏技术，成功将 BERT 模型的深层语义理解能力迁移至轻量化 CNN-BiLSTM 架构，实现了多协议车载网络的高效入侵检测。该方法解决了传统模型单一协议适配性差、资源开销与检测精度难以平衡的问题，在真实车载环境中表现出优异的准确性和鲁棒性。未来研究将进一步优化蒸馏策略，提升模型对未知攻击的检测能力和实时响应速度，为智能车辆安全提供更可靠的技术支撑。

参考文献

[1] 王浩轩，苏圣超，崔文霞．基于 GAN-Transformer 的车载网络入侵检测算法 [J]. 计算机工程与设计，2025, 46(6):1710-1716.

[2] Li S, Cao Y, Peng G, et al. Efficient Intrusion Detection for In-Vehicle Networks Using Knowledge Distillation from BERT to CNN-BiLSTM[J]. IEEE Transactions on Information Forensics and Security, 2025.

[3] Han M L, Kwak B I, Kim H K. TOW-IDS: intrusion detection system based on three overlapped wavelets for automotive ethernet[J]. IEEE Transactions on Information Forensics and Security, 2022, 18: 411-422.

[4] Song H M, Woo J, Kim H K. In-vehicle network intrusion detection using deep convolutional neural network[J]. Vehicular Communications, 2020, 21: 100198.

[5] Lampe B, Meng W. Can-train-and-test: A curated CAN dataset for automotive intrusion detection[J]. Computers & Security, 2024, 140: 103777.

[6] 蒋玉长，徐洋，李克资，等．基于深度学习的轻量级车载网络入侵检测方法 [J]. 计算机工程与应用，2023(22).DOI:10.3778/j.issn.1002-8331.2206-0474.

[7] 段晓英，曹生林，董力鸣，等 .SEP-LeNet: 基于深度学习的车载网络入侵检测方法 [J]. 计算机技术与发展 [2025-11-24].

面向演进的计算环境可信构建与分析关键技术研究

■ 严飞[1]、王鹃[1]、张立强[1]、朱强[1]
(1. 武汉大学 国家网络安全学院，湖北 武汉 430072)

摘要：随着计算环境向多架构、异构化、多元化演进，可信性与安全分析难度逐渐加大。因此，构建覆盖多场景的可信架构和安全分析体系变得尤为重要。本文提出了面向处理器的可信环境构造与安全分析方法，主要聚焦于硬件、虚拟化、智能计算与漏洞分析等领域。通过设计基于海光处理器的机密容器、华为鲲鹏处理器的链码可信化部署、商用 RISC-V 处理器的机密虚拟机架构以及 NPU 侧信道攻击的防护方案，提供了一整套可信环境和安全分析解决方案。同时，还提出了一种通用的可信动态混合远程证明方法和跨语言场景的计算环境漏洞挖掘方法，旨在为国产化、自主可控的可信计算环境提供理论支持与实践验证。

关键字：处理器环境、虚拟机环境、NPU 侧信道、远程证明、漏洞挖掘

1 引言

随着计算环境向多架构、异构化和多元化发展，系统的复杂性和安全性挑战日益增加。传统的安全分析方法已难以满足这些新兴平台的需求，尤其是在硬件、虚拟化和智能计算领域。因此，构建一个覆盖多场景的可信架构与安全分析体系显得尤为重要。

2 面向国产化处理器可信环境构造与度量方法

当前，国产化处理器平台存在可信环境容器度量能力不足问题 [1]。因此，依托海光处理器 CSV 硬件级安

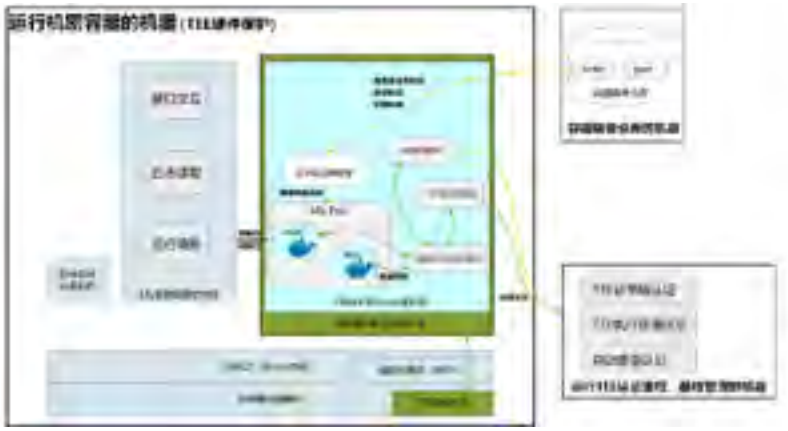


图 1 国产化处理器可信环境构造与度量架构

全防护能力，本文设计了一种基于 CSV 虚拟机的机密容器构建方法，实现了传统容器的快速迁移部署，并提供容器加载时可信度量能力。依托华为鲲鹏处理器的硬件级信任能力，本文设计了链码逻辑的可信化解耦与部署方法，确保链码的生命周期安全性。与普通的容器相比，在未引入额外的处理器性能损耗和内存损耗的情况下，实现了硬件级安全隔离保障功能与快速部署和迁移功能。该方法系统架构如图 1 所示。

3 基于商用 RISC-V 处理器的实用机密虚拟机架构

当前，RISC-V 平台不支持主流机密 VM 架构。运行在 RISC-V 平台上的非主流机密 VM 架构面临硬件兼容性的问题。因此，本文设计了一种可在现有 RISC-V 硬件上运行的 CVM 方案并实现了 Zion 原型系统，无需额外的安全硬件扩展的同时提高了兼容性 [2]。方案架构设计如图 1 所示。图 3 给出了各种操作的吞吐量和延迟比较，图 4 给出了不同文件大小的读写操作的性能比较。与当前现有的 CVM 解决方案相比，在 CVM entry 方面，Zion 的执行效率提高 44.7%。在 CVM exit 方面，Zion 的执行效率提高 55.3%。同时，Zion 在实际应用中产生的管理成本低于 5%。

图 2 机密虚拟机架构图

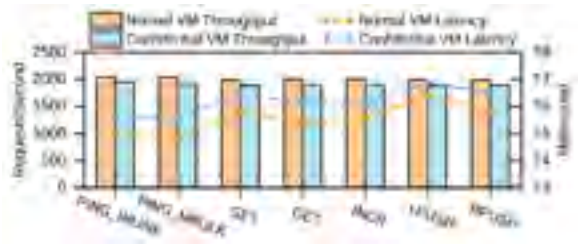


图 3 普通虚拟机和机密虚拟机之间各种操作的吞吐量和延迟比较

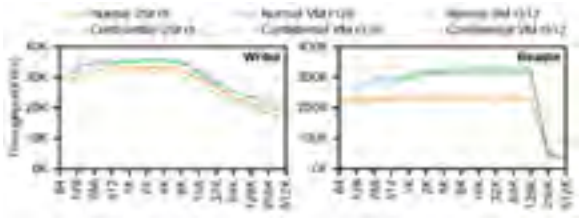


图 4 在普通和机密虚拟机中不同文件大小的读写操作的性能比较

4 面向 NPU 侧信道攻击的安全防护方案

当前，NPU 的内存侧信道攻击与故障注入攻击。因此，本文提出了一个面向 NPU 侧信道攻击的安全防护方案 [3],[4],[5]。方案架构如图 5 所示。核心设计包括: 特征图划分模块、加密压缩模块和完整性检测模块，分别从增加层边界、加密保护数据、完整性检测方面为 NPU 提供安全保障并全面抵御针对 NPU 的侧信道攻击。实验结果表明 , 该方案能够有效增加层边界 , 使攻击者通过内存侧信道攻击逆向推导的可能网络数量从 24 种增加到 7.86 × 105 种。可降低 60% 的存储空间的同时，仅带来 5% 的性能损失 , 比当前主流方案 DNNCloak[7] 减少 66.6% 的性能损失。

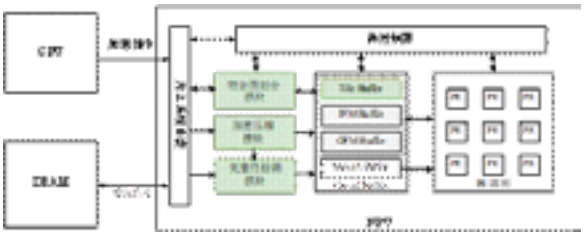


图 5 面向 NPU 侧信道攻击的安全防护方案架构

5 机密计算环境下通用可信动态混合远程证明方案

当前，国产化平台进行远程证明时，使用的算法缺乏时效性控制、跨平台兼容性差、过度依赖硬件等问题 [6]。因此，本文设计了一种通用可信动态混合远程证明方法，支持：跨平台认证、动态设备管理、跨平台兼容性等功能。同时，引入了 Shrubs 树并设计了静态与动态批量插入算法。与 Shrubs 树的原始插入算法相比，随着设备数量的增加，静态与动态批量插入算法至少减少 97.17% 和 97.13% 的计算成本。与发表在 NDSS2024 会议上的 zRA[8] 方案相比，非交互式模

式下执行时间最高减少 32.86%，交互式模式下执行时间减少 99.59%。方案架构设计如图 6 所示。

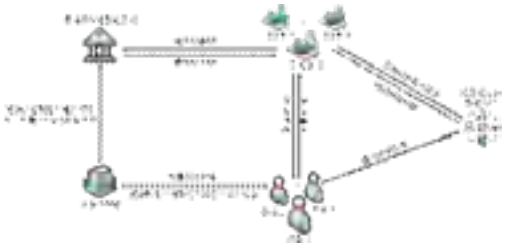


图 6 机密计算环境下通用可信动态混合远程证明方案架构

6 面向跨语言场景的计算环境漏洞挖掘方法

面向跨语言场景下计算环境漏洞挖掘领域，存在三个核心问题。一、如何全面准确的定位输入源点。二、如何进行高效的验证污点流。三、如何追踪跨语言的 Inter-Flow。因此，本文提出了一种基于数据标签的污点源识别方法、一种面向跨语言场景的静态控制流分析方法、一种基于关键结点感知的双向污点分析方案。同时，实现了一个面向跨语言场景的自动化固件漏洞挖掘系统 IFTaint。最终，IFTaint 成功挖掘了 100 余个漏洞，并获得了 40 余项 CVE 和 CNVE 证书，验证了该方法在跨语言场景下漏洞挖掘的有效性与应用潜力。

7 总结

本文通过深入研究处理器的可信环境与安全防护技术，提出了一系列创新性的解决方案。首先，在国产化处理器领域，通过依托海光处理器与华为鲲鹏处理器的硬件安全能力，设计了多种容器构建和链码部署方法，有效增强了可信度和安全性。其次，针对商用 RISC-V 平台的兼容性问题，设计了无需额外安全硬件扩展的机密虚拟机架构，显著提高了兼容性并优化了关键机制。对于 NPU 的侧信道攻击，提出了完整的安全防护方案，增强了对侧信道攻击的抵御能力。此外，本文还设计了一种跨平台、动态且通用的可信远程证明方法，并针对跨语言场景提出了高效的漏洞挖掘技术。这些研究不仅推动了国产化可信计算环境的建设，也为未来相关领域的安全防护提供了新的方法和工具。

参考文献：

[1] 严飞，何佳，宋飞扬，张立强，王鹃．一种面向端侧设备深度学习模型的抗逆向混淆方法及系统 :202510446301.5[P].2025-08-01.

[2] Wang Jie, Juan Wang, and Yinqian Zhang. ZION: A Practical Confidential Virtual Machine Architecture on Commodity RISC-V Processors.2025 62nd ACM/IEEE Design Automation Conference (DAC). IEEE, 2025.

[3] 胡文澳，严飞，张立强．一种面向 NPU 内存侧信道攻击的安全防护方案 [J]. 信息网络安全 ,2025,25(06):977-987.

[4] 胡文澳，张立强，严飞．基于混沌映射和压缩稀疏行的数据加密压缩方法及装置 :202510778636.7[P].2025-09-19.

[5] Ou Changhai, Zhenfang Qiu, Xingshuo Han, Fan Zhang, Shihui Zheng, and Fei Yan. MinMaxEntropy: Bound Model Errors for Side-Channel Leakages from Information Theory. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (2025).

[6] 朱强；严飞；张立强；王鹃；王瑞；欧长海．支持设备批量添加与删除的混合远程证明方法 :202511141120.8[P].2025-09-16.

[7]CHE Yuezhi, WANG Rujia. DNNCloak: Secure DNN Models Against Memory Side-channel Based Reverse Engineering Attacks.[C]// 2022 IEEE 40th International Conference on Computer Design (ICCD). New York: IEEE, 2022: 89-96.

[8]Ebrahimi, Shahriar, and Parisa Hassanizadeh. From interaction to independence:

zksnarks for transparent and non-interactive remote attestation.[C]// 31st

Annual Network and Distributed System Security Symposium, NDSS 2024,San Diego, California, USA, February 26 - March 1, 2024.

智能网联汽车网络安全检测技术规范研究

■ 孙秉稷[1]、范雪俭[2]、左世涛[3]、吕露[4]、安高峰[5]、胡雨翠[6]

(1. 湖北天融信网络安全技术有限公司；)

(2. 国家计算机网络应急技术处理协调中心；)

(3. 国家计算机网络应急技术处理协调中心湖北分中心；)

(4. 武汉市公安局交通管理局；)

(5. 东风汽车集团有限公司研发总院；)

(6. 岚图汽车科技有限公司)

摘要：为解决智能网联汽车车端网络及联网零部件系统的安全风险问题，构建系统化的网络安全检测体系，本文基于 GB/T 1.1—2020 等标准规范，制定了智能网联汽车网络安全检测技术要求。该技术要求涵盖车端总线、无线、主机三大类网络安全检测维度，明确了 CAN/CANFD 总线、蓝牙、固件等关键模块的检测指标、安全要求及实施方法。通过模糊检测、模拟攻击、漏洞扫描等技术手段，实现对数据真实性、保密性、完整性等核心安全属性的全面验证。该成果适用于汽车生产企业、安全产品服务商及检测评估机构，为智能网联汽车网络安全测试、评估与管理提供标准化技术支撑，有效提升车辆抵御网络攻击的能力。

关键字：智能网联汽车；网络安全；检测技术；车端安全；总线安全；无线通信安全

一、引言

随着汽车智能化、网联化水平的快速提升，车端总线、无线通信、主机系统等与外部环境的交互日益频繁，网络安全风险持续凸显。恶意攻击可能导致车辆控制异常、数据泄露等严重安全事件，威胁驾乘人员生命财产安全。目前，智能网联汽车网络安全检测缺乏统一的技术规范，检测项目、方法和要求存在差异，影响检测结果的一致性和权威性。

基于此，中国网络空间安全协会与武汉市网络安全协会联合牵头，组织汽车制造企业、网络安全技术公司、科研院校等多方力量，制定本智能网联汽车网络安全检测技术要求。本规范依据 GB 44495-2024《汽车整车信息安全技术要求》、GB/T 40861-2021《汽车信息安全通用技术要求》等国家标准，明确检测范围、技术指标和实施流程，为行业提供统一的检测依据，推动智能网联汽车网络安全水平提升。

二、检测范围与基础规范

（一）适用范围

本技术要求规定了汽车车端网络与车端联网零部件系统的网络安全检验项目、方法和要求，适用于汽车生产企业、汽车网络安全产品及服务提供商，以及汽车网络安全检测评估机构开展相关测试、评估和管理工作。

（二）规范性引用文件与术语定义

本规范引用 GB 44495-2024《汽车整车信息安全技术要求》、GB/T 25069《信息安全技术 术语》、GB 38900-2020《机动车安全技术检验项目和方法》、GB/T 40861-2021《汽车信息安全通用技术要求》等文件，其中注日期引用文件的对应版本适用，不注日期引用文件的最新版本（含修改单）适用。

术语和定义采用 GB/T 25069、GB 38900 和 GB/T 40861 界定的内容，核心缩略语包括 CAN（控制器局域网络）、CANFD（可变缩率的控制器局域网络）、ETC（电子不停车收费）、GNSS（全球导航卫星系统）、NFC（近距离无线通讯技术）、RFID（射频识别）、WLAN（无线局域网）等。

三、核心检测要求与实施方法

（一）车端总线网络安全检测

车端总线网络安全检测包括 CAN/CANFD 总线和车载以太网总线两大模块，聚焦数据安全属性验证与攻击防护能力检测。

1. CAN/CANFD 总线安全检测

检测需采用数据真实性、保密性、完整性等安全检测技术，支持总线模糊检测、泛洪攻击检测和 UDS 检测。模糊检测需配置报文类型、格式、发送间隔等参数，对报文 ID、DLC 及 payload 进行模糊测试；泛洪攻击检测需设定发送频率、负载率等策略，验证系统抗攻击稳定性；UDS 检测涵盖探测功能、诊断协议检测及漏洞扫描。

检测方法包括接入伪造外围设备验证识别能力、检查协议版本合规性、模拟注入攻击、欺骗攻击等，通过 OBD-II 接口发送测试消息，监测系统日志记录与报警响应。

2. 车载以太网总线安全检测

需验证数据可用性（丢包率、时延）和完整性（校验和、错误计数），检测 MAC 地址过滤、802.1X 认证等专用网络认证机制，以及通信名单过滤、网络分域等安全管理策略。检测通过抓取 SOME/IP、DoIP 业务报文进行协议分析，注入异常报文验证告警机制，模拟泛洪攻击测试业务连续性，解析报文结构确认加密处理情况。

（二）车端无线网络安全检测

车端无线网络安全检测覆盖蓝牙、WLAN、NFC、GNSS 及蜂窝网络，重点检测设备真实性验证、数据加密、访问控制等能力。

1. 蓝牙与 WLAN 网络安全检测

蓝牙网络需检测 ETC/RFID 设备真实性、协议版本合规性、安全审计功能及程序可信验证机制，通过接入伪造设备、模拟近场通信、篡改通信程序等方式验证防护能力。WLAN 网络需检查自动连接关闭功能，验证伪造设备识别、审计日志记录及程序启动安全性。

2. NFC 与 GNSS 网络安全检测

NFC 网络需检测 RFID 设备真实性、协议版本、非授权接入阻止及数据篡改识别能力，通过接入伪造设备、注入恶意代码等方式测试系统响应。GNSS 网络需验证数据完整性校验、加密传输、入侵检测及安全审计功能，采用渗透测试模拟攻击，监测系统攻击识别与报警能力。

3. 车载蜂窝网络安全检测

检测车辆手动开关蜂窝网络连接功能，验证通信数据的完整性保护、加密传输、身份认证及防重放机制，测试入侵检测与安全审计能力。通过抓取并修改通信报文、重放请求报文、模拟远程攻击等方式，评估系统防护有效性。

（三）车端主机网络安全检测

车端主机网络安全检测包括固件安全、接口安全及漏洞扫描三大内容。

1. 固件安全检测

固件需支持启动自检机制，采用安全散列算法验证完整性，对固件签名进行有效性校验，基于硬件可

信根实现安全启动，确保密钥安全存储。检测通过采用非完整、非真实固件，修改可信根及密钥存储方式，验证检测工具对异常情况的识别与记录能力。

2. 接口安全检测

针对 USB、OBD 及传感器接口，检测主动免疫恶意代码、阻止非授权设备接入的能力，验证安全审计功能。通过接入带病毒的 USB 设备、非授权 OBD 及传感器设备，模拟接触式访问，检查系统阻断响应与日志记录情况，篡改访问程序测试可信验证机制。

3. 漏洞扫描要求

采用漏洞扫描技术，检测固件、操作系统及应用软件是否存在国家权威漏洞平台（CNVD、CNNVD）公开发布 6 个月及以上未处置的高中危漏洞，并生成检测报告。

四、结论

本智能网联汽车网络安全检测技术要求构建了覆盖车端总线、无线、主机的全维度检测体系，明确了各模块的安全指标、检测内容及实施方法，为行业提供了统一、规范的检测依据。该技术要求通过标准化的检测流程与方法，能够全面验证智能网联汽车抵御模糊攻击、泛洪攻击、非授权接入等网络威胁的能力，保障车端数据安全与运行稳定性。

后续可结合智能网联汽车技术发展，持续更新检测指标与方法，纳入 5G-V2X 通信安全、自动驾驶系统安全等新兴领域检测内容，进一步完善检测体系。本规范的实施将推动汽车生产企业加强网络安全设计，促进网络安全产品创新，提升行业整体网络安全防护水平，为智能网联汽车产业健康发展提供安全保障。

参考文献

[1] GB 44495-2024，汽车整车信息安全技术要求 [S]

[2] GB/T 25069-2017，信息安全技术 术语 [S]

[3] GB 38900-2020，机动车安全技术检验项目和方法 [S]

[4] GB/T 40861-2021，汽车信息安全通用技术要求 [S]

[5] DB4403/T 355-2021，智能网联汽车整车信息安全技术要求 [S]

[6] GA/T 681-2018，信息安全技术 网关安全技术要求 [S]

[7] GB/T 35273-2020，信息安全技术 个人信息安全规范 [S]

[8] GB/T 37092-2018，信息安全技术 密码模块安全要求 [S]

[9] GM/T 0008-2012，安全芯片密码检测准则 [S]

[10] YD/T 3746-2020，车联网信息服务用户个人信息保护要求 [S]

起草单位

湖北天融信网络安全技术有限公司、国家计算机网络应急技术处理协调中心（CNCERT）、国家计算机网络应急技术处理协调中心（CNCERT）湖北分中心、武汉市公安局交通管理局、东风汽车集团有限公司研发总院、岚图汽车科技有限公司、东风悦享科技有限公司、东风商用车有限公司、武汉达安科技有限公司、东风汽车集团股份有限公司猛士汽车科技公司、中移（上海）信息通信科技有限公司、武汉大学国家网络安全学院、华中科技大学网络空间安全学院、武汉理工大学计算机与人工智能学院、湖北大学网络空间安全学院、华中师范大学计算机学院、湖北汽车工业学院汽车工程师学院、湖北省电子信息产品质量监督检验院、武汉安域信息安全技术有限公司、开源网安物联网技术（武汉）有限公司、广电计量检测（武汉）有限公司、宝牧科技（天津）有限公司武汉分公司。

基于关键表征和无关表征解耦的人脸识别反欺诈方法

■ 张帆[1], 古天龙[2], 刘小丽[2], 郝峰锐[1], 罗良逸[1], 孙平[1]
(1. 武汉轻工大学数学与计算机学院 , 湖北 武汉 430002；)
(2. 暨南大学网络空间安全学院 , 广东 广州 511443)

摘要：随着人脸识别技术的广泛应用，人脸识别反欺诈（Face Anti-Spoofing, FAS）成为保障系统安全的重要一环。然而，现有的 FAS 方法在应对各种攻击方式时，往往面临两大挑战：准确性下降以及缺乏可解释性的“黑箱”问题。针对上述问题，本文提出了一种“双自编码器解耦框架”（Twin Autoencoder Disentanglement, TAD），该框架通过将“对人脸真假识别起关键作用的关键表征（Critical Representation，CR）”与“对人脸真实识别起干扰作用的无关表征（Irrelevant Representation, IR）”进行分离，不仅显著提升了防欺骗系统的准确性与鲁棒性，而且大大增强了模型的可解释性。实验结果表明，TAD 在多个公开数据集上均表现出了优异的性能，尤其在复杂环境下，具有更强的适应能力。特别地，TAD 能够以可视化的方式，给出对目标图像做出真假判定的可审计、可追踪的“解释”。

关键字：人脸识别反欺骗；表征解耦；可解释性；双自编码器

一、引言

随着人脸识别技术的普及，其安全挑战日益增加，尤其是通过照片、视频或 3D 面具等手段进行的欺骗攻击，给人脸识别系统的安全性带来了严峻考验。尽管现有的 FAS 技术在提升识别准确性方面取得了一定进展，但在新型攻击手段的应对能力以及模型的可解释性方面，依然存在诸多不足。如何在提升检测准确性的同时增强模型的可解释性，成为当前防欺骗领域亟待解决的关键问题。

本文提出了“双自编码器解耦框架”TAD[1]。TAD 的目标在于将人脸图像中深度纠缠在一起“关键表征 CR”和“无关表征 IR”进行显式地分离，并利用分离得到的 CR 进行真假人脸判定；同时，TAD 能够将 CR 以热力图、深度图等图形化的方式进行展示，给出（人眼和机器）可识别的模型“可解释性”判定原因。实验表明，TAD 不仅有效提升了 FAS 的准确性和鲁棒性，而且能够清晰地展示模型的决策依据。

二、方法与创新

2.1 双自编码器解耦框架 TAD

与传统方法仅使用单一编码器提取图像特征的做法不同，TAD 引入了两个自编码器结构，其中一个负责提取与“活体 vs 伪造”相关的 CR，另一个专注提取与“身份、背景”等相关的 IR。这种设计能够将通常深度纠缠在一起 CR 和 IR 分别解耦到不同的空间，避免了 IR 对 CR 的干扰。

2.2 多分支监督 MSA

为了进一步优化模型性能，TAD 引入了多分支监督（Multi-branch Supervision, MSA）策略。MSA 通过施加深度图和纹理信息的辅助监督，进一步抑制 CR 中的残留 IR。这一设计使得模型能够更敏感地捕捉伪造图像中的细节特征，例如深度异常或者纹理异常，提升了 FAS 的准确性和鲁棒性。

2.3 可解释性的提升

传统的深度学习方法常被视为“黑箱”，因为缺乏足够的可解释性，用户和开发者难以理解模型的判断依据。而 TAD 通过解耦 CR，使得我们可以清晰地观察到每个分支的重构结果，从而揭示模型的决策过程。具体而言，当模型判定某张图像为伪造时，我们可以通过深度图、热力图等图形，以（人眼和机器）“可视化”的方式获知模型关注的伪造痕迹，如屏幕反射、纸张纹理、电子屏摩尔纹、深度异常等，这大大增强了模型的透明度。这种透明度带来的“可解释性、可审计性和可信性”等，是目前全球关注的热点 [2-3]。

三、与现有方法的对比

传统的 FAS 方法多依赖于单一编码器进行特征提取，然而，面对多变的伪造攻击方式，尤其是在跨攻击类型或跨域的场景下，已有的方法往往会遭遇特征纠缠以及由此而导致的准确性下降问题。作为对比，本文不仅针对性地提出了 CR 和 IR 的解耦方法，而且能够以 CR 为基础，通过可视化的方式直观地展示模型的判断依据。因此，在应对更为复杂的跨攻击类型（cross-attack）或跨域（cross-domain）数据时，TAD 展现了比传统方法更好的鲁棒性和可解释性。

与已有的最前沿工作相比（State-of-the-art，SOTA），本文并不旨在取代 SOTA 工作，而是探索新方法的可能性。例如，Chen 等明确指出，我们的解纠缠方案可以与他们工作形成互补 [4]。2025 年最新的 FaceShield[5] 采用了多模态大语言模型，通过自然语言生成的方式进行可解释性增强，与之相比，TAD 通过图像可视化展示了伪造痕迹的具体位置，二者可通过多模态对齐进行融合，在可解释性方面具有模态互补性。

四、未来方向与挑战

尽管 TAD 在多个数据集上展示了良好的性能，但仍存在一定的挑战和改进空间。首先，TAD 在训练过程中依赖于深度图或伪造线索等标签，这可能在某些实际应用中无法获得。未来的研究可以探索弱监督、自监督或无监督的解耦方法。其次，随着伪造攻击手段的不断演化，例如高仿真 3D 面具、生成式图像 / 视频、深度伪造等，TAD 需要扩展关键特征空间，加入更多的攻击模式，TAD 对此具备良好的可扩展性。最后，结合 TAD 的图像可视化输出与自然语言生成技术，将使得模型不仅能“看到”伪造特征，还能通过语言“说明”其判断依据，从而进一步提升系统的透明度、可信性和可用性。

参考文献

[1] S. Zhao, W. Chen, F. Zhang, et al. Disentangle irrelevant and critical representations for face anti-spoofing[J]. Neurocomputing, 2023, 536: 175-190

[2] The European Parliament and the Council. EU AI Act[EB/OL]. 2024-06-13. https://artificialintelligenceact.eu/

[3] 科技部 .《新一代人工智能伦理规范》发布 [EB/OL]. 2021-09-26. https://www.most.gov.cn/kjbgz/202109/t20210926_177063.html

[4] C. Chen, X. Li, B. Chen, et al. A distortion model guided adversarial surrogate for recaptured document detection[J]. Pattern Recognition (PR’24). 2024, (151): 110433

[5] H. Wang, Y. Shi, Z. Tao, et al. FaceShield: Explainable Face Anti-Spoofing with Multimodal Large Language Models[EB/OL]. 2025-111-15. https://arxiv.org/html/2505.09415v2

深度对抗技术在线上金融业务安全防护中的应用研究

■ 张雯[1] 陈思琪[1] 彭进[1] 白建武[1]
(1. 武汉众邦银行股份有限公司（金融科技管理部） 湖北 武汉 432200;)

摘要：本研究探讨数字化金融业务面临的安全风险困境，旨在构建安全可信数字银行，通过五位一体建设策略，落地企业级安全深度对抗平台系统群的建设，形成“知己知彼、深度对抗、精准处置”的方法论。构建“金融服务 +”体系，赋能全行业务创新，提升安全防控能力，实现安全与体验的动态平衡。

关键字：安全可信；深度对抗；精准处置；动态平衡

1. 引言

随着金融业务与互联网的深度融合，线上金融业务风险问题愈发凸显，已经成为制约金融业可持续发展的首要因素。一方面，随着业务种类不断丰富，业务安全风险呈现多样性态势，数字化程度越高，风险随之增大；另一方面，黑灰产组织利用先进技术，不断升级作案手法，呈现出产业化、精准化、移动化、技术化的特点。诸如虚假借贷、盗刷盗转、营销薅羊毛、APT 攻击等风险层出不穷，给金融机构和客户带来较大的安全威胁，已经成为制约金融行业可持续发展的首要挑战。

2. 线上业务风险防控的探索和实践

2.1 线上业务风险防控方法论

在当前 AI 技术飞速发展的背景下，生成式人工智能 (AIGC) 技术滥用与欺诈事件频发，智能化攻击愈发猖獗，众邦银行积累了一套深度对抗方法论，可有效应对和防范黑灰产威胁。一是知己知彼：“未知攻，焉知防”，知己知彼是安全对抗之根本，基于对自身业务风险的认识，深入研究黑灰产业链、工具手段及工具资源，从根本上认识攻击方，运用最合适的工具和方法应对攻击。二是深度对抗：“数据驱动，技术防控”，通过构建多层次的阶梯式对抗手段，深度挖掘黑灰产组织，实现有效对抗。三是精准处置：“动态防治，执中而行”，通过业务与科技的融合，实现动态决策、可信识别和精准处置。

2.2 线上业务风险防控体系

为构建安全可信数智银行，通过“五位一体”的建设策略，落地企业级线上业务风险防控平台系统群。一是战略驱动，秉持“数字化 + 智能化 + 可信”的理念，积极开展数字化建设，探索新模式、应用新技术、落地新场景；二是优化组织架构，由党委领导协调各部门协同合作，实现管理、流程、能力和数 据体系的统一；三是打通链路，赋能全行业务，打通全客户、全场景、全渠道、全流程和全业务，形成事前风险探测、事中风险防范和事后风险分析与管理的全生命周期风险运营闭环；四是运用数字科技，以数字化治理为切入点，坚持制度统一、流程统一、数据统一的数字化治理建设，

将数字科技融入产业金融，借助平台积累高质量的产业数据，提升精准风险防控和对抗能力；五是队伍建设，组建专业化线上业务风险防控队伍，积极响应并处置线上业务风险事件，同时加强安全宣教，打造全方位、渗透式、立体化的安全宣教服务，不断提升人员风险防控意识与技术防治能力。

2.3 线上业务风险防控平台

以深度对抗为导向，构建金融线上业务风险防控平台，沉淀黑灰产对抗技术和数据；同时，通过内外部多方协同、联防联控，不断迭代组合，优化安全对抗运营水平。系统架构图如图 1 所示。

图 1 线上金融业务安全深度对抗平台系统架构图

3. 线上金融业务安全的应用

3.1 应用情况

本平台作为业务安全对抗基础平台，对外连接包括直销 APP、微信小程序、开放平台等互联网生态圈，为 8000 余万用户提供安全保障服务；对接 14 个行内交易系统，覆盖 48 个业务场景，152 条规则的定制化部署。

3.2 落地效果

本平台有效实现了金融领域用户身份识别、风险防治、动态防御、跨机构合作、舒适体验与敏捷高效。

3.2.1“千人千面”，精准处置

通过智能多维度验证，根据不同风险等级匹配相应的验证强度，保障合法用户操作无感知，在屏蔽风险的同时，提供友好且高强度的智能验证。

3.2.2 可信体系，动态平衡

运用可信风险模型，采集可信环境、身份、行为等数据建立核身体系，结合业务系统数据形成可信数据模型，打造风险和体验相平衡的动态防控模式，根据不同情况动态调整防控措施，对于中低风险业务采取柔性策略，对于高风险业务则终止支付。

3.2.3 梯度防御，深度对抗

基于信任平台建模的威胁处置细粒度防护，提供多种智能对抗手段以保障用户账户安全。

3.2.4 安全融合，体系统一

本研究将基础安全和业务安全体系进行深度整合，实现了管理流程的统一；整合安全能力，协同互补，强化防御；统一数据，打破孤岛，确保数据准确完整，为决策提供支持，构建强大的协同安全体系，保障金融业务的顺利开展。

4. 结语

本研究围绕网络安全防护与业务风险防控的深度融合展开，借助于基于 BOT 的动态对抗、智能风险决策和安全自适应，为企业的数字化转型提供强大的安全保障。未来，在数字化转型与 AI 技术不断深化和发展的背景下，线上金融业务风险防御会更加智能化、自动化和协同化。

参考文献

[1] 曹越 .AI 换脸技术产生的危害与应对措施 [J]. 南海法学 ,2020(04)

[2] 吕培霖 , 张文韬 .AI 电信网络诈骗犯罪治理研究 [J]. 福建警察学院学报 ,2024,38(01):23-31.

[3] 李洋 , 唐秀江 , 陈春璐 , 等 . 金融行业“金融安全 3.0”理论与生态 [J]. 信息技术与网络安全 ,2018,37(07):6-8+21.DOI:10.19358/j.issn.2096-5133.2018.07.002.

[4] 刘瑞霞 . 打造基于大数据的智能化风控体系 [J]. 金融电子化 ,2018,(08):57-58+6.

[5] 章明 , 刘培 . 基于大数据的智能风险防控平台设计与实现 [J]. 中国工程科学 ,2020,22

(06):111-120.

基于人工智能的网络安全监测运营平台创新实践

■ 田聪 [1]
(1. 国网武汉供电公司信息通信分公司，湖北 武汉 430010)

关键字：网络安全、人工智能、新型电力系统

引言

电力系统作为国家关键基础设施，其网络安全防护意义重大。新型攻击手段不断涌现，传统的边界防护体系面临严重威胁 [1]。本项目聚焦新型电力系统海量异构设备接入、网络风险边界扩大等问题，打造基于人工智能技术的网络安全监测运营平台。创新电网企业自主可控的网络安全运营垂域模型，集成多源异构设备数据构建智能分析引擎，通过深度学习实现威胁特征自进化，增强网络安全威胁检测能力；基于知识图谱与智能体技术开发自动化编排系统，建立跨品牌设备联动响应机制，实现安全事件处置全流程智能化调度，提升网络安全应急处置效率；创新多模态人机交互平台，降低安全运维技术门槛。

一、研究背景

随着新型电力系统的加快建设，电网接入终端呈现海量异构化特征，网络边界持续扩大，传统以边界防护为核心的静态防御体系已难以应对高级持续性威胁（APT）等新型网络攻击。同时，安全设备品牌繁多、数据标准不一，导致安全数据形成孤岛，告警误报率高，事件响应严重依赖人工研判与跨设备协调，处置效率低下。在此背景下，人工智能技术凭借其在数据融合、智能分析与自动化决策方面的优势，为构建新一代智能化网络安全运营体系提供了关键支撑。

二、现状与挑战

当前，电力企业的网络安全运营普遍面临三大挑战：一是数据融合难，防火墙、入侵检测系统等各类安全设备独立运行 [3]，数据格式异构，难以进行有效的关联分析，大量无效告警淹没了真实威胁。

二是响应协同差，安全事件处置依赖人工在各系统间切换操作，流程割裂，跨品牌设备间缺乏联动机制，导致响应延迟，从发现到处置往往需要数小时。三是技术门槛高，高级威胁的检测与分析需要专家经验，而一线运维人员能力不均，难以快速、精准地应对复杂攻击。

尽管市场上存在部分安全编排与响应（SOAR）产品，但其规则固化、适应性差，缺乏针对电力业务场景的深度定制与智能决策能力，无法满足电网企业对自主可控和高效运营的迫切需求。

三、基于人工智能的网络安全监测运营平台设计

（一）平台整体架构

平台以“一体智能、协同驱动”为核心理念，构建了集数据采集、智能分析、决策编排与自动化响应于一体的技术架构。平台基于多源数据接入层，整合全网安全设备日志与网络流量；通过智能分析引擎，利用机器学习与深度学习模型进行深度关联与威胁挖掘；依托自研的网络安全垂域大模型作为“决策大脑”，驱动知识图谱与多智能体系统，最终实现安全事件的自

动化研判、策略生成与跨设备调度。

（二）智能分析与协同响应机制

为应对新型电力系统中海量异构设备接入导致的传统安全防护体系失效、安全数据孤岛及响应滞后等挑战，本研究设计并实现了基于人工智能的网络安全监测运营平台。该平台通过多源异构设备数据融合分析技术消除误报，通过设备接口逆向与标准化解析，实现对 90% 以上主流安全设备的数据接入。采用融合泛化技术对多元数据进行清洗、归一化与关键特征提取，并利用交叉关联算法进行误报消除，误报消除率超过 40%。

与此同时，本研究构建网络安全运营专用语料库，基于 Llama7b 模型训练并本地化部署网络安全垂域模型。该模型结合涵盖威胁情报、漏洞库与专家经验的知识图谱，实现对安全事件的智能分析与最优响应策略生成。创新性地构建了以网络安全垂域大模型为“智能大脑”，知识图谱 [2] 与多智能体协同响应为核心的技术架构，实现了安全事件的智能决策与自动化编排处置。

（三）安全运营的闭环与监管

平台通过形式语言标准化安全操作指令，构建了跨品牌设备的自动化调度能力。所有安全事件处置流程均被记录上链，实现操作可审计、过程可追溯。同时，平台内置态势感知大屏，为监管人员提供全局风险视图与实时处置进展，显著提升了安全运营的透明度和监管效率。

四、应用成效分析

平台在国网武汉供电公司投入实战化运行以来，取得了显著成效，充分验证了其技术先进性和实用价值。

在事件响应方面，平台实现了跨品牌安全设备的智能联动和自动化处置，彻底改变了传统依赖人工研判和手动操作的低效模式。典型场景中，当系统检测到内网异常渗透或横向移动行为时，能够自动触发预置的响应流程，同步指挥防火墙阻断恶意 IP 地址，并通过终端管理平台对感染主机实施快速隔离，将原本需要多部门协同、耗时数小时的安全事件处置流程压缩至分钟级完成，整体协同效率大幅提升。

在威胁检测方面，平台通过智能分析引擎对单日超过 2000 条的离散告警进行深度关联分析和上下文建模，有效识别传统规则引擎难以发现的 APT 攻击、隐蔽隧道和横向移动等高级威胁，实现威胁检测准确率提升至 95% 以上，大幅降低了误报和漏报风险。

在标准建设与推广方面，项目已总结形成《自动化网络安全运营流程规范》企业标准，系统梳理了智能安全运营的技术要求、处置流程和管理机制，为在省级电力公司及其他能源企业的规模化推广提供了可复制、可落地的完整解决方案，展现出重要的行业示范价值和推广前景。

五、总结与展望

基于人工智能的网络安全监测运营平台，有效解决了电力网络安全运营中的数据孤岛、响应滞后与协同低效难题。通过创新性地融合垂域大模型、知识图谱与多智能体技术，实现了安全运营从“人工驱动”到“智能驱动”的范式转变。

未来，平台将结合大模型技术持续优化决策能力，并逐步向工控场景、物联网边缘侧延伸，构建覆盖“云 - 网 - 边 - 端”的全场景智能化安全防护体系，为新型电力系统的稳定运行提供更坚实的安全保障。

参考文献

[1] 国家电网有限公司 . 新型电力系统网络安全白皮书 [R]. 北京，2022.

[2] 蔡豪 , 王珂 , 吕书林 , 季丰 . 基于知识图谱的网络安全事件检测与响应技术研究 [J]. 数码设计 , 2024(19):39-41.

[3] 张亮 , 屈刚 , 李慧星 , 等 . 智能电网电力监控系统网络安全态势感知平台关键技术研究及应用 [J]. 上海交通大学学报 , 2021(102):103-109.

基于 154N 体系驱动的超算中心纵深防御解决方案

■ 王俊华[1]、许龙舟[1]、胡文强[1]、蒋雨辰[1]
（1. 中金数据（武汉）超算技术有限公司，湖北 武汉 430040）

摘要：针对超算中心网络架构复杂、数据价值高、威胁场景多元的安全挑战，中金数据（武汉）超算技术有限公司研发了“1 套数智基座 + 5 大技术支撑系统 + 4 个专题赋能中心 + N 类行业场景”的 154N 安全防护体系。该体系以零信任动态访问控制为核心，构建“感知 - 防御 - 响应 - 恢复”全闭环防护架构。方案已在该公司运营的中金城市云平台落地，支撑第七届世界军人运动会等重大活动网络保障及武汉市 62 家委办局政务云系统安全运维。2025 年，中金数据（武汉）超算技术有限公司荣获“武汉市网络安全支撑单位”称号。实践表明，方案可将网络攻击拦截率提升至 99.7%，漏洞修复时效缩短 60%，为超算基础设施安全稳定运行提供了高效可靠的技术支撑。

关键词：超算中心；网络安全；纵深防御；协同审计；154N 体系；零信任架构；

一、引言

1.1 研究背景

超算中心作为数字经济核心基础设施，承载着科研数据处理、关键业务运行、大规模算力调度等核心职能，其网络安全直接关系到国家安全、产业升级与城市运行稳定。当前超算中心面临三重核心安全挑战：一是网络架构呈现多层级、跨区域特征，计算节点与存储系统交互频繁，传统单点防护难以覆盖全链路漏洞；二是承载的科研数据、政务数据等敏感信息价值极高，数据泄露与篡改风险隐患突出；三是攻击手段日趋复杂，ransomware、APT 攻击等新型威胁持续演进，对防护体系的动态适配能力提出更高要求。

1.2 研究目标与意义

本研究旨在解决超算中心“防护碎片化、数据难监管、威胁难预判”的行业痛点，构建兼具合规性与创新性的安全防护体系。方案通过融合多方安全计算与纵深防御架构，实现三大目标：一是建立全层级安全防护屏障，覆盖网络边界、计算节点、存储系统等核心环节；二是突破敏感数据协同审计的安全瓶颈，在保障数据隐私的前提下实现合规审计；三是提升安全态势感知与应急响应能力，实现威胁精准识别与快速处置。该成果的推广应用可为超算中心、大数据基地等关键信息基础设施提供可复制的安全解决方案，助力数字经济安全发展。

二、154N 安全体系的核心设计与技术实现

2.1 设计原则

154N 体系设计基于“资源集约化、防护立体化、运营智能化”三大原则。资源集约化核心是打破安全资源“分散部署、重复建设”的传统模式，通过统一规划、弹性调度实现安全能力的最大化利用。防护立体化聚焦“全场景、全链路、全生命周期”的安全防护需求，

通过四层架构的协同联动，形成“边界 - 计算 - 数据 - 管理”的闭环防护链。运营智能化依托大数据、AI 等技术，将四层架构从“被动防御”升级为“主动感知、智能响应”。

2.2 总体架构：四层协同的技术范式

以“数智基座 - 技术支撑 - 专题赋能 - 场景服务”四层逻辑，实现超算安全的全链路覆盖：

1 套数智基座：以“网、安、云、算”整合基础资源，实现网络接入、安全能力、云计算、算力资源的池化调度，是体系的底层支撑。具备跨模块动态编排、安全资源融合、高可用扩展的特点。

5 大技术支撑：通过安全计算环境、区域边界等模块，构建“环境 - 边界 - 网络 - 管理 - 运营”的立体防护技术体系，落地基础安全能力。具备协同防护、动态防御、运营闭环的特点。

4 个专题赋能中心：包含战略支撑、能力建设、运营研究、治理决策四大中心，将技术能力转化为合规适配、攻防研究、智能运营等专题服务。具备战略支撑 - 治理决策联动、运营研究协同、专题服务智能化的特点。

N 个一站式服务场景：输出云安全运营、攻防实战等场景化服务，覆盖政务、企业等不同需求，完成从资源到价值的落地。

整个架构以“资源集约化、防护立体化、运营智能化”为核心，形成“底层资源 - 技术能力 - 专题服务 - 场景输出”的闭环，是超算安全生态的完整落地框架。

三、方案实施效果与验证

3.1 实施场景成效

该方案已在中金数据（武汉）超算技术有限公司（以下简称“中金武汉超算”）运营的中金城市云平台全面部署，中金城市云平台承载国家网络安全人才与创新事业算力服务、武汉市电子政府等核心业务，服务覆盖华中地区科研机构、政府部门与重点企业。方案支撑中金城市云平台于 2023 年通过了湖北省发改委首批数字经济典型应用场景评审，有力促成了中金武汉超算于 2025 年通过武汉市委网信办评审，获评“武汉市网络安全支撑单位”（重点技术领域），成为华中地区超算安全领域的标杆成果。

3.2 测试验证结果

通过为期 6 个月的实际运行与测试，方案核心性能

154N 体系总体架构设计图

指标测试结果与行业平均水平对比结果如下：

指标名称	测试结果	行业平均水平
网络攻击拦截率	99.7%	95.2%
敏感数据审计效率	1000 条 / 秒	650 条 / 秒
漏洞修复平均时效	4 小时	10 小时
安全事件误报率	0.8%	3.5%

方案核心性能指标

3.3 获奖与合规认证

方案通过以下认证与奖项证明其技术先进性与实用性：

1.2025 年获评武汉市委网信办“武汉市网络安全支撑单位”（重点技术领域）；

2.2023 年入选湖北省首批数字经济典型应用场景

3. 支撑中金数谷武汉大数据中心通过 Uptime M&O 管理运维认证；

4. 符合 GB/T 22239-2019《信息安全技术 网络安全等级保护基本要求》；

5. 符合 GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》；

6. 核心技术“基于多方网络安全计算的敏感数据协同审计平台及方法”获国家发明专利（公开号：CN120342576A）。

四、结论

本研究针对超算中心网络架构复杂、数据价值高、威胁场景多元的核心安全挑战，构建了基于 154N 体系驱动的超算中心纵深防御解决方案。该方案以“资源集约化、防护立体化、运营智能化”为设计原则，通过“1 套数智基座 + 5 大技术支撑 + 4 个专题赋能中心 + N 类行业场景”的四层架构，实现了从基础资源到场景服务的全链路安全覆盖。

未来，方案将进一步融合 AI 与大数据分析技术，提升威胁预判与自适应防护能力；探索量子加密与多方安全计算的深度结合，应对量子计算带来的安全挑战，持续为数字经济高质量发展筑牢安全底座。

参考文献

[1] 国家知识产权局。一种基于多方网络安全计算的敏感数据协同审计平台及方法 [P]. CN120342576A, 2025-05-10.

[2] Cao P, Kalbarczyk Z, Iyer R K. Security Testbed for Preempting Attacks against Supercomputing Infrastructure[J]. IEEE Transactions on Dependable and Secure Computing, 2024, 21(3): 1024-1037.

[3] 武汉市网络安全协会。武汉市委网信办关于第三届武汉市网络安全支撑单位拟入选单位的公示 [EB/OL]. 2025-03-15.https://www.whcsa.org.cn/portal/article/index/id/737/cid/18.html.

[4] 湖北省发展和改革委员会。关于湖北省首批数字经济典型应用场景的公示 [EB/OL]. 2023-07-06. https://fgw.hubei.gov.cn/fbjd/zc/zcwj/gs/202307/t20230706_4735990.shtml.

[5] 国家市场监督管理总局，国家标准化管理委员会 . GB/T 22239-2019 信息安全技术 网络安全等级保护基本要求 [S]. 北京：中国标准出版社，2019.

[6] 国家市场监督管理总局，国家标准化管理委员会 . GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求 [S]. 北京：中国标准出版社，2021.

“透视”加密黑盒：基于 AI 自学习的加密流量威胁检测实践

■ 甘孝龙 [1]
（1. 北京神州绿盟科技有限公司）

摘要：随着 TLS/SSL 等加密协议的广泛部署，网络空间安全面临“流量加密化”带来的严峻挑战，传统基于深度包检测（DPI）与特征匹配的安全手段在加密流量面前逐渐失效，形成“加密黑盒”盲区。本文针对该问题，系统阐述了一项名为“透视加密黑盒”的创新性解决方案。该方案设计并实现了一套基于人工智能自学习引擎的加密流量威胁检测系统。系统采用多模型融合检测架构，从协议握手时空特征、证书元数据、会话行为序列及背景流量关联等多个维度进行协同分析，创新性地引入“限定域指纹”技术以实现同源攻击追踪与恶意家族聚类。通过“鱼骨图”可视化研判界面与基于增量学习的自适应优化机制，系统在保障用户数据隐私（无需解密）的前提下，显著提升了对高级持续性威胁（APT）、隐蔽隧道、恶意软件通信等加密威胁的检出率与识别精度。实践表明，该系统在运营商、金融等行业关键网络节点部署后，有效弥补了传统安全设备的检测盲区，提升了整体安全运维效率与合规管控能力。

关键词：加密流量分析；人工智能；威胁检测；不解密检测；自学习；网络安全

1. 引言

当前，互联网流量加密化已成不可逆转的趋势，加密协议在保障数据机密性与完整性的同时，也为网络攻击提供了天然的隐蔽屏障。攻击者广泛利用 TLS/SSL 等加密通道传输恶意载荷、建立命令与控制（C2）通信，使得传统依赖明文内容检测的安全设备，如入侵检测系统（IDS）、下一代防火墙（NGFW）等，效能大打折扣。因此，如何在不解密、不侵犯用户隐私的前提下，实现对加密流量的有效威胁检测，成为业界共同关注的核心难题。

现有的加密流量分析方法主要围绕流量元数据统计、握手报文特征、证书信息以及基于机器学习的分类模型展开，但仍普遍存在对未知威胁及变种识别能力不足、误报率高、可解释性差、跨环境适应性弱等问题。针对上述挑战，研究团队设计并研发了“加密流量分析系统”，旨在通过创新的 AI 自学习与多维度特征融合技术，“透视”加密流量的内部威胁，实现高效、精准、可解释的加密威胁检测。

2. 相关研究

加密流量分析技术大致可分为三类：基于统计特征的方法、基于深度学习的方法以及基于行为指纹的方法。早期研究侧重于利用包长、到达时间间隔、流持续时间等统计特征进行应用识别或异常检测。随着深度学习发展，CNN、LSTM 等模型被用于从原始字节序列或会话流中自动学习特征，提升了分类性能。此外，基于 TLS/SSL 握手阶段特定字段（如密码套件、扩展列表）生成指纹，用于恶意软件家族识别或追踪的研究也取得进展。然而，单一方法往往存在局限性：统计特征易受网络环境干扰；深度学习模型可解释性差且需要大量标注数据；静态指纹易被攻击者通过细微修改规避。

本文提出的系统综合了上述方法的优势，构建了一个多模型融合、具备自进化能力的检测框架，并在指纹技术、可视化分析等方面进行了针对性创新。

3. 系统设计与关键技术

3.1 总体架构

系统采用旁路部署模式，通过镜像方式采集网络中的加密流量。核心处理引擎包括流量解析层、特征提取层、多模型检测层、威胁研判层以及自学习优化层。系统支持对 TLS、HTTPS、DNS over HTTPS/TLS 等主流加密协议进行深度解析，提取多层次特征，在不触及应用层明文的前提下完成威胁判定。

3.2 多模型融合检测机制

为克服单一模型的局限性，系统构建了协同工作的多 AI 子模型集群：

时空特征模型：分析握手阶段的报文时序、交互轮次、特定标志位出现顺序等，识别异常或非标准的协议行为。

证书元数据模型：对服务器证书的颁发者、有效期、主题域名等信息进行信誉评估与异常模式发现，检测伪造证书或滥用。

会话行为序列模型：利用循环神经网络（RNN）分析加密会话建立后的数据包长度序列、传输方向模式，识别 C2 心跳、数据外传等可疑行为。

背景流量关联模型：结合同一源 / 目的 IP 的历史行为、端口使用情况、关联域名情报等进行上下文分析，提升检出置信度。

各模型输出经集成学习算法（如加权投票或 stacking）进行融合，最终得出综合威胁评分，显著提升了检测准确率并降低了误报。

3.3“ 限定域指纹”技术

该技术不仅提取 TLS Client Hello/Server Hello 中的静态字段，更聚焦于特定威胁家族或攻击工具在协议实现上遗留的、具有高度区分性的细微特征组合（如特定扩展排列顺序、非常规值域），生成高精度指纹。该方法增强了同源攻击活动的关联追溯能力，并能对未知样本进行有效的家族聚类，辅助威胁情报拓展。

3.4“ 鱼骨图”可视化与可解释性

为解决 AI 模型“黑盒”问题，系统设计了独创的“鱼骨图”可视化研判界面。该界面将一次加密会话的核心路径（如 TCP 连接、TLS 握手、应用数据）作为“主骨”，将多模型检测出的各项异常特征点（如可疑证书、异常时序、匹配的限定域指纹）及其置信度作为“鱼刺”标注于相应阶段。分析人员可直观理解触发告警的依据，极大提升了威胁调查与响应的效率。

3.5 基于增量学习的自适应优化

系统内置在线学习模块，支持基于增量学习算法对检测模型进行持续优化。利用经过分析师确认的现网流量数据（包括误报和漏报样本），系统能够自动调整模型参数，适应不断变化的网络环境和新兴威胁手法，实现检测能力的自我迭代与进化。

4. 总结

本文详细介绍了“透视加密黑盒：基于 AI 自学习的加密流量威胁检测”这一创新成果。该系统通过多模型 AI 融合检测、限定域指纹、鱼骨图可视化研判及增量自学习等关键技术，成功实现了在不解密前提下对加密流量中高级威胁的高精度、高可解释性检测。实际部署应用表明，该系统能够有效应对当前网络空间加密化带来的安全挑战，弥补传统安全防护体系的短板，为关键信息基础设施的加密安全防护提供了可靠的技术支撑。未来工作将继续聚焦于应对新型加密协议、增强模型鲁棒性以及提升超大规模网络环境下的应用效能。

参考文献

1. 一文读懂经典深度学习模型—CNN、RNN、LSTM、Transformer、ViT https://blog.csdn.net/qq_70350287/article/details/147287730

2. TLS 指纹识别与 JA3 和 JA3S https://zhuanlan.zhihu.com/p/658722158

3. AI 研习丨面向复杂大数据的自适应学习研究 https://mp.weixin.qq.com/s?__biz=MjM5ODIwNjEzNQ==&mid=2649886709&idx=2&sn=cc51658ba558da4d219cd7961a52fa9e&chksm=bec8e02d89bf693b3f014dd64002ea9d7adad84ec11af64aa308943515e24b63e94c055495cd&scene=27

4. TLS 指纹识别技术深度解析与反检测技术实战指南 https://blog.csdn.net/qq_33253945/article/details/152177931

政务网络安全运营—数智护航江汉政务：AI+ 一体化网络安全运营体系建设

■ 杨鹏[1]、全宏磊[1]、刘硕[1]
（1. 联通（湖北）产业互联网有限公司，湖北 武汉 430024）

摘要：本文以武汉市江汉区为例，探索区县级数字政府政务网络安全运营体系建设路径。通过融合大模型与“平台 + 组件 + 服务”模式，构建“五个一”架构，实现全域资产的集中监测、智能研判与快速响应，显著提升安全防御能力与运营效率，为区县级数字政府政务网络安全提供可复制的运营实践范式。

关键词：数字政府、政务网络、安全运营体系、安全运营平台、大模型

一、引言

党的二十大将统筹发展和安全提升至国家战略新高度，强调以新安全格局保障新发展格局，网络安全成为网络强国建设的核心支撑。在此背景下，武汉市“十四五”规划全面推进新型智慧城市建设，着力构建全域网络与数据安全态势感知体系。区县级数字政府政务网络承载大量民生服务与公共数据，其安全水平关乎整体数字生态的稳定。因此，构建区县级数字政府政务网络安全运营体系，既是落实国家战略的必然要求，也是夯实智慧城市安全底座的关键举措。本文以武汉市江汉区为例，系统阐述在网络安全大模型赋能下，依托“平台 + 组件 + 服务”融合架构开展政务安全运营的实践路径与创新机制。

二、安全运营痛点

3.1 管理上缺乏整体性

区政务网络各接入单位多以“属地自治”模式独立开展安全建设，缺乏统一的顶层设计与跨部门联动机制，导致顶层设计缺失和跨部门联动不足，安全策略难以统一执行。

3.2 运营上缺乏有效性

各接入单位普遍面临资产台账不清晰、更新滞后的问题，导致安全防护存在盲区。同时，“重采购、轻运维”的现象普遍存在，缺乏常态化的监测、策略调优与效能评估机制，使得设备利用率低下、告警处置滞后。面对高级持续性威胁或大规模攻击时，因缺乏统一响应流程与应急联动能力，极易从局部失守演变为系统瘫痪。

3.3 技术上缺乏系统性

各接入单位根据自身需求独立规划安全防御体系，缺乏全区统一的技术标准与集成框架，感知、预警、处置、溯源环节缺乏闭环联动机制，无法实现威胁情报共享与协同阻断，形成典型的“木桶效应”，整体防护效能受限于最薄弱环节。

3.4 人员缺乏安全意识

基层政务工作人员网络安全风险意识淡薄，缺乏

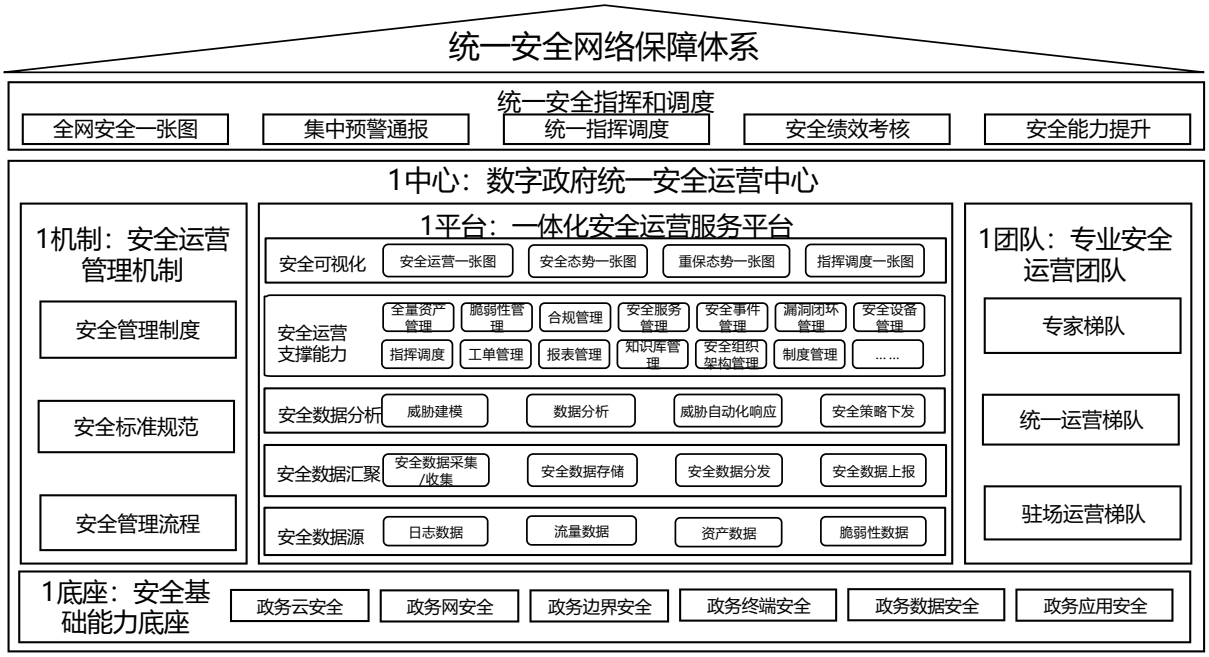


图 1 政务网络安全运营管理体系框架

系统的网络安全培训，常见弱口令设置、开放高危共享目录、离岗未锁屏或关机、违规使用移动存储介质等行为，为钓鱼攻击、勒索软件、数据泄露等事件埋下隐患。因此，需通过制度约束、技术管控与常态化培训相结合的方式提升人员安全意识。

四、安全运营体系

4.1 建设逻辑：“平台 + 组件 + 服务”提供安全管控能力

本文提出“平台 + 组件 + 服务”融合架构，系统整合安全资源，构建覆盖江汉区全域的网络安全保障体系。该架构以“五个一”为核心要素，推进数字政府统一安全运营体系建设，为全区数百个接入单位提供全业务场景的一体化安全运营服务，如图 1 所示。

“1 中心”即区数字政府统一安全运营中心，作为决策中枢与指挥大脑，实现网络安全态势集中感知、统一调度与应急响应；“1 底座”涵盖政务云、网、边界、终端、数据及应用安全六大维度，构建纵深防御的安全技术基座；“1 平台”集成安全可视化、工单管理、威胁情报和自动化编排等功能，提供标准化技术支撑；“1 机制”建立从制度设计到执行监督的闭环管理体系，确保运营规范化；“1 团队”由云端专家、驻场运营团队组成，形成常态化、重点时期的保障体系。该架构实现了安全能力集约化供给、标准化配置与常态化运营，打通了“监测—预警—处置—反馈—优化”的安全闭环，提升了主动防御能力和治理效能，提供了可复制、可推广的实践范式。

4.2 建设思路：建立“四位一体”安全运营新模式

构建“体系化、实战化、常态化”的统一安全运营体系，依托“安全建设 + 运营 + 监管 + 执法”四位一体协同机制和“能力融通、信息互通”底座，推动区政务网络安全实现“内部横到边、外部纵到底”的联防联动，如图 2 所示。

横向层面，区政务网络安全运营中心打通数据共享与通报反馈通道，实现与网信办、公安等跨部门高效协同；纵向层面，联动各接入单位，建立协作机制，贯通安全数据汇聚、风险通报、处置建议与能力共享。该体系整合资源、强化闭环，全面提升主动防御与应急响应能力，为区域数字化转型提供坚实安全保障。

图 2“四位一体”安全运营新模式联防联动示意图

4.3 AI 赋能：湖北省内首个融合人工智能 + 安全运营范式

以 AI 赋能安全运营为契机，统筹推进算力平台建设与大模型部署，推动人工智能与网络安全运营深度融合，体系架构如图 3 所示。

依托本地算力基础设施，构建面向政务安全运营场景的 AI+ 安全智能体。在模型基座层，融合网络安全专用大模型、DeepSeek 通用模型及开源模型，通过“选—改—用”闭环机制，实现大模型全生命周期管理，覆盖评估、优选、调优与部署等环节。集成知识库管理、智能体创建、模型仓库、自动化工作流与 API 服务，形成智能化运营支撑体系。以此为基础，构建多模态、可扩展的模型生态，支撑安全问答、单位画像、报告生成、告警研判等典型应用。该模式实现 AI 能力“一点突破、多面辐射”，助力构建自主可控的新一代安全运营体系。

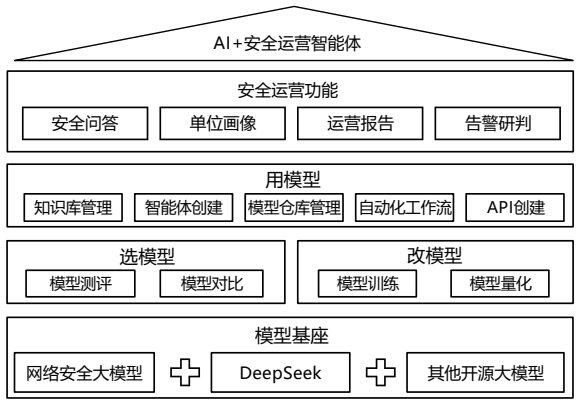


图 3 AI 赋能安全运营体系架构图

五、结论

本安全运营体系在江汉区实践表明，以“五个一”架构为核心、融合大模型技术的一体化安全运营模式，能有效应对区县级数字政府政务网络安全挑战。该体系整合平台、机制与专业力量，推动安全防护由分散向协同、被动向主动、人工依赖向智能驱动转变，显著提升治理水平。其设计契合数字政府安全需求，为同类地区提供了可落地、可持续、可推广的范式。未来，随着 AI 与安全技术深度融合，该模式有望更广泛赋能基层网络安全治理现代化。

参考文献

[1] 陆利栋 . 政务网络安全运营管理体系实践研究 [J]. 广播电视网络 ,2025,32(07):54-57.DOI:10.16045/j.cnki.catvtec.2025.07.008.

[2] 张滨 . 数字政府安全保障体系研究 [J]. 电信工程技术与标准化 ,2022,35(12):1-7.DOI:10.13992/j.cnki.tetas.2022.12.005.

[3] 柴力 . 数字政府背景下网络安全建设研究 [J]. 信息技术与信息化 ,2022,(11):181-184.

[4] 励范洪 .“五位一体”筑牢绍兴政务信息安全体系 [J]. 信息化建设 ,2022,(09):59-61.

[5] 荣晓燕 , 刘海峰 , 刘国伟 . 政务单位网络安全综合合规及评估 [J]. 网络空间安全 ,2020,11(04):30-34.

[6] 束维国 . 政务应用集约化模式下的信息安全治理 [J]. 网络安全技术与应用 ,2020,(01):141-145.

[7] 徐羽佳 , 胡影 , 上官晓丽 . 我国数据安全标准化情况综述 [J]. 中国信息安全 ,2019,(12):56-59.

武网安协发布推动武汉市“综合安全防护平台”（城市盾、行业盾）建设的倡议书

2025 年 5 月 16 日下午，武汉市网络安全协会通过腾讯会议召开第二届理事会第六次会议。会议上，武汉市网络安全协会理事单位安恒信息提出的《关于构建“综合安全防护平台”（城市盾、行业盾）的建议》提案获通过，秘书处跟进办理。现发出以下倡议：

推动武汉市“综合安全防护平台”（城市盾、行业盾）建设的倡议书

产业龙头企业、供应链链主企业、国资平台企业：

为深入学习习近平总书记关于网络强国的重要思想，贯彻《网络安全法》《数据安全法》《个人信息保护法》《网络数据安全管理条例》等法律法规。在数字经济蓬勃发展的当下，网络和数据安全已成为城市数智化创新发展的核心基石。我市众多中小单位、企业在安全合规建设中面临技术力量薄弱、投入成本高、风险抵御能力不足等现实困境，亟需构建一个普惠便利的安全防护体系。我们郑重发出倡议，呼吁武汉区域产业龙头企业、供应链链主企业、国资平台企业等牵头谋划建设区域性、行业性的＂综合安全防护平台＂（城市盾、行业盾），共同守护我市数字经济发展生态。

一、以“行业盾”为载体，引领安全防护普惠共享

我们倡议，产业龙头企业、供应链链主企业发挥技术与资源优势，牵头建设行业性安全防护服务平台（行业盾）。结合行业特性，提供安全评估、防护措施、应急响应等一站式服务。通过集约化建设，降低中小单位、企业在安全设备采购、人员配备等方面的成本，让更多企业能够以低廉的价格享受专业的安全服务，提升整体安全防护水平。

二、以“城市盾”为支点，护航数据设施多元共治

我们倡议，国资平台企业发挥引领示范作用，构建区域性＂综合安全防护平台＂（城市盾）平台。推动公共数据与企业数据的安全流通，构建安全可信的数字基础设施，为全市数智化应用提供坚实保障。同时，带动社会资本参与，形成多元共治的网络安全防护格局。

构建＂综合安全防护平台＂，是守护中小单位、企业安全合规发展的重要举措，也是我们共同的社会责任。让我们携手共进，以平台建设为抓手，强化全市安全风险管理，为武汉数智化创新发展筑牢安全屏障！

武汉市网络安全协会人工智能专业委员会第一次全体会议召开

6 月 11 日武汉市网络安全协会人工智能专业委员会在武汉人工智能研究院召开第一次全体委员会议。会议由专委会主任彭骏主持，协会领导、特邀嘉宾及全体委员出席。会议旨在贯彻国家网络安全战略，凝聚政、产、学、研、用各方力量，构建人工智能安全生态，为武汉市人工智能产业高质量发展筑牢安全底座。

会议重点围绕三项议程展开：一是委员受聘仪式，明确专委会组织架构，凝聚首批核心力量；二是讨论2025年工作计划，聚焦技术研发与产业协同、标准化建设、应用场景拓展、人才培养、安全治理，推动人工智能安全与应用深度融合；三是修订《关于提升人工智能基础设施内生安全水平行动的倡议书》，集思广益强化社会共识。

授牌仪式由协会张玉萍主任主持，潘宣辰会长为主任委员单位和副主任委员单位授牌并颁发聘书。刘悦恒秘书长为专委会秘书长单位、副秘书长单位及委员单位授牌。随后会议围绕专委会2025年的重点方向进行深入讨论，讨论环节由专委会主任彭骏主持，专委会秘书长史琳波汇报《2025年工作计划（讨论稿）》，并结合人工智能发展趋势，阐述如何在各方向工作中把握机遇、应对挑战。专委会副主任国网武汉供电公司高级工程师顾显俊及各委员代表依次围绕工作计划的针对性、可行性等方面展开讨论。会议形成聚焦五大模块的共识，并以“揭榜挂帅”形式征集落实各项工作的牵头单位。最后，黄鹤实验室技术总监丁勇介绍了倡议书的起草背景和相应文本，湖北天融信网络安全技术有限公司研发中心总经理左世涛等代表依次发表相关修订建议。

潘宣辰会长对所有当选的专委会成员单位及代表们表示祝贺，希望专委会要强化政治引领，筑牢安全根基，积极发挥专委会平台枢纽功能，助力武汉国家新一代人工智能创新发展试验区和国家网络安全人才与创新基地建设，不断推进人工智能与网络安全技术产业的深度融合创新。

第三届软件创新发展大会网络安全论坛在汉启幕 共探 AI 时代网安产业新路径

2025 年 6 月 13 日，以“AI 驱动网络安全革新”为主题的第三届软件创新发展大会网络安全论坛在武汉光谷希尔顿酒店隆重召开。本次论坛由第三届软件创新发展大会组委会主办，武汉临空港经济技术开发区经济和科技创新局、国家网络安全人才与创新基地产业联盟、武汉市网络安全协会、黄鹤网络安全实验室联合承办，汇聚政产学研用各界精英，以“技术研发 - 产业应用 - 生态构建”三位一体的合作模式，共商网络安全产业创新发展大计。

中国工业互联网研究院标准化技术研究所所长薛强、国家工业信息安全发展研究中心软件所所长助理姚珊、武汉大学国家网络安全学院二级教授赵波、武汉市经济和信息化局和武汉市委网信办等行业专家和部门相关负责人，以及奇安信、天融信、安恒信息等网络安全头部企业代表近 200 人出席论坛。

武汉市委网信办副主任黄国东在致辞中指出，人工智能技术在为经济社会发展注入新动能的同时，也带来网络攻击智能化、深度伪造、算法偏见等安全挑战。他强调，武汉正以国家网络安全人才与创新基地为依托，构建网络安全“政产学研用”协同生态链，本次论坛既是 AI 与网络安全的技术碰撞，更是展示武汉“网安赋能数字经济”成果的重要窗口。

论坛主题演讲环节围绕人工智能与网络安全深度融合展开：

中国工业互联网研究院标准化技术研究所所长、高级工程师薛强以《大模型安全》为题，从新型工业化视角剖析 AI 作为经济增长新引擎的作用，强调大模型安全与新型工业化融合的战略意义，为产业发展指明方向。

国家工业信息安全发展研究中心软件所所长助理、正高级工程师姚珊在《AI 与软件安全》中，聚焦 AI 编程工具漏洞、大模型生态风险及 AI 驱动攻击等新型挑战，基于国家战略与行业实践，为筑牢软件供应链安全防线提供专业指引。

武汉大学国家网络安全学院二级教授、博导、珞珈特聘教授赵波带来《可信的人工智能实现方法思考》，

中国工业互联网研究院标准化技术研究所
所长、高级工程师薛强

国家工业信息安全发展研究中心软件所
所长助理、正高级工程师姚珊

武汉大学国家网络安全学院二级教授、
博导、珞珈特聘教授赵波

黄鹤网络安全实验室
执行主任孙进

国网武汉供电公司信息通信分公司
副总经理顾显俊

武汉大学人工智能学院副院长、
教授、博导洪亮

他提出构建覆盖 AI 大数据全生命周期、计算环境及隐私保护的完整解决方案，打开可信 AI 技术落地的新思路。

在技术实践与案例分享环节：

黄鹤网络安全实验室执行主任孙进提出《人工智能时代，数据中心基础设施内生安全的测试方法探索》，结合实验室建设布局，针对 AI 安全研究中的语料与大模型安全挑战，给出智算中心基础设施内生安全的测试方案与公测规划。

国网武汉供电公司信息通信分公司副总经理顾显俊分享《基于人工智能的电力网络安全监测运营》案例，通过 AI、大数据分析和区块链技术，构建具备智能分析、智慧编排能力的安全监测体系，为关键领域安全防护提供实践范本。

建平台聚智赋能创新生态 立倡议凝心共筑安全防线

会议期间，揭牌仪式与倡议发布成为论坛亮点：

武汉市网络安全协会人工智能专业委员会正式揭牌，专委会主任武汉人工智能研究院副院长彭骏与秘书长黄鹤网络安全实验室副总经理史琳波共同揭牌，市委网信办与市经信局相关领导共同见证。该专委会以“人工智能 + 安全”深度融合为使命，将开展技术研发攻关、标准体系建设、应用场景拓展及人才培养等工作，助力武汉构建 AI 安全创新集聚区。

武汉大学人工智能学院副院长、教授、博导洪亮发布《人工智能基础设施产品内生安全能力提升倡议书》，倡导坚守安全理念、构建全生命周期保障体系，凝聚政产学研用多元主体合力，为 AI 产业健康发展指明方向。

政产学研聚力共商协同之道 网安产业破局擘画变革新篇

圆桌对话环节以“网络安全产业变革下的政产学研协作”为主题，由武汉临空港经开区经科局副局长、华科网络空间安全学院博士生导师胡胜山主持，六位嘉宾围绕产业痛点展开深度探讨：

武汉城市职业学院计算机学院院长向健极提出，职校与企业合作的核心是建立中介服务机制，强调学生

圆桌对话：网络安全产业变革下的政产学研协作

需提升政治、专业与职业素养以贴合产业需求。

湖北大学网络空间安全学院副院长何鹏分享通过模块化课程设计、强化实践教学、深化校企合作的人才培养模式，让教学内容与企业需求精准对接。

金银湖实验室常务副主任陈兴跃提出以有组织科研整合资源，聚焦工业互联网安全领域，打造“技术研发 - 成果转化”闭环体系，支撑网安产业发展。

奇安信集团湖北省分区总经理黄宝分享与高校共建人才培训基地的经验，强调“研发型、技术型、应用型”三类人才分类培养模式，破解产业人才缺口问题。

天融信集团湖北公司总经理张敬民指出，“产学研”合作落地需建立需求导向的协同机制，明确利益分配规则，实现技术攻关与产业化无缝衔接。

安恒信息湖北公司副总经理张吉浩建议以“智能体生态共创”机制促进产学研需求对接，通过标准化流程解决成果转化效率难题。

锚定网安产业高地 为数字中国筑牢安全屏障

作为国家网络安全人才与创新基地核心承载地，武汉已汇聚奇安信、天融信、安恒信息等头部网安企业，布局黄鹤网络安全实验室、金银湖实验室等创新载体，并新建全国首个网络安全大学。武汉市网络安全协会将携手国家网安基地产业联盟以本次论坛为契机，深化“智算赋能、软硬协同、生态共生、安全护航”的发展模式。

此次论坛不仅标志着武汉市在推动 AI 与网络安全融合创新中迈出关键一步，更是协会推动各方依托武汉区位优势与产业基础，在“加快建成中部地区崛起重要战略支点中当好龙头、走在前列”进程中积极发挥网络安全专业性社团行业组织作用的具体实践，为数字中国建设筑牢安全屏障，贡献“武汉方案”。

武汉市网络安全协会人工智能专业委员会揭牌仪式

《人工智能基础设施产品内生安全能力提升倡议书》

数链聚能 产业共融

——2025 年数据安全供需对接会成功举办

6 月 20 日，由武汉市数据局、武汉市委网信办主办，国家网络安全人才与创新基地产业联盟、武汉市网络安全协会、武汉市工程科学技术研究院有限公司、武汉安域信息安全技术有限公司承办的 2025 年度“数链聚能 产业共融”数字经济场景“对对碰”暨数据安全供需对接会，在网安基地举行。活动旨在为数据安全供需双方搭建对接平台，促进数据安全领域科技与产业创新深度融合，推动武汉数据安全产业高质量发展。来自数据安全领域产品服务供应商、需求企业、第三方机构、科研机构及高校共百余名代表齐聚一堂，共探行业发展新路径。

在专题分享环节，我会副会长单位武汉吧哒科技股份有限公司、湖北天融信网络安全技术有限公司、武汉安域信息安全技术有限公司，理事单位武汉达梦数据库股份有限公司等供应商进行专题分享，详细介绍了在硬件设备、软件产品、安全服务等方面的最新成果及优势；艾普工华科技 (武汉) 有限公司、武汉市中心医院等机构代表分享了在数据安全管理方面的经验及需求。随后，供需双方围绕数据安全开展对接交流，现场气氛热烈。

数据安全是国家安全的重要基石，也是数字经济稳健发展的核心保障。随着数字技术在各行业的广泛渗透，数据已成为关键生产要素，其安全与否直接关系到企业的生存发展、公民的隐私权益以及社会的稳定运行。近年来，国家相继颁布了如《中华人民共和国数据安全法》《个人信息保护合规审计管理办法》《人脸识别技术应用安全管理办法》等一系列数据安全法规。这些法规的出台，构建起严密的数据安全治理体系，明确了数据处理活动的规范与边界，为数据安全产业发展提供了坚实的法律支撑。

未来，国家网络安全与人才创新基地产业联盟将携手武汉市网络安全协会，发挥平台优势整合资源，多组织供需对接与技术交流活动。联合高校、科研机构攻关技术、培养人才，为武汉网络安全产业提供支撑保障；配合政府加强行业自律，开展技术交流与标准制定，促进供需对接和成果转化，共同培育产业生态，护航武汉数字经济发展。

凝聚网安力量 共绘发展新篇

2025 年 6 月 27 日，武汉市网络安全协会第二届第三次会员大会在国家网络安全人才与创新基地隆重举行。协会会长、副会长、监事、秘书长、各分支机构负责人、理事、会员代表及秘书处全体工作人员参会，共同谋划武汉网络安全发展新路径。

武汉市网络安全协会第二届第三次会员大会成功召开

武汉市网络安全协会第二届第三次会员大会

会上，协会会长潘宣辰作 2024-2025 年度工作报告，全面总结协会在党建引领、自身建设、宣传活动、标准建设、人才培养等领域的工作成果与创新实践。

报告指出，2024 年以来，协会坚持党建引领，在强化党员责任与践行社会责任上双向发力。通过开展主题党日活动，联合武汉革命博物馆、武汉联通等单位开展党建联建，增强党员网络安全责任意识；同时积极开展防汛慰问、网络安全知识进社区校园等活动，彰显行业协会担当。在自身建设与服务能力提升方面，协会成绩斐然。2024 年获评“AAAA 级社会组织”，2025 年新增医疗卫生与健康分会、人工智能专业委员会、国家网安基地产业联盟工委会三大分支机构，并吸纳多家优质单位入会，会员队伍不断壮大。此外，协会还组织会员代表赴重庆交流合作，与当地协会签订战略合作协议，进一步提升行业影响力。活动创新与标准建设同样亮点频出。在国家网络安全宣传周期间，协会策划长江网络安全灯光秀、全市公安反电诈宣传机网络安全宣传投放等创新活动，有效提升市民网络安全意识。在标准体系构建上，2024 年发布六项团体标准，2025 年与中国网络空间安全协会联合发布《智能网联汽车网络安全检测技术要求》，为行业发展提供规范指引。人才培养与行业赋能工作扎实推进。协会开展网络安全技术人才职称评审，组织多场专业培训讲座，举办“黄鹤杯”“楚慧杯”等赛事，开展网络安全攻防演练、供需对接会等活动，搭建产学研用协同发展平台，激发行业创新活力。财务数据显示，2024 年协会收入大于支出，财务运行稳健，为各项工作开展提供有力保障。该报告获大会全票通过。

武汉市网络安全协会专家聘任仪式（部分）

武汉市网络安全协会专家聘任仪式（部分）

武汉市网络安全协会专家聘任仪式（部分）

受第二届理事会第六次会议委托，秘书长刘悦恒向大会提交五项提案，涵盖注册地址变更、会费标准调整、支持国家网安基地产业联盟建设、继续聘任赵波教授为专家委员会主任及续聘孙宝林等 55 位专家充实智库力量等内容。大会一致通过相关提案，特别在支持国家网安基地产业联盟建设上，全体会员同意集体加入联盟，助力国家网安基地建设发展。

会议强调，协会将坚守“服务会员、行业、政府、社会”的办会宗旨，紧扣国家网络安全战略，深化党建与业务融合，加强多方协同合作，推动技术创新、标准建设与人才培养，支持国家网络安全人才与创新基地建设，为武汉市网络安全事业高质量发展持续赋能，在网络强国建设中贡献“武汉力量”。

此次会员大会的成功召开，凝聚了会员共识，明确了发展方向。未来，武汉市网络安全协会将携手业界同仁，不断筑牢我市网络安全防线，共同书写数字经济时代的新篇章。

国家网安基地产业联盟在汉全面启动 助力打造网络安全产业高地

近日，国家网络安全人才与创新基地产业联盟大会在汉召开，网络安全领域企业、高校、科研机构代表 200 余人参加。武汉市委网信办、东西湖区相关负责人共同发布《2025 国家网络安全人才与创新基地产业联盟工作规划》，标志着集“供需对接枢纽站、网安人才交流港、网安企业服务区、产教融合加速器”于一体的网安基地产业服务综合体全面启动。

工作规划明确依托国家网安基地，打造四大功能服务载体：供需对接枢纽站搭建线上线下平台，破解技术与市场融合壁垒；网安人才交流港绘制人才产业图谱，构建全链条服务；网安企业服务区推动跨区商务合作，引入专业服务机构；产教融合加速器成立成果转化中心，加速技术商业化进程。

会上，14 家行业协会跨区域跨行业联动签约，覆盖长三角、西南、中部等多区域，实现人工智能等前沿领域与网安产业跨界融合。22 家专业机构入驻联盟，服务范围涵盖金融赋能等六大领域，增强了对网安企业全生命周期的专业化服务能力。

会议期间还举办了全市医疗健康领域网络安全应用场景供需对接会，组织上海、重庆、云南等省市网络安全产业代表考察网安基地，推动全省军民融合、低空经济等十余个行业领域代表与基地洽谈。

据介绍，历经十年发展，位于武汉的国家网安基地已形成以网络空间安全为主赛道，人工智能与大数据为分赛道，工业软件等信息技术服务新业态为延伸的“1+2+N”特色产业体系。4 平方公里核心区汇聚了奇安信、天融信等众多头部企业。依托国家关键信息基础设施安全保护培训基地和武汉大学、华中科技大学网安学院，累计开展各类培训超 4 万人次。武汉金银湖实验室、黄鹤实验室、网络安全众测平台等十大平台落地运营，智算中心一期 125P 智算算力已投用。目前，国家网安基地正朝着“人才高地、创新高地、产业高地”目标迈进。

国家网安基地与各行业组织战略合作签约仪式

武汉市网络安全协会医疗卫生与健康分会首次工作会议召开 开启医疗网安协同新征程

2025 年 6 月 27 日，武汉市网络安全协会医疗卫生与健康分会第一次全体工作会议在国家网络安全人才与创新基地成功召开。会议以贯彻习近平总书记网络强国重要思想、落实《医疗卫生机构网络安全管理办法》为指引，为武汉医疗健康领域网络安全建设凝聚智慧、搭建合作桥梁，推动形成“政医企研”协同发展新格局。

分会正式揭牌 构建行业组织引领体系

会议举行了揭牌仪式与聘书颁发仪式。武汉市中心医院信息中心主任李海受聘医卫分会会长，武汉市中医医院信息中心主任孙淼受聘秘书长，多家医院网络安全和信息化负责人受聘分会副会长、理事。揭牌仪式标志着医卫分会正式启航，分会将在我市医疗网络安全领域发挥关键的组织引领作用。

多维度专业赋能 输出医疗网安解决方案

会上，分会携手行业专家带来深度技术分享：会长李海结合武汉市中心医院实践，详解《商用密码应用安全建设经验》，展示密码技术在电子病历加密、医疗设备认证等场景的落地成效；武汉安域公司专家解读《医疗卫生行业商用密码应用安全性评估工作》，为医疗机构提供合规测评路径；奇安信数据安全团队发布《健康医疗行业数据分类分级解决方案》，并发起团体标准征集，推动医疗数据安全管理标准化建设。此外，分会同步解读网络安全人才职称评审政策，为行业技术人才职业发展搭建通道。

锚定三大发展方向 规划行业安全蓝图

分会秘书长孙淼在总结中明确三项重点工作：一是启动新会员招募计划，扩大医疗网安“朋友圈”；二是组建防勒索攻击应急专班，建立行业级应急响应机制；三是常态化举办技术对接会，促进安全方案与医疗场景深度融合。市卫生健康信息中心安全管理部主任李娜强调，分会需通过搭建资源对接平台，助力武汉医疗行业在数字化转型中实现“安全与发展并重”。

此次会议的召开，标志着武汉医疗网络安全工作迈向系统化协同阶段。未来，医卫分会将以“护航健康武汉”为使命，搭建网络安全企业、医疗机构、科研院所等多方沟通合作桥梁，推动建立具有武汉特色的医疗网络安全防护体系，为智慧医疗建设筑牢安全基石。

武汉市网络安全应用场景供需对接会金融保险专场顺利召开 全国首个风险量化标准发布

7 月 24 日，武汉市网络安全应用场景供需对接会金融保险专场在国家网络安全人才与创新基地成功举办。此次活动由武汉市委网信办指导，国家网络安全人才与创新基地产业联盟主办、武汉市网络安全协会网安保险工作委员会承办，市经信局、市住建局、东西湖区等单位，中国人保、中国平安、长江财险、国任财险、江泰保险等金融保险公司，以及天融信、奇安信等网安企业共 50 余家单位代表参会。

武汉市作为拥有国家网络安全人才与创新基地和唯一国家级科技保险示范区的城市，此次专场活动亮

点纷呈。会上发布全国首个面向全社会的网络安全风险量化评估的指南《网络安全风险量化评估规范》团体标准，并通过全国团体标准信息平台审核。该标准创新构建快速风险识别框架与量化评估方法，为提升网络安全管理水平提供支撑，获金融保险机构及相关单位高度认可，未来可广泛应用于网络安全保险核保、定损等各流程全场景。

活动现场，举行了《网络安全风险量化评估规范》团体标准参编证书颁发仪式，广东省电信规划设计院专家深度解读标准编制情况，良品铺子分享了企业应用实践案例，直观展现标准落地成效。在供需对接环节，网络安全企业与金融保险机构围绕“风险量化、技术服务、保险托底”融合方向达成共识。会上，毕昇云公司、天融信、中国人保、中国平安等单位形成多项合作意向。

此次对接会有力推动了武汉网络安全产业与金融业的深度融合，进一步彰显了国家网安基地产业联盟的桥梁纽带作用，为我市数字经济高质量发展提供有力网络安全保障。

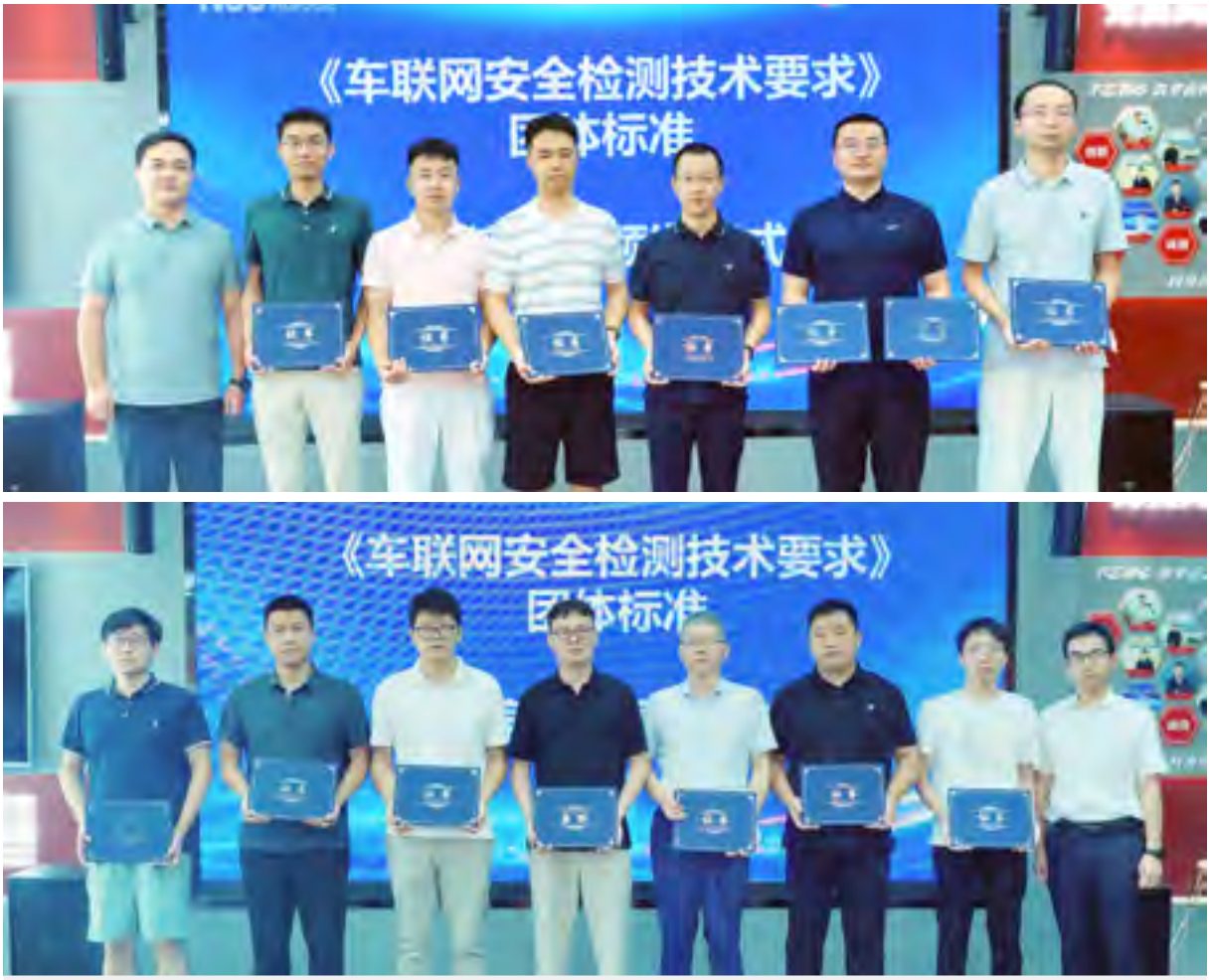
武汉市网络安全应用场景供需对接会智能网联汽车专场顺利召开 车联网安全标准落地助力产业合规发展

2025 年 9 月 9 日，武汉市网络安全应用场景供需对接会智能网联汽车专场在国家网络安全人才与创新基地（以下简称“国家网安基地”）培训中心成功召开。本次活动由国家网安基地产业联盟主办、武汉市网络安全协会智能汽车专委会承办，汇聚东风汽车集团、岚图汽车、东风悦享、湖北天融信、襄阳达安汽车检测中心、湖北省电检院、武汉大学、华中科技大学、湖北大学、江汉大学等 40 余家整车制造企业、网络安全企业、检验检测机构及高校科研院所代表，通过政策解读、技术分享、标准宣贯与供需对接，明确车联网安全合规路径，促成多项技术合作与检测服务对接意向，为武汉智能网联汽车产业安全有序发展注入新动能。

一、政策解读与技术创新双轮驱动 筑牢产业安全合规根基

活动伊始，国家级机构专家以线上形式开展智能网联汽车数据安全法规政策专题解读，紧扣国家数据安全战略部署，聚焦汽车数据全生命周期管理核心要求，从政策红线界定、合规路径梳理、实操指引落地三个维度，为参会单位提供系统性指导，有效解决整车厂商、安全服务企业在技术研发与业务开展中的合规困惑，夯实产业发展政策基础。

随后，襄阳达安汽车检测中心有限公司安浩杨博士发布《车联网漏洞数据库及检测技术研究与应用》成果报告。针对当前行业面临的车联网专用漏洞数据



颁发参编证书

库缺失、通用漏洞扫描工具误报率高等痛点，襄阳达安基于 GB/T《汽车安全漏洞分类分级评价》国家标准，成功构建车联网专属漏洞数据库，研发集成 POC 漏洞验证脚本的高效检测系统，实现漏洞“科学管理、精准检测、快速定位”，已成功支撑多款车型通过出口认证及国家标准认证，为产业安全技术落地提供关键支撑。

二、团体标准正式落地 填补车联网安全检测规范空白

会上，《车联网安全检测技术要求》团体标准（由中国网络空间安全协会、武汉市网络安全协会联合发布）宣贯成为核心环节。湖北天融信技术总监谭咏涛代表标准编制组，结合车载安全领域实践案例，详细解读标准在不同应用场景的实施要点。该标准不仅填补当前车联网安全检测领域的规范空白，更能有效降低企业网络安全合规成本、提升检测效率，为产业链上下游协同提供“通用安全语言”，解决技术合作与服务对接中的标准壁垒问题，得到参会单位高度认可。

武汉大学国家网络安全学院曹越教授分享标准编制经验时指出，该标准充分体现产学研融合优势，具备较强创新性与实用性，同时展望在低空经济设备检测领域开展技术合作、推动标准化落地的可行路径，为产业跨界发展提供思路。

活动现场，武汉市网络安全协会、国家网安基地产业联盟秘书长刘悦恒，与武汉市网络安全协会智能汽车专委会主任、岚图汽车科技有限公司数字化高级总监陶先锋共同为标准参编单位及专家颁发参编证书，标志着该团体标准从编制阶段正式迈向落地应用阶段，


襄阳达安汽车检测中心有限公司安浩杨


武汉大学国家网络安全学院曹越教授


湖北天融信技术总监谭咏涛


岚图汽车陶先锋


珈港科技杨世昭


宝牧科技肖海涛


湖北天融信左世涛


武汉中科晶上郝斌


武汉市网络安全协会
智能汽车专委会秘书长吕露

为行业安全检测提供统一遵循。

三、供需对接凝聚产业共识 聚焦核心领域协同发展

在供需对接交流环节，参会单位围绕智能网联汽车产业安全发展痛点、难点展开深入研讨，形成多项重要共识

一是加快车联网安全芯片国内标准制定。

岚图汽车陶先锋、珈港科技杨世昭等代表提出，当前行业依赖 AEC-Q100 等国外车规级规范，亟需出台符合我国产业实际的安全芯片标准，破解核心技术“卡脖子”问题。面对这一现状，武汉市网络安全协会智能汽车专委会将持续搭建对接平台，推动标准体系完善。

二是强化供应链安全与数据源头防控。

宝牧科技肖海涛表示，“无安全零部件则无整车安全”，需推动安全要求与供应链规划设计同步推进；针对数据安全，建议行业联合推广同态加密、隐私计算等技术，从源头阻断数据泄漏风险

三是推动检测技术升级与新技术融合。

湖北天融信左世涛介绍，其自适应弹性安全解决方案已在前装生产线及多测试示范区落地，建议行业进一步强化全生命周期检测覆盖、深化车路云协同检测技术研发、加强整车厂供应链安全检查；武汉中科晶上郝斌提出，需将星闪无线短距、高低轨卫星通信等新通信技术纳入安全标准，应对智能汽车“移动智能终端化”带来的远程攻击、隐私泄露等新风险。

四、会后延伸拓展合作空间 助力技术产业化落地

活动结束后，参会代表团赴武汉中科晶上国际星闪联盟湖北创新实验室开展实地调研，详细了解星闪通信技术在智能汽车场景的产业化应用进展。部分代表现场与中科晶上就技术研发、场景落地等方面展开深入交流，初步明确后续合作方向，为会议成果转化与产业协同发展拓展新空间。

本次对接会由武汉市网络安全协会智能汽车专委会秘书长吕露主持。活动的成功举办，不仅充分发挥国家网安基地产业联盟桥梁纽带作用，推动武汉市智能网联汽车产业链上下游资源整合与协同创新，更以“标准落地 + 技术对接”为抓手，为我国智能网联汽车产业安全、有序、高质量发展提供“武汉实践”样板。

本次对接会由武汉市网络安全协会智能汽车专委会秘书长吕露主持。活动的成功举办，不仅充分发挥国家网安基地产业联盟桥梁纽带作用，推动武汉市智能网联汽车产业链上下游资源整合与协同创新，更以“标准落地 + 技术对接”为抓手，为我国智能网联汽车产业安全、有序、高质量发展提供“武汉实践”样板。

武汉市网络安全应用场景供需对接会人工智能专场顺利召开 公约与标准双轮驱动助力 AI 产业合规发展

2025 年 10 月 15 日，武汉市网络安全应用场景供需对接会人工智能专场在国家网络安全人才与创新基地（以下简称“国家网安基地”）培训中心成功召开。本次活动由国家网络安全人才与创新基地产业联盟主办、武汉市网络安全协会人工智能专委会承办，汇聚相关主管单位、武汉人工智能研究院、黄鹤实验室、湖北天融信、金山办公、浪潮智慧科技、国网电力、湖北移动、中金数据（武汉）超算、武汉大学、武汉理工大学、江汉大学、武汉轻工大学等 30 余家单位。聚焦人工智能安全发展核心议题，通过工作汇报、公约发布、标准立项、技术分享与供需对接，明确人工智能安全合规路径，促成网络安全企业为 AI 用户单位提供定制化安全服务，为武汉人工智能产业安全有序发展注入新动能。

总结汇报与公约落地 筑牢 AI 安全发展根基

活动伊始，武汉市网络安全协会人工智能专委会秘书长史琳波开展人工智能专委会工作汇报。武网安协人工智能专委会自今年 5 月成立以来，已构建“政产学研用”多元协作架构。在 6 月第一次全体委员会议上，专委会完成首批委员受聘仪式，明确技术研发与产业协同、标准化建设、应用场景拓展、人才培养、安全治理五大工作方向。同月，专委会承办了以“AI 驱动网络安全革新”为主题的第三届软件创新发展大会网络安全论坛，并同步发布《人工智能基础设施产品内生安全能力提升倡议书》，为区域 AI 安全协作奠定基础。

随后，《武汉市生成式人工智能发展安全公约》（以下简称《公约》）审议表决与发布环节成为核心内容。

据武汉市网络安全协会人工智能专委会主任、武汉人工智能研究院副院长彭骏介绍，当前生成式 AI 快速发展，面临数据安全、模型可信、伦理边界模糊等多重挑战，《公约》的制定旨在凝聚企业、科研机构、监管单位的共同智慧，明确 AI 发展的安全准则与伦理底线，为武汉 AI 产业划定“安全红线”与“发展绿线”。随后协会人工智能专委会主任、副主任等嘉宾共同发布《公约》，正式推动《公约》落地。

检测标准立项发布填补领域规范空白

本次会议针对《生成式 AI 安全检测技术要求》标准的立项进行深入讨论。据该标准牵头立项单位黄鹤实验室技术负责人索凯华介绍，当前生成式 AI 安全检测缺乏统一技术规范，企业普遍面临“检测无依据、选型无标准”的困境，该标准立项将填补这一领域的规范空白，为 AI 产品安全测评提供科学、可量化、可执行的技术指引，降低企业合规成本、提升检测效率，为产业链上下游协同提供“通用安全语言”。该标准将围绕“数据安全、模型安全、内容合规、服务安全”四大安全维度构建，为企业技术选型、检测机构服务提供清晰方向，为 AI 产品安全测评提供科学指引，得到参会单位高度认可。

技术与实践双维分享赋能 AI 安全路径探索

人工智能安全相关领域专家、二级教授陈伟以《人工智能 + 网络安全的机遇与挑战》为主题，从技术演进、应用场景、安全挑战三方面展开分享。陈教授指出，AI 已从“专家系统（规则驱动）”迈入“深度学习（数据驱动）”阶段，安全风险同步升级。他结合“交通领域、制造领域、医疗领域、金融领域”四大典型应用场景剖析风险点，从技术原理到风险应对，内容兼具前瞻性与实用性，为企业解决 AI 安全痛点提供宝贵思路。

湖北移动区域技术总监宋文以《中国移动人工智能发展安全需求与未来展望》为题，结合企业实践解

武汉市网络安全协会人工智能专委会秘书长史琳波

黄鹤实验室技术负责人索凯华

人工智能安全相关领域专家、二级教授陈伟


湖北移动区域技术总监宋文

读 AI 安全落地路径。他指出，中国移动作为“人工智能 +”行动核心参与者，锚定“供给者、汇聚者、运营者”三大定位，已形成完善的 AI 安全保障体系。

场景供需对接研讨 凝聚协同发展共识

自由讨论环节，参会嘉宾围绕“AI 大模型安全检测难点”“行业合规成本控制”等话题自由交流，部分 AI 企业与安全服务机构初步达成技术对接意向。

武汉软件工程职业学院信息化中心副主任罗滨介绍，该校目前正在与行业主管部门在人工智能领域共建职教基础创新平台，积极推进产权成果建设。学校在网信人才培养及 AI 教学管产研应用、私有算力安全保障等方面工作，热忱欢迎各专业性组织、产业企业积极参与和支持。

武汉理工大学网络信息中心安全监管部主任喻辉结合工作指出，建议聚焦网络安全场景：一是研究数据安全保护与信息泄露发现检测，二是关注生成内容合规性，三是让 AI 赋能网络安全工作，探索新应用。

武汉轻工大学副教授张帆表示愿推动学校积极参与协会各项标准建设。希望搭建校企沟通平台，促进供需对接，同时向头部单位学习。

中金云链（武汉）数字科技有限公司客户经理张铭表示企业希望能与行业加强协作，及时获取行业动态、新标准等信息，以更好地服务社会发展。

本次人工智能专场对接会的成功举办，将充分发挥国家网络安全人才与创新基地产业联盟的桥梁纽带作用，推动武汉市人工智能产业链上下游资源整合与协同创新，通过“明确安全共识、提供技术标尺、破解落地痛点、促进成果转化”四维发力，不仅为武汉人工智能产业筑牢安全屏障，更形成可复制的“政产学研用”协同模式，助力武汉数字经济高质量发展。

网安基地招聘双选会火热启幕
助力国家网安基地人才高地建设

10 月 25 日，2025 年秋季招聘双选会暨网信人才集市在国家网络安全人才与创新基地火热启幕。本次活动由国家网安基地产业联盟（武汉市网络安全协会）携手华中科技大学网络空间安全学院、武汉大学国家网络安全学院联合主办，精准对接两所高校千余名应届本硕博毕业生，近四十家行业顶尖企业携数千个优质岗位组团“揽才”，搭建起校园人才与产业需求无缝衔接的桥梁。

01 名企云集阵容空前 覆盖多元核心领域

本次双选会的企业阵容堪称“豪华”，既有华为、小米这样的世界 500 强巨头，也涵盖天融信、绿盟科技、奇安信、启明星辰等网络安全领域全链条头部企业；既吸引了谋先飞等聚焦具身智能、物理仿真的人工智能新锐，达梦数据库等基础软件骨干，也包括腾讯、美团等互联网领军者，以及宁德时代、复星财富控股等跨界大型企业。

参会企业业务覆盖网络安全、人工智能、智能制造、金融科技、数字孪生等多个前沿领域，与华中科大、武大网安学院的人才培养方向高度契合。

02 岗位聚焦应届生需求 技术岗成招聘主力

本次双选会的岗位设置紧扣优秀应届生特点，以技术研发岗为核心，兼顾多元发展需求，普遍降低职



场经验门槛。核心岗位主要集中在三大类别：

网络安全核心类：多家网络安全领域企业推出安全服务工程师、渗透测试工程师、等保测评工程师等岗位，面向 2026 届应届生。要求熟悉 OWASP Top 10 漏洞类型、渗透测试工具使用或网络安全合规标准，部分岗位明确“对攻防渗透感兴趣即可”，不强制要求工作经验。某科技企业的安全研发工程师、网络安全工程师等岗位，还将开源项目经验、技术分享经历列为加分项，鼓励学生发挥专业所长。

新兴技术应用类：某新兴技术企业的初级引擎开发工程师、具身智能技术应用工程师等岗位，欢迎数学、物理、计算机相关专业应届生，重点考察学习能力和技术热情。某汽车检测与技术研发机构的车规芯片测试技术、智能网联汽车信息安全测试技术等岗位，面向硕士应届生，聚焦汽车网信领域前沿需求，提供技术研发与测试的成长路径。

综合支撑类：某金融控股企业的“财富星耀生”“科创星耀生”岗位，面向本科及以上应届生，分别聚焦金融业务服务和量化策略交易系统设计，提供系统化培训机会。

03 福利适配青年需求 校企联动深化产教融合

为吸引应届生留汉发展，参会企业纷纷推出针对性福利政策。除五险一金、入职礼、生日礼等基础福利外，不少企业为武汉岗位提供免费人才公寓，解决住宿后顾之忧；工作模式上，“无需打卡、效率为先”“平等同学式沟通氛围”成为主流，契合年轻群体职场期待。

同时，企业普遍重视应届生培养，多数岗位配备高级工程师“一对一带教”，协助参与核心项目，如安全防护体系搭建、物理引擎模块开发、仿真场景测试等，帮助应届生快速完成校园到职场的衔接。

双选会现场人头攒动，来自华中科大、武大的应届生手持简历，围绕岗位技术要求、成长空间、留汉福利等问题与企业招聘负责人深入交流。

国家网络安全人才与创新基地产业联盟相关负责人表示，本次双选会暨网信人才集市是落实网络强国战略、深化产教融合的具体实践。未来将持续常态化举办此类活动，当好“连接器”和“催化剂”，吸引更多网信领域青年人才留汉创业就业，助力武汉打造国家网络安全人才与创新高地。

2025 年首场武汉市工业领域数据安全能力提升专题宣贯培训汉口片区活动成功举办

11 月 5 日下午，2025 年武汉市工业领域数据安全能力提升专题宣贯培训首场活动在东西湖区临空港会展酒店顺利启幕，正式拉开全市三场分片覆盖培训的序幕。本次活动由工信部电子第五研究所、湖北省经济和信息化厅指导，武汉市经济和信息化局、国家网络安全人才与创新基地联合主办，武汉市工业信息化中心、东西湖区经济信息化和科创局共同承办，武汉企业信息化促进会、国家网络安全人才与创新基地产业联盟、武汉市网络安全协会协办支持。来自江岸区、江汉区、硚口区等 7 个片区的工业领域重点企业代表、数据安全专家学者齐聚一堂，围绕政策落地、技术应用、实践经验等核心议题深度交流，为筑牢武汉工业数据安全防护体系凝聚共识、注入动能。武汉市经济和信息化局总工程师谌斌、湖北省经济和信息化厅人工智能和大数据产业处二级调研员贺斌出席活动并致辞。

谌斌总工程师在致辞中指出，工业数据是驱动制造业数字化、网络化、智能化转型的核心要素，其安全与否直接关系到企业生产经营稳定、产业链供应链韧性，更是保障全市工业经济高质量发展的关键基石。本次培训作为 2025 年武汉工业数据安全宣贯的开篇活动，精准聚焦企业在数据安全管理中面临的痛点难点，搭建起政策解读、技术交流与经验分享的专业平台。他希望参会企业能充分把握此次学习机会，认真吸收活动中的专业知识与实践经验，切实将数据安全理念融入生产经营各环节，不断提升企业自身数据安全管理水平，为全市工业数字化转型筑牢坚实的安全屏障。

贺斌调研员围绕全省工业数据安全工作提出“四点期待”与“七项目标”。期待方面，希望参训人员专注学习、专家提供针对性方案，企业落实《数据安全法》等法规标准，武汉依托产业优势在数据安全工作中为全省做表率，各方共同落实工信部相关实施方案。省经信厅将持续联动各地市州相关部门，完善政策支持体


系，搭建供需对接平台，推动数据安全技术创新与产业应用深度融合，助力全省工业企业在数字时代实现安全与发展协同推进。

政策解读环节，工信部电子五所数据安全室副主任王帆作为核心讲师，对《数据安全标准体系》进行了系统解读。他从标准体系的框架构成、核心内容及落地要求出发，结合工业领域数据安全的典型场景，详细剖析了重要数据识别、分级分类保护、风险评估等关键环节的实施要点，并针对不同行业的差异化需求提供了实操性建议，为企业精准落实数据安全合规要求提供了专业指导。

在案例分享与技术交流环节，各领域专家带来了丰富的实践经验与前沿理念。益海嘉里（武汉）粮油工业有限公司 IT 负责人刘业豪聚焦企业数据安全管理实践，从组织架构搭建、制度流程完善、技术工具部署等方面，分享了益海嘉里在数据全生命周期防护中的具体做法与成效，为传统制造业数据安全建设提供了可借鉴的实践样本。

深信服湖北区安全运营主管陈明明带来《AI 时代下的网络安全防护理念》主题分享，他结合工业场景中

AI 技术的应用实例，提出“智能预判 + 动态防御”的防护新思路，强调通过 AI 算法实时分析工业数据流转中的异常行为，提前识别潜在安全风险，助力企业摆脱传统被动防御的局限；青藤云安全专家张晓慧则围绕《工控系统供应链安全建设》展开演讲，聚焦工控设备采购、运维、升级全流程的安全隐患，提出从供应商资质审核、设备固件安全检测到供应链应急响应的全链条防护方案，两位专家分别从新兴技术应用与关键领域防护的角度，为参会企业提供了多元化的安全解决方案思路。

培训尾声，主办方组织全体参会人员前往奇安信安全智能展厅、360 安全智能展厅进行实地参观。通过近距离观摩前沿数据安全技术产品与解决方案的演示，参会企业代表对工业数据安全防护的最新发展趋势有了更直观的认识，进一步拓宽了安全建设的思路与视野。

本次活动的成功举办，是武汉市贯彻落实《工业领域数据安全能力提升实施方案（2024-2026 年）》的具体举措，通过“政策解读 + 案例分享 + 实地观摩”的多元化形式，有效搭建了政企学研多方交流的桥梁。活动不仅帮助工业企业精准把握数据安全政策要求，提升了安全防护实操能力，更推动了数据安全技术资源与企业实际需求的精准对接。未来，随着系列宣贯培训活动的持续开展，将进一步夯实武汉市工业数据安全基础，为新型工业化发展提供坚实的安全保障，助力全市工业经济实现高质量、可持续发展。

极智守护 驭见未来
第一届小米汽车守护活动圆满结束

历经 7 天，由武汉市网络安全协会支持的深度攻防技术博弈与网络安全验证，聚焦汽车网络安全的第一届「小米汽车守护活动」于 2025 年 11 月 12 日在武汉圆满落幕。在此，我们向鼎力支持本次活动的行业机构、权威专家，以及 17 支顶尖白帽专家团队致以最诚挚的谢意！作为小米汽车践行“安全是前提，安全是基础，安全是一切”核心理念的重要实践，本次活动以开放姿态搭建起技术探索与行业协作的桥梁，为智能汽车安全生态建设注入强劲动力。未来，小米将持续开放技术边界、深化行业协作，与全球安全研究人员携手并肩，共同筑牢小米汽车网络安全防线。

本次活动于 11 月 6 日在小米武汉总部正式启动，小米武汉区域总部总经理、集团技术委员会副主席王扉，小米集团技术委员会信息安全部负责人王书魁，小米汽车部合规与安全负责人单渤凯，武汉市网络安全协会党支部书记、专职秘书长刘悦恒，中汽智能科技（天津）有限公司副总经理（主持工作）杨正军，中汽协会数据分会执行秘书长滕添益，中国汽研 - 融合安全技术中心主任贺鹏，北京犬安科技有限公司 CEO & 创始人李均，小米集团技术委员会智能终端安全实验室负责人罗丁，小米汽车部车联网安全产品网络安全负责人曹小锋共同出席启动仪式，见证这场聚焦智能汽车安全的技术盛会。

活动为期 7 天，17 支白帽子团队对 9 辆小米 YU7 开展全方位网络安全攻击测试，覆盖智能汽车核心安全领域，通过实际测试验证车辆安全防护能力，同时收集宝贵的漏洞报告与技术反馈，为小米汽车安全体系优化提供直接支撑。

行业共识，共筑安全新生态

作为智能汽车安全领域的一次重要实践，本次活动得到了行业伙伴的广泛认可与深度参与。各出席机构

与企业通过活动交流，围绕智能汽车安全生态建设展开深入探讨，凝聚“强化技术协作、共筑安全防线”的行业共识，为后续安全合作奠定基础。活动期间，各方结合测试实践与行业经验，就智能汽车安全防护重点、技术迭代方向等话题交换意见，进一步明确“开放协作”对安全生态建设的重要性，为推动行业安全水平提升提供了实践参考。

持续启程，安全守护不止步

本次「小米汽车守护活动」的圆满结束，是小米汽车网络安全建设的新起点。未来，小米将始终坚守“安全是前提，安全是基础，安全是一切”的理念，持续开放技术边界、深化行业协作，与全球安全研究人员携手并肩，将本次活动收获的技术反馈与协作经验，转化为车辆安全迭代的动力，不断完善小米汽车安全防护体系。同时，小米汽车将继续联动行业伙伴，推动安全技术交流与资源共享，以实际行动筑牢智能汽车安全防线，为消费者打造更安心的智能出行体验。安全无终点，守护永在线。小米汽车将以本次活动为契机，持续深耕智能汽车安全技术创新，与行业同仁并肩前行，用技术守护每一次出行！

筑牢工业数据安全屏障 | 2025 中国 5G+ 工业互联网大会工业数据安全防护平行论坛在武汉成功举办

2025 年 11 月 23 日，中国 5G+ 工业互联网大会工业数据安全防护平行论坛在武汉光谷科技会展中心成功举办。论坛以“筑盾工业数安护航”为核心指引，聚焦工业数据安全风险防控、重要数据分级分类、技术实践与生态协同三大关键议题，搭建起“政策解读 - 技术创新 - 产业落地”三位一体的高端交流平台，为推进制造强国、网络强国、数字中国战略落地筑牢安全支撑。

本次论坛由工业和信息化部新闻宣传中心、2025 中国 5G+ 工业互联网大会组委会主办，湖北省经济和信息化厅、武汉市委网信办、武汉市数据局支持，武汉市网络安全协会、国家网络安全人才与创新基地产业联盟承办，北京赛昇科技有限公司、杭州安恒信息技术股份有限公司协办，汇聚了来自政府部门、高校科研院所、工业制造及网络安全领域的近两百位嘉宾，共话工业数据安全治理新路径。

政策引领定方向 锚定安全发展双主线

工业数据作为新型生产要素，其安全直接关系产业链供应链稳定与国家产业安全。论坛上，政策层面的战略部署与地方实践形成呼应，为行业发展明确路径。

湖北省经济和信息化厅党组成员、副厅长刘良博在致辞中指出，湖北已汇聚工业数据 917 亿条，2025

年底预计突破 1000 亿条，数据安全已成为制造业数字化转型的核心命题。他提出共筑工业数据安全坚固防线，聚焦完善制度标准、强化技术攻关、培育产业生态、深化开放合作四个方面，呼吁加强跨部门、跨区域协作，共同应对数据安全挑战。

武汉市委网信办副主任黄国东强调，武汉作为全国首个国家网络安全人才与创新基地核心承载地，已依托“中国光谷”“中国车谷”“中国网谷”产业优势，汇聚武汉大学、华中科技大学等高校智力资源与众多网络安全和数据安全头部企业，构建起覆盖制造龙头与中小企业的安全防护网。针对当前工业数据防护面临的场景化防御不足、全链条协同薄弱、实战型人才缺口等问题，他提出共筑标准规范、共建技术平台、共育人才梯队、共构协同生态四项建议。

国家工业信息安全发展研究中心数据安全所副所长王墨在主旨演讲中，通过详实数据揭示工业数据安全风险态势：2023 年工业领域数据安全风险同比增长 145.7%，2024 年中高危风险达 349 起，电子信息制造业已成为风险增长最快的细分行业。她从风险形势、工作背景、应对措施三个维度，系统解读了工业数据全生命周期防护的实践路径，为企业安全建设提供专业指引。

技术创新强支撑 产学研用协同破局

技术创新是工业数据安全的核心驱动力，论坛上多项前沿技术成果与实践案例集中亮相，展现了“AI 赋能 + 场景落地”的融合发展趋势。

武汉大学国家网络安全学院教授石小川分享了 AI 驱动的工业互联网安全威胁智能防御方案。其团队研发的 BRNN-GAN 缺失数据补齐技术，在工业数据集上使检测误差降低 21.3%；MtGCN 多时间尺度时序知识图谱建模框架，实现了工业系统动态关联的精准刻画；CCPO 保守约束策略优化算法则确保了防御决策的安全合规，相关技术已成功应用于主管部门网络安全管理平台与电力工控仿真靶场，实现了从实验室到产业界的高效转化。

岚图汽车科技股份有限公司数字化部总监陶先锋带来企业实践案例，展示了智能汽车“云 - 管 - 端”一体化安全防护体系。该体系通过三张专网差异化防控、AI 安全大脑实时监测、全生命周期安全管理等措施，实现了研发核心数据不落地、生产制造安全可控、用户隐私精准保护，为汽车行业数据安全防护提供了可借鉴的实践样本。

论坛同期举行了《数据要素场内流通安全评估技术规范》团体标准颁证仪式，该标准由武汉市网络安全协会归口并发布，武汉安恒信息科技有限公司、武汉大学国家网络安全学院、中国长江电力股份有限公司等 14 家参编单位获颁证书。该标准凝聚行业多方智慧，明确了数据要素场内流通的安全评估指标与实施路径，将为数据要素安全高效流转提供重要技术支撑。

人才赋能固根基 生态协同启新篇

工业数据安全的落地实施，离不开专业人才支撑与协同治理生态。论坛上，国家网络安全人才与创新基地产业联盟举行专家受聘仪式，聘任赵波、张明武、孙宝林、刘腾红、曹越、尚建嘎、向广利等 24 位行业专家，为国家网络和数据安全产业发展提供智力支持。作为全国首个国家网络安全人才与创新基地，湖北武汉正通过人才集聚效应，打造网络数据安全人才培养与技术创新高地。

在“数据驱动时代下工业安全的跨领域协同”圆桌讨论环节，来自学术界、安全企业、科技公司与制造业的嘉宾围绕人才培养、技术落地、生态构建等议题展开深度对话。该环节主持人，武汉职业技术大学人工智能学院信创产业学院副院长邓小飞提出，现如今单打独斗的时代已经过去，如何打破壁垒，实现跨领域、跨行业、跨学科的协同防护，是我们面临的一项课题。武汉大学教授赵波指出，高校需通过“学历教育 + 职业培训 + 实战演练”深度融合，培养既懂工艺流程又懂攻防技术的复合型人才；杭州安恒信息副总裁梁浩强调，安全企业应从“外部赋能”转向“内生安全”，推动安全方案与工业系统深度融合；小米科技安全实验室主任罗丁分享了消费物联网数据安全治理经验向工业场景迁移的实践路径；武汉华工正源光子技术有限公司 IT 部总监陈烨则从制造企业视角，提出了安全解决方案“可定制化”与“系统融合度”的核心诉求。

论坛闭幕式上，本次平行论坛组委会、国家网安基地产业联盟和武汉市网络安全协会联合发布了《工

业数据安全协同防护倡议》，发出共同坚守法定责任筑牢防护根基、深化协同共治凝聚防护合力、强化创新驱动提升防护效能、健全人才体系夯实防护支撑四大行动纲领，呼吁各方携手构建“企业主体、政企协同、产业联动、人才支撑”的安全治理体系。

此次论坛的举办，不仅集中展示了工业数据安全领域的政策成果、技术创新与实践经验，更凸显了湖北武汉在工业数据安全治理中的示范引领作用。未来，湖北武汉将以国家网络安全人才与创新基地为核心，持续推动“5G+ 工业互联网 + 数据安全”融合创新，为全国工业数据安全防护提供可复制、可推广的“湖北模式和武汉方案”，助力新型工业化建设行稳致远。

武汉市网络安全协会服务指南

一 移动应用安全公益检测服务

依托由我会主办的全国首个“移动应用安全公益检测平台”，向广大会员提供移动应用安全公益检测服务。

二 网络安全等级保护测评

依托我会各专业网络安全等级保护测评机构，向广大会员提供网络安全等级保护测评服务。

三 网络安全保险服务

我会与武汉东湖科技保险发展促进中心共建的“东湖网络安全保险服务中心”，提供网络安全保险有关安全服务。依托我会专家库及专业会员力量，协会设立了“数字资产网络安全风险量化实验室”，为我市各类型机构提供风险量化评估服务。

四 网络安全相关标准制定服务

我会是全国团体标准信息平台注册发布单位，具有全国团体标准发布资格，并与全国信息安全标准化技术委员会建立了长期合作关系。我会依据国家法规政策与地方发展需要，根据市场需求，可为各会员单位提供各类网络安全相关标准化制定、发布与推广服务。

五 资质认证

1、ISO 体系类
2、CCRC 信息安全服务资质
3、ITSS 运维服务能力评估
4、CS 信息系统建设及服务能力评估
5、CMMI 软件研发能力成熟度
6、DCMM 数据管理能力成熟度
7、知识产权
8、软件测试

六 人才服务

1、网络信息安全技能培训及认证
2、网络信息安全师资培训及认证
3、CISP 注册信息安全专业人员
4、CISSP（ISC）^{2} 注册信息系统安全师
5、CCSSP 国际注册云安全系统认证专家
6、CISM 注册信息安全经理
7、CSSLP（ISC）^{2} 注册软件生命周期安全师
8、中级高级职称
9、八大员
10、承接类定制专业网络安全培养培训工作

七 咨询服务

我会建有拥有全市最大最全的网络安全高级专家智库，长期为各级主管部门提供智力支撑。可承接网络安全领域各类的课题研究、政策与法律咨询工作。

八 网络安全宣传与会务服务

我会长期参与组织历年省市“国家网络安全宣传周”系列宣传活动，主办承办了各类各级别专业性论坛、赛事等大型活动。拥有丰富的活动策划与组织经验和专业团队。

武汉市网络安全协会入会指南

在武汉市委网信办主管下，作为唯一代表全市网络安全产业的专业性社团法人，“武汉市网络安全协会”积极发挥好政府与企业间的桥梁纽带作用，全面推进全市网络安全工作，服务网安各领域企事业单位，得到了主管部门和广大网安企业的广泛认可。

武汉网安协会将继续规范办会，以服务会员为中心，积极谋划主动作为，带动上下游产业链，开展形式多样的学习交流等活动，协助主管部门推动全市网络安全与信息化建设，向全国推介“武汉网络安全”集体品牌，助力武汉网络产业健康发展。

为了更好地发挥协会职能，凝聚更多的网络安全优秀企事业单位，我会诚邀贵单位积极加入到“武汉网络安全”的大家庭中来，凝心聚力，共谋产业升级，助力武汉崛起，为武汉网络安全产业健康发展贡献我们的集体智慧和力量！

入会基本条件

依据我会《章程》规定，我会会员分为单位会员和个人会员，入会基本条件如下：

一、在武汉市注册的企事业法人单位、具有武汉市户籍或长期居住的专业人士。

外地企业在汉分公司或办事处机构，需提交驻汉相关证明，协会需实地考察实际经营情况，非武汉户籍个人入会需提供本地工作或长期居住证明。

二、从事以下某项或多项领域的单位和专业人士：

1. 物理安全：环境安全（灾备防护等）、设备安全（设备防毁、电磁屏蔽、防电磁干扰等）、介质安全（介质数据安全等）；

2. 主机安全：身份识别（电子 / 生物信息鉴 别）、主机防护（可信计算、入侵检测、访问控制等）、防恶意代码（病毒防治等）、操作系统安全；

3. 网络安全：通信安全（通信鉴权、保密等）、网络监测（入侵检测、网络监测）；

4. 边界安全：内容安全（内容过滤与控制、防泄漏）边界安全、边界隔离、入侵防范、边界访问控制（防火墙、安全路由器等、网络终端安全（接入控制等）

5. 应用安全：应用服务安全、应用服务安全支持；

6. 数据安全：数据平台安全（安全数据库、数据库安全部件等）、备份与恢复；

7. 安全管理与支持：综合审计、应急响应支持、密码支持（密钥管理）、风险评估、安全管理（安全产品管理平台、安全监控等）、等保测评、网络安全运行维护；

8. 工业信息安全：应用工业互联网的工业企业、工业互联网平台企业、工业互联网基础设施运营企业及专业人士；

9. 从事网络安全和信息化领域相关的信息系统集成、运维服务、科学研究、检验检测、评价评估、人才培养、法律服务、金融服务等方面的专业机构及专业人士；

10. 在网络安全和信息化产业链上下游关系紧密的有关机构和专业人士。

三、单位会员在武汉市有实际经营的独立办公场所，开展正常经营活动超过一年以上时间。个人会员在武汉市从事本专业领域工作超过一年以上时间。

四、单位或个人信用良好，经“信用中国”等国家各级信用平台查询，无违法违规记录。

五、单位会员有专业从事网络信息安全领域的技术人员，个人会员有从事本专业的技术能力并提供相关证明材料。

六、同意协会《章程》，支持并拥护协会相关《公约》、《倡议》、《团体标准》，积极参加协会活动，愿为武汉网络安全产业发展贡献自己力量。

入会流程

一 申请人填写《武汉市网络安全协会入会申请表》提交协会；

二 协会进行入会资格审核；

三 符合入会条件，协会核发《入会通知书》；

四 申请单位或个人按要求提交纸质版材料 1 份，并按规定标准缴纳会费；

五 会籍资料存档，协会颁发会员证书或标牌并公示；

入会联系人：张玉萍　　联系电话：027—85519110　　https://www.whcsa.org.cn

WHCSA
武汉市网络安全协会
Wuhan Cyber Security Association

没有网络安全　就没有国家安全

There is no national security without network security.

公众号二维码　　视频号二维码

地址：武汉市江汉区发展大道 164 号武汉科技大厦 605-1
电话：027—85519110　　网址：www.whcsa.org.cn　　邮箱 :hz@whcsa.org.cn