网安联
Wang An Lian

网络与数据安全治理

FRONTIERS OF REGULATORY OVERSIGHT IN CYBERSECURITY AND DATA GOVERNANCE

前沿洞察（月刊）

2025年5月第5期（总第22期）

2025年5月15日

主办单位：公安部第三研究所网络安全法律研究中心
联合主办：北京网络空间安全协会
牵头组织：网安联秘书处
协办单位：网安联认证中心
技术支持：北京关键信息基础设施安全保护中心
广东关键信息基础设施保护中心

声明：本刊定位于网络与数据安全前沿动态梳理，侧重全面跟踪、及时掌握，如需针对特定领域或前沿动态进行针对性专题研究，请将需求发送至 cinsabj@163.com。

目　录

境内前沿观察一：安全事件

导读：4 月，国家互联网信息办公室发布《中国网络法治发展报告（2024 年）》，从网络法治发展概述、网络立法加快推进、网络执法提质增效等 7 个方面，系统梳理总结 2024 年我国网络法治建设的理念、成就、经验。

中国网络空间安全协会发布《美情报机构利用网络攻击中国大型商用密码产品提供商事件调查报告》指出，2024 年美国情报机构对中国一家大型商用密码产品提供商发动网络攻击，利用客户关系管理系统漏洞入侵并植入木马，窃取客户关系管理系统和代码管理系统中的大量数据，包括客户档案、合同订单以及密码研发项目代码等敏感信息。

国家计算机病毒应急处理中心捕获到针对中国网络用户，特别是财务和税务人员的“银狐”木马病毒变种。该病毒伪装成与税务稽查、所得税汇算清缴、放假安排等相关的诱饵文件，通过社交媒体上的钓鱼链接传播，针对Windows平台用户。一旦运行，用户可能被远程控制、窃取信息、挖矿，甚至被利用作为电信诈骗的跳板。

关键词：商用密码产品；网络攻击；木马病毒

1. 国家互联网信息办公室发布《中国网络法治发展报告（2024 年）》

4 月 27 日，国家互联网信息办公室组织召开发布会，公开发布《中国网络法治发展报告（2024 年）》。

中央网信办副主任、国家网信办副主任杨建文指出，《中国网络法治发展报告（2024 年）》是首部国家部门层面发布的网络法治综合性年度报告，既是《中国网络法治三十年》报告的续篇，也是中国网络法治发展年度报告的开篇，对于充分展现网络法治建设新进展新成效，奋力谱写网络法治建设新篇章具有重要意义。新征程上，加强网络法治建设，要坚守为民初心，凝聚网络法治思想共识；要总结经验规律，夯实网络法治底气信心；要勇于开拓进取，再绘网络法治崭新图景。

司法部党组成员、副部长李明征表示，加强网络法治建设，要突出重点，健全完善网络法律制度体系，强化重点领域、新兴领域法律法规供给；要强化监管，提高网络执法标准化规范化水平，坚决防止违规异地执法和趋利性执法；要加大力度，推动网络法治宣传取得新突破，生动展示新时代全面依法治国实践成就，助力提升广大网民法治素养和全社会法治意识。

《报告》共 5 万余字，分为正文和附录。正文共 7 章，分别从 2024 年中国网络法治发展概述、网络立法加快推进、网络执法提质增效、网络司法持续深化、网络法治宣传教育创新发展、涉外网络法治稳步推进、网络法治建设的形势与展望 7 个方面，系统梳理总结 2024 年我国网络法治建设的理念、成就、经验。附录以大事记的形式，收录了 2024 年中央和地方推进网络法治建设的重点和亮点工作。（来源：网信中国、人民日报）

2. 中国网络空间安全协会发布《美情报机构利用网络攻击中国大型商用密码产品提供商事件调查报告》

4 月 28 日，中国网络空间安全协会发布《美情报机构利用网络攻击中国大型商用密码产品提供商事件调查报告》。

报告显示，2024 年，国家互联网应急中心 CNCERT 发现处置一起美情报机构对中国大型商用密码产品提供商网络攻击事件。该公司利用客户关系管理系统漏洞进行攻击入侵，对两个系统进行攻击并植入特种木马程序。

2024 年 3 月至 9 月，攻击者用 14 个境外跳板 IP 连接特种木马程序并窃取客户关系管理系统中的数据，累计窃取数据量达 950MB。客户关系管理系统中有用户 600 余个，存储客户档案列表 8000 余条，合同订单 1 万余条，合同客户包括我相关政府部门等多个重要单位。攻击者可以查看合同的名称、采购内容、金额等详细信息。2024 年 5 月至 7 月，攻击者用 3 个境外跳板 IP 攻击该公司的代码管理系统，累计窃取数据量达 6.2GB。代码管理系统中有用户 44 个，存储了 3 个密码研发项目的代码等重要信息。（来源：中国网络空间安全协会）

3. 我国境内捕获“银狐”木马病毒变种

4 月 25 日消息，国家计算机病毒应急处理中心和计算机病毒防治技术国家工程实验室近日依托国家计算机病毒协同分析平台（virus.cverc.org.cn）在我国境内连续捕获一系列针对我国网络用户，特别是财务和税务工作人员用户的木马病毒。这些病毒的文件名称与 2025 年“税务稽查”“所得税汇算清缴”“放假安排”等诱饵主题相关，实际为恶意可执行程序，全部针对

Windows 平台用户，主要通过社交媒体中转发的钓鱼网页链接进行传播。经过分析后发现这些病毒均为“银狐”（又名：“游蛇”“谷堕大盗”等）家族木马病毒变种，如果用户运行相关恶意程序文件，将被攻击者实施远程控制、窃密、挖矿等恶意操作，并可能被利用充当进一步实施电信网络诈骗活动的“跳板”。（来源：国家计算机病毒应急处理中心）

境内前沿观察二：政策立法

导读：4 月，数据安全与发展、网络安全等仍是国家和地方政策立法重点关注内容。

中国人民银行、金融监管总局、中国证监会等六部门联合印发《促进和规范金融业数据跨境流动合规指南》，进一步明确数据出境的具体情形及可跨境流动的数据项清单。国家互联网信息办公室发布《数据出境安全管理政策问答（2025 年 4 月）》，指导和帮助数据处理者高效合规开展数据出境活动。国家发展改革委、国家数据局印发《2025 年数字经济发展工作要点》，对 2025 年推进数字经济高质量发展重点工作作出部署，提出加快释放数据要素价值、筑牢数字基础设施底座等重点任务。中央网信办等四部门联合印发《2025 年提升全民数字素养与技能工作要点》，明确工作目标是到 2025 年底，我国全民数字素养与技能发展水平再上新台阶，数字素养与技能培育体系基本建成等。公安部十一局印发《关于对网络安全等级保护有关工作事项进一步说明的函》，强调网络安全等级保护备案原则上由地市级以上公安机关网安部门受理备案。河南省人民政府办公厅印发《河南省数据要素市场培育行动方案（2025—2027 年）》，围绕数据基础制度创新行动、数据开发利用提升行动等方面展开。江苏省国家密码管理局发布《行政执法事项目录（2025 年版）》明确江苏省密码管理部门的行政处罚和行政检查事项。

关键词：数据跨境流动；数字素养；网络安全等级保护；密码管理

（一）部委层面动向

1. 中国人民银行等六部门联合印发《促进和规范金融业数据跨境流动合规指南》

4 月 17 日消息，中国人民银行、金融监管总局、中国证监会等六部门近日联合印发《促进和规范金融业数据跨境流动合规指南》，进一步明确数据出境的具体情形，以及可跨境流动的数据项清单。

《指南》针对跨境支付、跨境汇款、跨境开户、跨境购物等，明确了免予申报数据出境安全评估、订立个人信息出境标准合同、通过个人信息保护认证的数据出境情形。对无法免于数据跨境相关合规义务，但基于实际情况又存在数据出境需求的，梳理形成了常见金融业务场景 60 余项。

《指南》充分衔接现行法律法规、金融管理部门要求，要求金融机构采取必要的数据安全保护管理和技术措施，切实保障数据安全。（来源：金融时报、新华社）

2. 国家互联网信息办公室发布数据出境安全管理政策问答

4 月 9 日，国家互联网信息办公室发布《数据出境安全管理政策问答（2025 年 4 月）》，指导和帮助数据处理者高效合规开展数据出境活动。《问答》就 9 个方面问题作出回答，包括如何理解中国数据出境安全管理制度设计、如何保证不同自贸试验区制定数据出境负面清单标准的一致性、如何理解和判断个人信息出境必要性等。

在识别重要数据方面，国家互联网信息办公室指出，根据《网络数据安全管理条例》第六十二条规定，重要数据是指特定领域、特定群体、特定区域或者达到一定精度和规模，一旦遭到篡改、破坏、泄露或者非法获取、非法利用，可能直接危害国家安全、经济运行、社会稳定、公共健康和安全的数据。《数据安全技术 数据分类分级规则》（GB/T 43697-2024）附录G《重要数据识别指南》提出了重要数据识别方法。数据处理者可依据相关法律法规、技术标准等识别申报重要数据。

在重要数据出境方面，国家互联网信息办公室指出，对于确需出境的重要数据，法律作了制度上的安排，经数据出境安全评估认为不会危害国家安全和社会公共利益的，可以出境。截至2025年3月，国家互联网信息办公室共完成数据出境安全评估项目298个，其中，44个申报项目涉及重要数据，评估结果为不通过的7个，不通过率为15.9%；44个申报项目涉及509个重要数据项，评估后准予出境的重要数据项为325个，占申报数据项总数的63.9%。《促进和规范数据跨境流动规定》明确，数据处理者按照相关规定申报重要数据，未被相关部门、地区告知或者公开发布为重要数据的，数据处理者不需要作为重要数据申报数据出境安全评估。（来源：网信中国）

3. 国家发展改革委、国家数据局印发《2025年数字经济工作要点》

4月15日消息，国家发展改革委、国家数据局近日印发《2025年数字经济发展工作要点》，对2025年推进数字经济高质量发展重点工作作出部署，提出7个方面重点任务。

一是加快释放数据要素价值。以数据要素市场化配置改革为主线，加快完善数据产权、全国一体化数据市场等数据基础制度，配合开展基层报表数据“只报一次”试点，推进数据资源整合共享，组织开展企业、行业、城市三类可信数据空间创新发展试点，以公共数据为突破口深化数据资源有序开发利用。

二是筑牢数字基础设施底座。统筹“东数西算”工程与城市算力建设，以全国一体化算力网建设优化算力资源布局，推动建设国家数据基础设施，加快统一目录标识、统一身份登记、统一接口要求等标准规范建设，抓好隐私计算、区块链等数据流通利用基础设施先试先行。

三是提升数字经济核心竞争力。促进科技创新和产业创新深度融合，梯次培育布局具有国际竞争力、区域支柱型、区域特色型数字产业集群，推动数据产业、数据标注产业高质量发展，支持人工智能技术创新和产业应用。

四是推动实体经济和数字经济深度融合。实施数字消费提升行动、品质电商培育行动，打造数智化消费新场景。深入实施数字化转型工程，协同构建技术模式和商业模式，“一链一策”推进重点行业数字化转型，探索金融、文旅、医疗等领域数字化赋能路径，搭建转型公共服务平台，培育数字化转型服务商。

五是促进平台经济规范健康发展。支持平台企业创新发展，强化灵活就业和新就业形态劳动者权益保障，鼓励平台企业开辟新的就业空间。

六是加强数字经济国际合作。加快发展数字贸易，推进海外智慧物流平台建设，促进跨境电商发展，拓展“丝路电商”合作空间，高质量组织2025年上海合作组织峰会数字经济论坛，探索数据跨境流动管理新模式。

七是完善促进数字经济发展体制机制。深化适数化改革，加大财税金融等综合性政策支持力度，优化高等学校数字经济领域学科设置、人才培养模式。（来源：国家数据局）

4. 国家发展改革委等三部门联合发布《市场准入负面清单（2025年版）》

4月16日，国家发展改革委、商务部、市场监管总局联合发布《市场准入负面清单（2025年版）》。相比2022年版清单，2025年版清单事项数量由117项缩减至106项，减少了11项。

市场准入负面清单分为禁止和许可两类事项。对禁止准入事项，经营主体不得进入，政府依法不予审批、核准，不予办理有关手续；对许可准入事项，地方各级政府要公开法律法规依据、技术标准、许可要求、办理流程、办理时限，制定市场准入服务规程，由经营主体按照规定的条件和方式合规进入；对市场准入负面清单以外的行业、领域、业务等，各类经营主体皆可依法平等进入。

在互联网市场准入禁止许可方面，《清单》提出2项禁止准入事项以及5项许可进入事项。禁止准入事项中，《清单》提出，一是禁止违规开展互联网相关经营活动，包括禁止个人在互联网上发布危险物品信息、禁止特殊医学用途配方食品中特定全营养配方食品进行网络交易等；二是禁

止违规开展新闻传媒相关业务，包括禁止非公有资本从事新闻采编播发业务、禁止非公有资本引进境外主体发布的新闻等。

许可进入事项中，《清单》提出，一是未获得许可，不得从事互联网信息传输和信息服务；二是未获得许可，不得从事互联网中介和商务服务；三是未获得许可，不得从事网络视听节目服务或互联网文化娱乐服务；四是未获得许可，不得从事互联网游戏服务；五是未经认证检测，不得销售或提供网络关键设备和网络安全专用产品。（来源：国务院、新华网）

5. 国家互联网信息办公室等七部门联合发布《终端设备直连卫星服务管理规定》

4 月 23 日，国家互联网信息办公室、国家发展和改革委员会、工业和信息化部、公安部、海关总署、国家市场监督管理总局、国家广播电视总局联合发布《终端设备直连卫星服务管理规定》。

《规定》明确，向中华人民共和国境内提供终端设备直连卫星服务，终端设备接入境内公用电信网和在境内使用无线电频率的，应当依照《电信条例》《无线电管理条例》等的规定，取得相关许可和核准。

《规定》要求，终端设备直连卫星服务提供者依照《网络安全法》《数据安全法》《个人信息保护法》和《密码法》等法律法规的规定和国家标准的强制性要求，履行网络安全、数据安全和个人信息保护义务，落实网络安全等级保护、通信网络安全防护、数据分类分级保护和商用密码应用安全性评估等制度，采取必要措施保障数据和个人信息安全。（来源：中国网信）

6. 中央网信办等四部门印发《2025 年提升全民数字素养与技能工作要点》

4 月 27 日消息，中央网信办、教育部、工业和信息化部、人力资源社会保障部近日联合印发《2025 年提升全民数字素养与技能工作要点》。

《工作要点》明确了工作目标：到 2025 年底，我国全民数字素养与技能发展水平再上新台阶，数字素养与技能培育体系基本建成，数字资源供给能力显著增强，数字人才队伍进一步壮大，劳动者数字工作能力明显提高，群体间数字技能鸿沟不断缩小，数字发展环境更加普惠包容，数字生活智慧便捷，网络空间安全有序，数字法治道德伦理水平持续提升。

《工作要点》部署了 6 个方面 16 项重点任务。一是健全数字人才培育体系，包括培养复合型人工智能人才、完善高水平人才培育体系、壮大应用型技能人才队伍、增强劳动者数字工作能力。二是拓展数字经济增长空间，包括释放数字消费潜力、激发企业数字动能。三是构建普惠包容数字社会，包括推进数字助老助残行动、促进教学资源开放共享、实施数字公益志愿项目。四是打造智慧便捷数字生活，包括强化人工智能应用赋能、丰富新型数字应用场景。五是营造安全有序数字环境，包括健全人工智能治理机制、强化法治道德规范意识、筑牢网络安全防护屏障。六是完善协同联动工作格局，包括深化多方协作机制、加强国际交流合作。（来源：网信中国）

7. 公安部十一局印发《关于对网络安全等级保护有关工作事项进一步说明的函》

4 月 27 日，公安部十一局印发《关于对网络安全等级保护有关工作事项进一步说明的函》，针对网络安全等级保护有关工作事项进一步研究细化，做出具体说明。

文件指出，运营者需全面梳理已备案系统的情况，对于已完成定级备案的第二级（含）以上网络系统，无论网络系统是否涉及级别变更，运营者均需重新依据 2025 版定级报告和备案表模板进行编写和填报，并及时按照属地公安机关网安部门要求及时报送。

文件强调，网络安全等级保护备案原则上由地市级以上公安机关网安部门受理备案。省级公安机关可以根据实际情况，指定具有受理备案条件的县级公安机关受理备案。备案单位工商注册登记地、实际业务运营机构所在地、安全管理机构所在地、网络设备所在地等不一致的，以备案单位安全管理机构、运维所在地为主受理备案。若安全管理机构和运维所在地等不一致的，以安全管理机构所在地为主受理备案。

文件提出，《网络安全等级保护备案证明》有效期为三年。2025 年 1 月 1 日前备案的，有效期自 2025 年 1 月 1 日起算。完成等级测评后有效期自动延长一年。期满需要延期的，应当于期满前三个月内向受理备案的公安机关申请延期。（来源：关键信息基础设施安全保护联盟）

8. 司法部办公厅印发《行政检查文书基本格式文本（试行）》

4 月 30 日消息，为贯彻落实党中央、国务院关于开展规范涉企执法专项行动的决策部署，根据《国务院办公厅关于严格规范涉企行政检查的意见》，司法部办公厅近日印发《行政检查文书基本格式文本（试行）》（以下简称《基本格式文本（试行）》），对涉企行政检查文书基本格式作出了规范。

《基本格式文本（试行）》由司法部编制，由扉页、前言、说明、目录、正文和注意事项等部分组成，各地区、各部门可以结合实际进一步完善，但不得违法改变法定程序，不得违法减损被检查人权益，不得违法增加被检查人义务。有关地区、部门已经制定的行政检查文书格式文本，在包含本基本格式文本关键要素且不相抵触的情况下，可以继续使用。

《基本格式文本（试行）》对行政检查文书的一些共性要求作了简要阐释，便于各地区、各部门理解掌握、参照适用，主要涉及基本格式文本的适用范围、文书的基本结构、审批程序、填写规范、编号要求、被检查人确认、送达方式，以及多个部门联合检查时有关文书的使用要求等。注意事项附在每份文书之后，对《国务院办公厅关于严格规范涉企行政检查的意见》执行中的个别问题作了进一步明确，既是对行政执法人员填写各种文书的具体要求，也是对适用行政检查规定的指导。

同时，《基本格式文本（试行）》包括《行政检查审批表》《行政检查通知书》《行政检查情况记录表》等覆盖行政检查主要环节的七种文书。其中，《行政检查审批表》《行政检查通知书》《行政检查情况记录表》是行政检查过程中的必备文书，《回避申请决定书》《抽样（采样）通知

书》《现场检查（勘验）笔录》《询问笔录》根据实际情况选用。行政检查实践中需要使用其他文书的，由各地区、各部门根据实际情况制作使用。（来源：司法部）

9. 全国数据标准化技术委员会秘书处发布《可信数据空间技术架构（征求意见稿）》

4 月 18 日，全国数据标准化技术委员会秘书处发布《可信数据空间技术架构（征求意见稿）》。征求意见稿规范了可信数据空间技术架构，明确可信数据空间在国家数据基础设施中的定位，可信数据空间的核心技术特征、最小功能集合以及关键业务流程，适用于地方数据基础设施试点及可信数据空间试点的规划、建设和运营、管理。

可信数据空间是基于共识规则，联接多方主体，实现数据资源共享共用的一种数据流通利用基础设施，以数字合约、使用控制技术为核心，以数据跨主体流通使用的可信（符合预期）为目标。通过数字合约技术描述特定参与方对数据内容、使用方式、使用次数等流通利用行为预期并达成共识；通过集成在特定软硬件环境中的使用控制技术对算法、应用进行控制和审计，实现数据访问、分析、计算等行为的管控，保证数据的流通利用过程符合预期。（来源：数字科技和基础设施建设司）

（二）地方层面动向

1. 河南省人民政府办公厅印发《河南省数据要素市场培育行动方案（2025—2027 年）》

4 月 13 日，河南省人民政府办公厅印发《河南省数据要素市场培育行动方案（2025—2027 年）》，围绕数据基础制度创新行动、数据开发利用提升行动、数据市场需求激活行动等八个方面，共提出 28 项任务。

数据基础制度创新行动方面，《方案》提出完善数据领域司法保障体系。推动加快河南省数据条例立法进程，明确数据归集、开发利用、流通交易、安全保护等方面要求，促进数据要素依法有序流动。支持郑州等具备条件的城市设立数据资源法庭，推进数据采集存储、开发利用、流通交易等全生命周期争议案件刑事、民事、行政集中归口审理，完善数据领域司法保障体系。

数据开发利用提升行动方面，《方案》提出强化数据资源管理。开展全省数据资源统计调查，摸清数据资源底数。建立一体化登记制度和数据登记服务体系，明确登记对象、登记内容、登记程序、凭证发放等规则，统筹开展数据产权、数据资源、数据产品等登记管理。深化公共数据治理，推动实现“一数一源”，加快建立全省一体化公共数据资源体系。鼓励企业设立首席数据官，提升企业数据治理能力。

数据要素安全治理行动方面，《方案》提出健全数据安全治理机制。制定加强数据安全保障体系建设意见，明确各类数据安全保护范围、主体、责任和措施，完善数据分级分类、开发利用、流通交易等安全治理原则和具体细则。建立健全数据联管联治机制，完善数据安全风险评估、信息共享、监测预警和应急处置机制，强化分行业监管和跨行业协同监管。加强

合规激励，推广数据合规自愿性认证和信用承诺制度。（来源：河南政府网）

2. 江苏省国家密码管理局发布《行政执法事项目录（2025 年版）》

4 月 30 日，江苏省国家密码管理局发布《行政执法事项目录（2025 年版）》，共十四项行政执法事项，涉及八项行政处罚、六项行政检查。

行政处罚方面，江苏省省、市、县三级密码管理部门开展对商用密码检测机构违反有关规定开展商用密码检测认证的处罚、对未经认定从事电子政务电子认证服务的处罚、对电子认证服务机构违反有关规定使用密码的处罚等。

行政检查方面，江苏省省、市、县三级密码管理部门开展对商用密码活动的监督检查、对商用密码检测机构的监督检查、对电子政务电子认证服务活动的监督检查等。（来源：江苏省国家密码管理局）

境内前沿观察三：治理实践

导读：4 月，公安、网信、通信管理部门等机构持续发力，对网络空间安全进行全方位、多层次治理，旨在提升网络安全防护能力，构建更加安全的网络空间。

公安机关方面，公安部网安局分别公布 10 起涉民生等领域网络谣言案件，10 起涉敏感案事件等领域网络谣言案件，10 起涉险情、疫情、警情等领域谣言案件。黑龙江省哈尔滨市公安局公开悬赏通缉 3 名实施亚冬会网络攻击的美国特工。浙江警方破获一起“网络水军”刷单案，打掉“网络水军”团伙 1 个抓获犯罪嫌疑人 15 人缴获作案手机、电脑 60 余部涉案资金流水高达 3000 余万元。山东、甘肃、福建、山西发布非法获取计算机信息系统数据罪、侵犯公民个人信息罪。

网信部门方面，中央网信办秘书局印发《关于开展“清朗·整治短视频领域恶意营销乱象”专项行动的通知》，部署开展专项行动。本次专项行动重点聚焦：恶意虚假摆拍、散布虚假信息、违背公序良俗、违规引流营销等 4 类问题。上海市委网信办会同市公安局、市市场监管局、上海互联网应急中心，对属地短视频类、生活服务类、论坛社交类等 12 家网站平台开展专项检查，指导整改工作。网信部门会同体育主管部门持续加大对网上体育饭圈问题治理力度，依法严惩拉踩引战和攻击谩骂等行为。网信部门今年以来持续强化未成年人网络保护，持续清理利用未成年人形象发布的违法不良信息，多批次从严处置违规账号。

通信管理部门方面，工业和信息化部信息通信管理局组织第三方检测机构进行抽查，共发现52款APP及SDK存在侵害用户权益行为。山东省通信管理局对山东省各类APP进行合规性检测，对违规APP书面要求限期整改。安徽省通信管理局对省内APP进行拨测检查，发现24款APP存在违法违规收集使用个人信息的问题，要求限期完成整改工作。上海市通信管理局组织第三方检测机构对上海市移动互联网应用程序进行抽查，共发现5款APP及小程序存在侵害用户权益行为。浙江省通信管理局组织第三方检测机构对群众关注的网络社区、网上购物、实用工具等类型APP进行检查，要求违规APP开发运营者限期整改。

安徽省检察院上线人工智能辅助办案系统。该系统是全国检察机关首个全省上线使用，利用基础性、主干性智能化基座研发的人工智能辅助办案系统。市场监管总局部署开展整治滥用行政权力排除、限制竞争专项行动，整治重点包括限制企业自主迁移、阻碍商品要素自由流动、妨碍企业公平参与异地经营、设置地方保护和市场分割隐性门槛四大类突出问题。

关键词：网络谣言；个人信息保护；恶意营销乱象

（一）公安机关治理实践

1. 公安部网安局公布 10 起涉民生等领域网络谣言案件

4 月 17 日，公安机关公布 10 起涉民生等领域网络谣言案件：

一是孙某刚编造传播“河南焦作多县将合村并镇”谣言案。近日，河南公安网安部门查明，孙某刚（男，48 岁）为吸粉引流，在某短视频平台发布“河南焦作沁阳市、孟州市、博爱县、温县、修武县、武陟县将合村并镇”的谣言信息，引发当地网民关注、讨论，严重误导网民。

二是王某超编造传播“许昌将投资 10 亿建 3 个机场”谣言案。近日，河南公安网安部门查明，王某超（男，41 岁）为吸粉引流，在某短视频平台发布“许昌将建设禹州、襄城、鄢陵 3 个机场，其中禹州通用机场具体位置在朱阁镇下宋村，项目总投资 10 个亿，计划占地 1000 亩”的谣言信息，引发当地网民关注、讨论，扰乱公共秩序。

三是梁某成编造传播“四川三奥雪山‘解封’”谣言案。近日，四川公安网安部门查明，梁某成（男，20 岁）为吸粉引流，在互联网平台发布“4.1 解封冲顶倒计时|川西奥太娜 4800 米云端挑战全攻略”的谣言信息，引发大量网民关注、讨论，给广大户外活动爱好者和户外俱乐部带来了误解与困扰，给当地文旅部门正常工作造成影响。

四是张某宝、沙某浩编造传播“安徽明光市地铁已经动工”谣言案。近日，安徽公安网安部门查明，张某宝（男，58 岁）、沙某浩（男，36 岁）分别在短视频平台发布“明光地铁已开始动工”“明光到滁州的地铁正在修建中”

的谣言信息，引发大量网民关注、讨论，造成网民对该市的交通建设和规划的误读，扰乱公共秩序。

五是童某海编造传播“重庆全日制本科十年直接认定副高”谣言案。近日，重庆公安网安部门查明，童某海（男，38 岁）在某短视频平台发布“重庆全日制本科十年直接认定副高”的谣言信息，引发大量网民关注，影响职称评定工作正常开展，扰乱公共秩序。

六是某公司发布“海关将对进口煤炭实施延迟检查”谣言案。近日，北京公安网安部门查明，某科技有限公司在互联网平台发布“4 月 1 日起，多地海关将加强对进口煤的检查，或将导致通关时间延长，进口量减少的可能性进一步加大”的谣言信息，引发大量网民关注、讨论，引起业界担忧，属地公安机关已对公司负责人依法处理。

七是孙某强编造传播“杭州外省家庭无门槛就读”谣言案。近日，浙江公安网安部门查明，孙某强（男，32 岁），为杭州某教育信息技术有限公司负责人，为吸粉引流，在某短视频平台发布“外省家长带娃来杭州可无门槛上公办学校”“为条件不足人员办理社保退休”“为外地人员办理上海落户”等谣言信息，引发大量网民关注，造成网民对杭州教育政策产生误解，误导网民带孩子来杭州读公办学校。

八是刘某哲编造传播“暴雨后许昌满目疮痍”谣言案。近日，河南公安网安部门查明，刘某哲（男，20 岁）利用人工智能工具，自动生成并在某网络平台发布了“许昌暴雨人们惊慌失措，四处奔逃”“暴雨过后，许昌满目疮痍”的谣言信息，引发大量网民关注、讨论，造成社会恐慌，扰乱公共秩序。

九是朱某珍编造传播“大米涨价，快去抢米”谣言案。近日，安徽公安网安部门查明，朱某珍（女，50 岁）为吸引眼球，在某短视频平台发布“赶紧去抢米，米涨价了”的谣言信息，造成网民恐慌、囤积大米，扰乱公共秩序。

十是律某雪、逄某峰编造传播“某餐饮企业后厨检查出艾滋病”谣言案。近日，吉林公安网安部门查明，律某雪（女、38 岁）、逄某峰（男，38 岁）先后在互联网群组发布“徐家地锅鸡体检，后厨一个人检查出了艾滋病了”“@所有人，徐家地锅鸡不能吃了，他家厨师检查出来 HIV”的谣言信息，引发大量网民关注和担忧，严重影响相关餐饮企业正常经营。（来源：公安部网安局）

2. 公安部网安局公布 10 起涉敏感案事件等领域网络谣言案件

4 月 18 日，公安机关公布 10 起涉敏感案事件等领域网络谣言案件：

一是顾某庆编造传播“山西一火车与汽车相撞”谣言案。近日，河南公安网安部门查明，顾某庆（男，59 岁）为吸粉引流，将某短视频平台上一段“火车撞上老年车”视频与某搜索引擎上“火车撞老年车”的相关新闻进行移花接木，在某短视频平台发布“3 月 4 日山西晋城一名女司机驾车抢越铁路道口被火车撞上，晋煤集团铁运工作人员告诉记者‘当时火车拉了 59 节车皮不能马上制动，将轿车往前推行 200 米才停下，所幸事故未造成人员伤亡’”的谣言信息，引发大量网民关注、讨论，引起网民对该公司煤炭外运安全生产的误解，扰乱公共秩序。

二是铁某某编造传播“观影途中女子出轨”谣言案。近日，四川公安网安部门查明，铁某某（男，27 岁）为吸粉引流，在某短视频平台发布“2 月 8

日西昌太平洋电影院 7 排 2 座穿蓝色风大衣黑色头发看哪吒的兄弟，你在中途出去的那十来分钟左右，你的女朋友亲了你的兄弟，他们笑得很开心，希望你能看见”的谣言信息，引发大量网民关注、讨论，铁某某发布虚假信息后，自导自演使用小号再次作“伪证”发布不实评论，并称要当网红博取流量赚钱，该行为严重扰乱公共秩序。

三是张某凌摆拍捏造“钓鱼钓到手雷”谣言案。近日，四川公安网安部门查明，张某凌（男，32 岁）为博人眼球，自导自演“钓鱼钓到疑似手雷”的短视频，并在某短视频平台发布，引发大量网民关注、讨论，扰乱公共秩序。经属地公安机关专业探测、现场甄别，确定该物品为模型，无药块、无雷管、无爆炸的可能，后按规定将该手雷模型进行销毁处理。

四是吴某亮移花接木，编造传播“3 名学生骑 1 辆摩托致 1 死”谣言案。近日，四川公安网安部门查明，吴某亮（男，26 岁）为吸粉引流，将一篇“某地三名初中生发生车祸一人死亡”的公开报道移花接木，编造事发地在绵阳，发布在某短视频平台，并配文“绵阳三名初中生发生车祸一人死亡”，引发大量网民关注、讨论，扰乱公共秩序。

五是覃某、刘某利用人工智能工具编造“郑州公交车司机无证驾驶”等谣言案。近日，河南公安网安部门查明，覃某（男，25 岁）为博取眼球，吸引流量，利用某 AI 工具编辑“郑州公交司机无证驾驶”“科目二代考”等谣言信息，在某网络平台发布；刘洋（男，33 岁）为吸粉引流，利用某 AI 工具编辑生成“郑州公交车祸造成几人轻伤”等谣言信息，在某网络平台发布。上述 2 条谣言引发大量网民关注、讨论，对郑州公交公司正常运营产生影响，扰乱公共秩序。

六是李某某编造传播“山西一工厂燃气管道爆炸”谣言案。近日，山西公安网安部门查明，李某某（男，47 岁）出于猎奇心理，在某短视频平台发布多张河津市宏达钢铁有限责任公司的照片，并配以“河津一工厂燃气管道爆炸”的虚假信息后发布。引发大量网民关注、讨论，对相关工厂正常运营造成影响。

七是唐某编造传播“成都艾滋病患者已达十万”谣言案。近日，四川公安网安部门查明，唐某（男，30 岁）与网民石某产生矛盾，为泄私愤，在某短视频平台编造“网民石某长期以来通过成都外调资源群等各种大量外调渠道平台发布照片信息等，使成都大量女性客户群体遭受艾滋病传播，并有梅毒等性病”“成都艾滋病已达十万数据，千万小心”的不实信息，引发大量网民关注、讨论，造成当地居民恐慌，扰乱公共秩序。

八是东某某编造传播“三江源国家公园工作人员放恶犬围捕雪豹致其瘫痪”谣言案。近日，青海公安网安部门查明，东某某（男，31 岁）为博人眼球，将互联网上一段牧羊犬驱赶雪豹的视频与三江源国家公园工作人员救助受伤雪豹幼崽的视频进行拼接，并配以“雪豹 VS 藏獒”文字后在某短视频平台，引发大量网民关注，造成网民对三江源国家公园动物救护工作的误解，影响正常工作开展。目前，小雪豹经过救治，生命体征平稳，各项身体机能正在恢复。

九是任某文编造传播“漂流小孩哥大闹幼儿园和小学”等谣言案。近日，河北公安网安部门查明，任某文（女,29 岁）无中生有、乱贴标签、博取流量，将网上关于“10 岁‘赤岭亮哥’孤身海钓 海上漂流一天一夜获救”的信息

转发至自己的短视频平台，捏造“智斗人贩子”“大闹幼儿园和小学”等谣言信息，引发大量网民关注，扰乱公共秩序。

十是刘某编造传播“上海地铁不招聘上海户籍员工”谣言案。近日，上海公安网安部门查明，刘某（男,49 岁）为某人力资源有限公司员工，编辑制作上海地铁招聘海报，并自行添加了“非沪籍”的招工门槛要求后，在多个网络群组发布称“招聘非本市户籍地铁安检员”，造成该谣言信息传播，导致网民对招聘政策产生误解，影响相关单位正常招聘工作开展。

以上人员均已被依法追究法律责任。（来源：公安部网安局）

3. 公安部网安局公布 10 起涉险情、疫情、警情等领域谣言案件

4 月 19 日，公安机关公布 10 起涉险情、疫情、警情等领域谣言案件：

一是李某普编造传播“河南发生 4.3 级地震”谣言案。近日，河南公安网安部门查明，李某普（男，30 岁）在某社交平台发布“2 月 22 日凌晨 3 时 17 分，河南省淅川县发生 4.3 级地震，震源深度 10 千米，地震发生时，南阳、洛阳、郑州等多地居民被震醒”的谣言信息，引发大量网民关注、议论，造成多地居民恐慌，扰乱公共秩序。

二是王某勇编造传播“四川凉山一烟囱引发大规模火灾造成人员伤亡”谣言案。近日，四川公安网安部门查明，王某勇（男，25 岁）为吸粉引流，在某互联网平台发布称“四川省凉山州，一座高耸的烟囱由于长期未进行维护和刷漆，表面严重腐蚀，最终引发了大规模火灾，造成人员伤亡”的谣言信息，引发大量网民关注、议论，造成当地居民恐慌，扰乱公共秩序。

三是刘某编造传播“新疆拜城县5.4级地震‘3人死亡65户房屋受损’”谣言案。近日，新疆公安网安部门查明，刘某（男，48岁）为博人眼球，在某短视频平台发布“新疆拜城县发生5.4级地震已致3人死亡，65户房屋不同程度损伤”的谣言信息，引发大量网民关注、议论，造成当地居民恐慌，扰乱公共秩序。

四是王某利编造传播“天津滨海新区海水倒灌”谣言案。近日，天津公安网安部门查明，王某利（男，58岁）为吸粉引流，在多个互联网平台发布“3月4日天津滨海新区曹妃甸滨海大道发生海水倒灌”的谣言信息，引发大量网民关注、议论，造成当地居民恐慌，扰乱公共秩序。

五是冯某远编造传播“重庆发生3.0级地震有人员伤亡”谣言案。近日，重庆公安网安部门查明，冯某远（男，68岁）为吸粉引流，在某短视频平台发布“重庆市石柱县发生地震”的谣言信息，引发大量网民关注、议论，造成当地居民恐慌，扰乱公共秩序。

六是任某编造传播“黑恶势力拐卖致3人死亡”谣言案。近日，山西公安网安部门查明，任某（男，58岁）为吸粉引流，将网络中的一段视频进行编辑，并配以“山西省大同市浑源县人(李大红)，犯有黑势力组织者，拐卖妇女致死3人”文字后，在某短视频平台发布，该谣言信息发出后引发大量网民关注、议论，扰乱公共秩序。

七是李某君编造传播“南充一小学生被人用迷魂药迷倒”谣言案。2025年3月17日10时，西充公安接报一起小学生张某失踪警情，属地公安机关立即开展搜寻工作，于当日15时在南台花园将张某找到。后经查实系张某因作业问题怕被老师责备，独自躲在南台花园逃避上学。四川公安网安

部门查明，李某君（女，59 岁）系警方寻找张某期间的现场围观群众，李某在未确认实际情况的前提下，在某短视频平台发布“有小学生被人用迷魂药迷倒，扔在楼上”的虚假警情，引发大量网民关注、议论，引起当地网民对治安状况的担忧。

八是丁某某、黄某某等人编造传播“河北一女孩被活埋”谣言案。近日，河北公安网安部门查明，丁某某为博人眼球，在某短视频平台发布“河北一女孩被活埋”的虚假警情后，黄某某为吸粉引流，转发该视频，并编造“河北出事了，一个叫谭悦晴的小女孩没了，被活埋了，小脚被两个大人打断了，发生事件 2025.2.23 日”的虚假警情，渲染恐慌情绪，引发大量网民关注、议论，扰乱公共秩序。

九是刘某楠编造传播“烟台发生 1 人当场昏迷,14 人轻度呼吸困难事件”谣言案。近日，山东公安网安部门查明，刘某楠（女，36 岁）为博人眼球、达到对自己店铺虚假宣传的目的，在某短视频平台发布“重磅消息！！15 人在龙口奥莱仓抢夺尺码，导致 1 人当场昏迷，另外 14 人轻度呼吸困难，天降之祸”一条涉及群体公共安全的谣言信息，引发大量网民关注、议论，扰乱公共秩序。

十是张某瑞编造传播“重庆万象城倒闭”谣言案。近日，重庆公安网安部门查明，张某瑞（男，35 岁）在某互联网平台发布“重庆万象城快倒闭关门”的谣言信息，引发大量当地居民关注、议论和误解，严重影响相关企业正常运营，扰乱公共秩序。

以上人员均已被依法追究法律责任。（来源：公安部网安局）

4. 黑龙江省哈尔滨市公安局公开悬赏通缉 3 名对我实施亚冬会网络攻击的美国特工

4 月 3 日，国家计算机病毒应急处理中心发布“2025 年哈尔滨第九届亚冬会”赛事信息系统及黑龙江省内关键信息基础设施遭境外网络攻击情况监测分析报告。

报告指出，赛事期间，各赛事信息系统、黑龙江省域范围内的关键信息基础设施遭到来自境外的大量网络攻击。攻击源大部分来自美国、荷兰等国家和地区。此次遭受的网络攻击以 Web 攻击为主，具体包括文件读取漏洞攻击、SQL 注入攻击、HTTP 协议头 X-Forwarded-For 字段伪造攻击等。

4 月 15 日，黑龙江省哈尔滨市公安局公开悬赏通缉 3 名实施亚冬会网络攻击的美国特工。经查，美国国家安全局特定入侵行动办公室凯瑟琳·威尔逊、罗伯特·思内尔、斯蒂芬·约翰逊等 3 名特工，参与实施了上述网络攻击活动。同时，调查显示该 3 名特工曾多次对我国关键信息基础设施实施网络攻击，并参与对华为公司等企业的网络攻击活动。为依法严厉打击境外势力对我国网攻窃密犯罪，哈尔滨市公安局决定对上述 3 名犯罪嫌疑人进行悬赏通缉。（来源：国家计算机病毒应急处理中心、央视新闻）

5. 山东警方依法打击 1 起非法获取计算机信息系统数据案

4 月 7 日消息，公安网安部门近日侦破一起非法获取计算机信息系统数据案，犯罪嫌疑人非法获取两万余条学生个人信息，后利用人工智能技术向其中的两千余名学生发送骚扰短信。

犯罪嫌疑人胡某是一名在校大学生，非法入侵学校某系统并获取两万余条该校学生个人信息。为寻求刺激、炫耀技术，胡某通过之前发现的某小程序存在的技术漏洞，利用人工智能编写程序，把其中盗取的上千余名学生的手机号码在该小程序上批量注册账户，后将短信验证码篡改为淫秽内容发送至学生本人，对其进行短信骚扰。目前，犯罪嫌疑人对非法获取计算机信息系统数据罪供认不讳，案件正在进一步侦办中。（来源：公安部网安局）

6. 因内容审核缺位，某网站被责令停更整改

4 月 12 日消息，山西公安网安部门近日联合属地网信部门依法约谈整改某违规“资源网”。

经查,该网站长期放任用户以“楼中楼”形式夹带发布一些非法网址信息,以“福利”“资源”等为噱头，诱导用户搜索下载非法应用程序，暗藏软色情信息、木马程序及赌博广告，严重危害网络安全。

核查发现，网站负责人马某自网站注册以来，未建立任何内容审核机制，疏于管理。公安机关当即责令暂停网站服务，下发限期整改通知书，要求全面清理违规内容、切断联网，并建立发布审核制度。调查显示，此类“擦边球”链接不仅污染网络环境,更易引发财产损失与隐私泄漏风险。部分链接通过诱导下载非法应用，实施违法犯罪活动。（来源：公安部网安局）

7. 浙江警方破获一起“网络水军”刷单案

4 月 22 日消息，浙江警方近日破获一起“网络水军”刷单案，打掉“网络水军”团伙 1 个抓获犯罪嫌疑人 15 人缴获作案手机、电脑 60 余部（台）涉案资金流水高达 3000 余万元，实现对刷单炒信类“网络水军”犯罪行为的全链条打击。

2024 年 4 月，云和公安接到报案称某网络购物平台上存在同类型的电商刷单行为，构成恶意竞争。案件受理后云和公安第一时间组织警力展开调查。

经查，自 2024 年以来，犯罪嫌疑人范某某等人以非法牟利为目的开发“云创助手”“易评助手”“星评助手”“创优助手”等刷单软件搭建后台服务器购买大量电商平台账号，招募何某某、余某某等人组建刷单工作室，以虚假交易的方式有偿为电商商家提供更高的商业排名、信用度和用户访问量。

在掌握大量犯罪事实和证据后，云和公安网安部门迅速组织警力开展统一收网行动成功，一举打掉以范某某、何某某为首的刷单“网络水军”犯罪链条。经调查，该团伙为 5000 余家商户提供了刷单业务，遍及 20 个省份，累计刷单 2000 万余条虚假评论、点赞 4000 万余条，极大危害网购环境及市场经济秩序。

同时，公安机关还对刷单商户、电商平台开展工作，将案件相关情况通报属地公安机关及市场监管部门，使其他商家不敢刷、不能刷、不想刷，让诚信回归，推动电商市场步入规范健康发展轨道。（来源：公安部网安局）

8. 甘肃公安常态化开展网络“三俗”内容专项治理

4 月 23 日消息，甘肃公安机关网安部门按照公安厅党委部署要求，常态化开展网络“三俗”内容专项治理。今年以来共发现“三俗”信息 910 余条，约谈 326 人，行政处罚 41 人，串联案件线索 130 条，刑事打击 31 人，中断直播 210 次。（来源：甘肃网警）

9. 福建警方发布一起涉非法获取计算机信息系统数据典型案例

4 月 25 日消息，福建警方近日发布一起涉非法获取计算机信息系统数据典型案例。

裘某某在日常工作中偶然发现某科技有限公司开发的两款 App 软件存在后门漏洞，后裘某某伙同林某某通过破解软件获取到内部秘钥，非法调用后台数据获利。该公司在发现后台数据异常后立即报警，当地公安机关迅速开展调查。目前，2 名犯罪嫌疑人已被公安机关缉捕归案。经审查，二人非法获取企业上货链接数据 2000 余万条，涉案金额 10 余万元。（来源：公安部网安局）

10. 山西警方发布一起侵犯公民个人信息典型案例

4 月 26 日消息，山西警方近日发布一起侵犯公民个人信息典型案例。

山西省忻州市公安局网安部门工作中发现，辖区人员薛某某长期通过某即时通讯工具组建网络群组，搜集公民手机号码及验证码，批量注册账号提供给他人，并从中非法获利达 3.7 万余元。目前，薛某某已被属地公安

机关依法采取刑事强制措施，其名下作案手机被扣押。案件正在进一步侦办中。（来源：公安部网安局）

11. 甘肃警方发布一起侵犯公民个人信息典型案例

4 月 27 日消息，甘肃警方近日发布一起侵犯公民个人信息典型案例。

刘某鹏制作开发黑客软件“刘某控”,该软件通过传播植入木马程序实现计算机端远程控制。团伙成员刘某山、刘某昊、刘某等人将“刘某控”打包伪装，通过通讯软件投送至受害人电脑，在受害人点击伪装文件后木马病毒立即激活，即可对受害人电脑进行远程控制，刘某昊、刘某 2 人使用“刘某控”非法控制他人计算机并窃取公民信息牟利。

2023 年 6 月，刘某鹏团伙被公安机关抓获归案，查获非法获取公民信息一批。2024 年 9 月，法院依法对刘某鹏等犯罪团伙人员分别以提供侵入、非法控制计算机信息系统程序、工具罪和非法控制计算机信息系统罪、侵犯公民个人信息罪分别判处有期徒刑并处罚金。（来源：公安部网安局）

（二）网信部门治理实践

1. 中央网信办部署开展“清朗·整治短视频领域恶意营销乱象”专项行动

4 月 8 日，中央网信办秘书局印发《关于开展“清朗·整治短视频领域恶意营销乱象”专项行动的通知》，部署开展专项行动。本次专项行动重点聚焦 4 类问题：

一是恶意虚假摆拍问题。打造悲惨人设，假冒新就业群体身份，虚构“苦情”戏，利用公众善意卖惨营销。通过自我包装、作秀等手段，编造“社会名流”“成功人士”等虚假人设和情节，虚夸“爽剧”经历，收割流量牟取利益。打着“助农”“扶贫”名义，编造悲情剧本引流敛财。打造低俗恶俗人设，摆拍编造打架斗殴、谩骂吐脏、无底线骚扰等低俗恶俗内容。

二是散布虚假信息问题。以“剪切拼凑”“断章取义”“故意模糊时间地点”“冒用身份”等方式恶意制造不实信息。编造、夸大渲染家庭矛盾、职场冲突、暴力案事件，制造社会焦虑、网络戾气，挑动群体对立。利用“换脸”“换声”“P 图”等手段编造不实内容。假借“科普”“解读”名义，或假冒、“碰瓷”权威机构、专家学者，恶意编造、散布涉经济、法律、历史、医学等专业领域虚假信息。

三是违背公序良俗问题。以“户外搭讪”“街头采访”等方式尾随陌生路人进行语言、肢体骚扰，或在互动交流中以“撩妹”“相亲”“求吻”等话题为噱头，诱导受访者口述隐晦色情内容。在短视频标题、配文中故意关联低俗、“软色情”字眼或话题，在短视频内容中突出呈现低俗声音、暴露着装、诱惑动作等，刻意制造性暗示、性挑逗氛围诱导用户低俗互动。

四是违规引流营销问题。利用“情感交流”“国学文化”“中医养生”“快速致富”等噱头，诱骗老年人等特定群体非理性消费。使用“揭露行业秘密”“曝光行业内幕”“举报行业骗局”“我被行业封杀”等夸张、煽情的“标题党”文案博眼球吸粉引流。打着“网络打假”“维权斗士”等旗号发布虚假“打假”“测评”“探店”内容，误导用户对相关品牌形象、商品质量、服务水平认知。（来源：网信中国）

2. 网信部门牵头开展打击网上体育“饭圈”问题行动

4 月 2 日消息，网信部门近日会同体育主管部门持续加大对网上体育饭圈问题治理力度，依法严惩拉踩引战和攻击谩骂等行为，清理违法违规信息 160 万余条，处置账号 7.6 万个，其中关闭账号 3767 个。重点包括：一是严打挑动互撕、引战的“大粉”“粉头”账号；二是惩处编造谣言、恶意炒作的“自媒体”账号；三是清理冒用运动员名义的账号群组；四是查处一批违规售卖涉运动员商品的商家店铺；五是及时处置存在不良导向的产品功能；六是强化线上线下联动处置工作。（来源：中国网信）

3. 网信部门依法查处一批低俗炒作娱乐明星信息账号

4 月 7 日消息，网信部门近日持续打击文娱领域“饭圈”乱象，督促网站平台依法依约关闭和长期禁言处置一批低俗炒作绯闻丑闻八卦的违法违规账号。

一段时间以来，相关账号通过偷拍、跟拍明星非公开行程，发布未经核实的“爆料”信息；或以“知情人”名义编造、转发不实信息，或借“标题党”和虚假预告等形式，制造噱头，恶意博取流量；或使用暗语、隐喻等手段，无底线炒作明星八卦信息，严重破坏网络生态。

网信部门将继续压实网站平台主体责任，督促严格落实《网络信息内容生态治理规定》《关于进一步加强娱乐明星网上信息规范相关工作的通知》等要求，聚焦泛娱乐化倾向和低俗炒作现象，坚决整治流量至上和“饭圈”乱象，加大网络执法力度，努力营造积极向上的网络环境。同时，欢迎广大网民积极参与监督举报，共同营造清朗网络空间。（来源：中国网信）

4. 网信部门持续整治利用未成年人形象不当牟利问题

4 月 18 日消息，网信部门今年以来持续强化未成年人网络保护，根据日常管理和网民举报线索，持续清理利用未成年人形象发布的违法不良信息，多批次从严处置违规账号。通过压实平台主体责任，网信部门指导平台加大违规线索摸排打击力度，累计对 1.1 万余个违规账号采取禁言、取消营利权限、关闭等处置措施。

典型问题有：一是恶搞儿童、博取眼球。包括用道具刀假装砍儿童肢体，制造“万万没想到”场景；在孩子身上扔食物、乱涂画，进行所谓“惩罚教育”。二是虚假摆拍、制造争议。部分账号摆拍亲子冲突剧情，让未成年人演绎分手、相亲感悟，教唆孩子模仿成人抽烟。三是不当言行、歪曲导向。在部分短视频中，未成年人频繁展示奢侈品开箱或巨额现金场景，进行网络炫富。有视频打着揭露批判、警示教育的名义，刻意让未成年人演绎不当行为、作出危险动作，发布同质化文案渲染炒作，造成不良示范。四是违规引流、规避打击。部分账号以“举牌”售卖所谓定制图片、发布定制舞蹈等名义，引流添加好友，通过“一对一”交流等隐蔽形式传播低俗色情内容。（来源：网信中国）

（三）通信管理部门治理实践

1. 工信部、山东、安徽、上海等部省通信管理局发布侵害用户权益 APP/SDK 名单

（1）工信部

4 月 21 日消息，工业和信息化部信息通信管理局近日组织第三方检测机构进行抽查，共发现 52 款 APP 及 SDK 存在侵害用户权益行为。上述 APP 及 SDK 应按有关规定进行整改，整改落实不到位的，工业和信息化部信息通信管理局将依法依规组织开展相关处置工作。（来源：工业和信息化部信息通信管理局）

（2）山东

4 月 3 日消息，山东省通信管理局近日对山东省各类 APP 进行合规性检测，对违规 APP 书面要求限期整改。截至 4 月 3 日，有 12 款存在问题并被通知限期整改的 APP 未按要求在限期内完成整改。4 月 11 日前，上述 12 款 APP 开发运营者务必完成整改与情况反馈工作。如再次逾期仍未整改到位，山东省通信管理局将视情采取下架、关停、行政处罚等措施。

此外，1 月 20 日，山东省通信管理局向社会公开通报了 15 款经检测发现存在侵害用户权益和安全隐患问题且下发整改通知书后未在规定时限完成整改的 APP，并再次要求限期整改。截至再次要求的规定时限，仍有 4 款 APP 未完成整改反馈。为维护用户合法权益，依法严肃处理 APP 违规行为，山东省通信管理局决定对上述 4 款 APP 予以下架。（来源：山东省通信管理局）

（3）安徽

4 月 7 日消息，安徽省通信管理局近日对省内 APP 进行拨测检查，检测发现 24 款 APP 存在违法违规收集使用个人信息的问题，2025 年 3 月 4 日对上述违规 APP 企业下达责令改正通知书，要求限期完成整改工作。截至 4 月 7 日，尚有 5 款 APP 未完成问题整改，相关 APP 企业应在 2025 年

4 月 11 日前落实整改要求。逾期不整改的，安徽省通信管理局将依法依规组织开展相关处置工作。（来源：安徽省通信管理局）

（4）上海

4 月 11 日消息，上海市通信管理局近日组织第三方检测机构对上海市移动互联网应用程序进行抽查，共发现 5 款 APP 及小程序存在侵害用户权益行为。上述 APP 及小程序应按有关规定在 4 月 19 日前落实整改工作。整改落实不到位的，上海市通信管理局将依法依规组织开展处置工作。（来源：上海通信圈）

（5）浙江

4 月 21 日消息，浙江省通信管理局近日组织第三方检测机构对群众关注的网络社区、网上购物、实用工具等类型 APP 进行检查，书面要求违规 APP 开发运营者限期整改。截至 4 月 21 日，尚有 13 款 APP 未按要求完成整改。上述 APP 开发运营者在 4 月 27 日前完成整改落实工作，整改落实不到位的，浙江省通信管理局将视情采取下架、关停、行政处罚等措施。（来源：浙江省通信管理局）

（四）其他部门治理实践

1. 安徽省检察院上线人工智能辅助办案系统

4 月 6 日消息，安徽省检察院近日上线人工智能辅助办案系统。该系统是全国检察机关首个全省上线使用，利用基础性、主干性智能化基座研发

的人工智能辅助办案系统。安徽省检察院组织研发人工智能辅助办案系统，开始在全省 79 家检察院试用。（来源：安徽检察）

2. 市场监管总局部署开展整治滥用行政权力排除、限制竞争专项行动

4 月 15 日消息，市场监管总局近日部署开展整治滥用行政权力排除、限制竞争专项行动。专项行动的整治重点包括限制企业自主迁移、阻碍商品要素自由流动、妨碍企业公平参与异地经营、设置地方保护和市场分割隐性门槛四大类突出问题。通过开展专项行动，集中查处一批重点案件，推动修订废除一批妨碍全国统一市场和公平竞争的政策措施，着力解决人民群众和经营主体关心关切的滥用行政权力排除、限制竞争突出问题，支持各类企业在公平竞争中成长壮大，服务经济社会高质量发展。

专项行动要求各地拓宽问题线索收集渠道，深化与企业常态化沟通交流，加强线索闭环管理。将执法办案作为主线，依法依规处理有关问题线索，严查快处违法案件。积极运用多种方式，强化惩戒约束和警示效果，形成有力的执法震慑。市场监管总局将突出加大对重大案件的督办和查办力度，确保专项行动取得实效。（来源：国家市场监督管理总局）

境内观察四：人工智能安全专题

导读：4 月，中共中央政治局就加强人工智能发展和监管进行第二十次集体学习。中共中央总书记习近平在主持学习时强调，面对新一代人工智能技术快速演进的新形势，要充分发挥新型举国体制优势，坚持自立自强，突出应用导向，推动我国人工智能朝着有益、安全、公平方向健康有序发展。

中国气象局、国家互联网信息办公室联合发布《人工智能气象应用服务办法》。《办法》提出，发展人工智能气象应用服务应当坚持总体国家安全观，统筹发展和安全，将促进创新和依法治理相结合等。

国家互联网信息办公室发布《关于发布生成式人工智能服务已备案信息的公告（2025 年 1 月至 3 月）》。截至 2025 年 3 月 31 日，共有 346 款生成式人工智能服务在国家网信办完成备案等。

北京市经济和信息化局印发《北京市关于支持信息软件企业加强人工智能应用服务能力行动方案（2025 年）》。方案提出：支持 MaaS 企业在京集聚发展、提升数据治理能力、加速构建开源生态新体系等多项措施。

湖北警方查处一起利用人工智能工具编造虚假信息案，涉案公司为提高所运营网站的流量，购买一个人工智能写作软件，通过输入自设的关键词，由系统自动抓取网络信息生成文章。该公司发布文章前未按规定对发布内容履行审核责任。公安机关根据相关法律法规，对涉事公司予以行政处罚。

关键词：人工智能发展；人工智能气象应用；人工智能编造虚假信息

1. 习近平强调坚持自立自强、突出应用导向、推动人工智能健康有序发展

4 月 25 日，中共中央政治局就加强人工智能发展和监管进行第二十次集体学习。中共中央总书记习近平在主持学习时强调，面对新一代人工智能技术快速演进的新形势，要充分发挥新型举国体制优势，坚持自立自强，突出应用导向，推动我国人工智能朝着有益、安全、公平方向健康有序发展。

习近平指出，人工智能作为引领新一轮科技革命和产业变革的战略性技术，深刻改变人类生产生活方式。党中央高度重视人工智能发展，近年来完善顶层设计、加强工作部署，推动我国人工智能综合实力整体性、系统性跃升。同时，在基础理论、关键核心技术等方面还存在短板弱项。要正视差距、加倍努力，全面推进人工智能科技创新、产业发展和赋能应用，完善人工智能监管体制机制，牢牢掌握人工智能发展和治理主动权。

习近平强调，人工智能领域要占领先机、赢得优势，必须在基础理论、方法、工具等方面取得突破。要持续加强基础研究，集中力量攻克高端芯片、基础软件等核心技术，构建自主可控、协同运行的人工智能基础软硬件系统。以人工智能引领科研范式变革，加速各领域科技创新突破。

习近平指出，我国数据资源丰富，产业体系完备，应用场景广阔，市场空间巨大。要推动人工智能科技创新与产业创新深度融合，构建企业主导的产学研用协同创新体系，助力传统产业改造升级，开辟战略性新兴产业和未来产业发展新赛道。统筹推进算力基础设施建设，深化数据资源开发利用和开放共享。

习近平强调，人工智能作为新技术新领域，政策支持很重要。要综合运用知识产权、财政税收、政府采购、设施开放等政策，做好科技金融文章。推进人工智能全学段教育和全社会通识教育，源源不断培养高素质人才。完善人工智能科研保障、职业支持和人才评价机制，为各类人才施展才华搭建平台、创造条件。

习近平指出，人工智能带来前所未有发展机遇，也带来前所未遇风险挑战。要把握人工智能发展趋势和规律，加紧制定完善相关法律法规、政策制度、应用规范、伦理准则，构建技术监测、风险预警、应急响应体系，确保人工智能安全、可靠、可控。

习近平强调，人工智能可以是造福人类的国际公共产品。要广泛开展人工智能国际合作，帮助“全球南方”国家加强技术能力建设，为弥合全球智能鸿沟作出中国贡献。推动各方加强发展战略、治理规则、技术标准的对接协调，早日形成具有广泛共识的全球治理框架和标准规范。（来源：新华社）

2. 中国气象局、国家网信办联合发布《人工智能气象应用服务办法》

4 月 23 日，中国气象局、国家互联网信息办公室联合发布《人工智能气象应用服务办法》，自 2025 年 6 月 1 日起施行。《办法》共五章二十九条，包括支持与促进、应用服务规范、监督管理等内容。

《办法》提出，发展人工智能气象应用服务应当坚持总体国家安全观，统筹发展和安全，将促进创新和依法治理相结合，对人工智能气象应用服务实行包容审慎和分类分级监管。

《办法》围绕数据开放、算法模型研发和应用场景赋能等提出了具体政策支持和促进措施，加强人工智能与气象监测预警、预报预测、数值预报等领域深度融合应用，构建人工智能气象应用服务场景。同时对气象主管机构参与国际气象领域人工智能应用服务的发展和治理做出了规定。

《办法》明确人工智能气象应用服务提供者的权利和义务，规定了算法备案和安全评估、人工智能生成合成内容标识、算法安全审核、网络安全、数据安全、信息发布审核、投诉举报等制度。（来源：网信中国、中国气象局）

3. 国家互联网信息办公室发布《关于发布生成式人工智能服务已备案信息的公告（2025 年 1 月至 3 月）》

4 月 8 日，国家互联网信息办公室发布《关于发布生成式人工智能服务已备案信息的公告（2025 年 1 月至 3 月）》。截至 2025 年 3 月 31 日，共有 346 款生成式人工智能服务在国家网信办完成备案；对于通过 API 接口或其他方式直接调用已备案模型能力的生成式人工智能应用或功能，共有 159 款生成式人工智能应用或功能在地方网信办完成登记。（来源：网信中国）

4. 北京市经济和信息化局印发《北京市关于支持信息软件企业加强人工智能应用服务能力行动方案（2025 年）》

4 月 8 日，北京市经济和信息化局印发《北京市关于支持信息软件企业加强人工智能应用服务能力行动方案（2025 年）》，提出八项措施。

《方案》提出支持 MaaS 企业在京集聚发展。支持云服务和大模型厂商等搭建全栈式 MaaS 平台，提升规模化服务能力。建立可量化的 MaaS 平台动态指标跟踪和评价机制，对达到一定服务规模的 MaaS 平台给予算力券支持，降低 MaaS 平台在算力匹配、大模型调用、数据治理等方面成本。利用全球数字经济大会、中国国际服务贸易交易会和中关村论坛等科技创新交流合作平台，发布 MaaS 平台实践案例，加大推广力度。

《方案》提出提升数据治理能力。发挥信息软件企业的行业知识优势，瞄准人工智能应用需求，支持信息软件企业开展 DCMM（数据管理能力成熟度评估模型）贯标评估，推动信息软件企业牵头创建行业数据采集实验室，开展智能化标注平台、数据治理平台、数据合规流通平台等建设，形成并发布一批行业语料库。

《方案》提出加速构建开源生态新体系。利用开源软件已形成的资源优势，建设服务全国的人工智能开源平台，并给予配套支持。打造人工智能国际开源社区，支持基于开源平台开展大模型商业化应用，吸引人工智能开源组织落地并实施共享开源项目，建立基于人工智能开源贡献的评价和激励机制。（来源：北京市经济和信息化局）

5. 湖北警方查处一起利用人工智能工具编造虚假信息案

4 月 20 日消息，湖北警方近日查处一起利用人工智能工具编造虚假信息案。

湖北警方工作中发现，某资讯网站发布的文章严重失实。网警及时取证，并与网站所属公司取得联系，通过法治教育，该公司迅速删除了不实文章。据查，该公司为提高所运营网站的流量，购买了一个人工智能写作软件，通过输入自设的关键词，由系统自动抓取网络信息生成文章。涉案文章系人工智能机械拼接多地文本而成，该公司发布前未按规定对发布内容履行审核责任。公安机关根据相关法律法规，对涉事公司予以行政处罚。目前，涉事公司已在网站首页公开致歉声明，下架全部人工智能生成内容，并在公司内进行整改。（来源：公安部网安局）

五、境外前沿观察：月度速览十则

导读：4 月，境外国家和地区在人工智能、网络安全、数据安全等方面的政策法律和热点事件持续发生。

人工智能方面，欧盟委员会发布《人工智能大陆行动计划》，旨在将欧盟打造为全球人工智能领域的领导者。美国众议院美中战略竞争特别委员会发布报告，称中国 DeepSeek 模型构成对美国的国家安全威胁。英国地方政府协会等机构共同发布相关指南，指导政府部门负责任采购人工智能产品。德国汉堡数据保护与信息自由事务专员呼吁 Meta 用户及时对 Meta 行使拒绝权，从而保护其社交平台个人信息不被用于人工智能训练。

网络安全方面，英国政府发布《网络安全与韧性法案》的政策声明，介绍法案的立法意图、政策背景及拟议的核心措施。美国众议院通过《删除法案》，旨在把发布未经同意的私密影像的行为定为犯罪。新加坡网络安全局推出拓展版网络安全认证标志，涵盖云服务、人工智能安全等领域。

数据安全方面，美国总统特朗普签署《延长 TikTok 执行推迟》行政令，宣布将此前针对 TikTok 的《保护美国人免受外国敌对方控制的应用程序法》执行延期宽限至 2025 年 6 月 19 日。美国司法部国家安全司主导的“数据安全计划”正式生效，旨在防止中国、俄罗斯、伊朗和其他外国对手利用商业活动访问和利用美国政府相关数据和美国人的敏感个人数据。欧盟委员会认定苹果公司和 Meta 公司违反《数字市场法》的关键条款，对其分别处以 5 亿和 2 亿欧元罚款。

关键词：人工智能；DeepSeek；深伪色情；数据安全

1. 欧盟委员会发布《人工智能大陆行动计划》

4 月 9 日，欧盟委员会发布《人工智能大陆行动计划》，旨在将欧盟打造为全球人工智能领域的领导者。计划主要内容包括：

一是建设大规模人工智能计算与数据基础设施，2025 年前建立 13 个人工智能工厂，覆盖 17 个欧盟国家及合作伙伴，总投资达 100 亿欧元，配备 9 台新型 AI 超级计算机，算力提升 3 倍。此外，研发下一代人工智能模型，单厂集成超 10 万颗人工智能芯片，通过公私合作建设 5 座千兆工厂等。

二是构建统一的欧洲数据市场，建立“数据实验室”，在人工智能工厂内设立数据实验室，汇聚并整理来自不同来源的大规模高质量数据，支持人工智能模型的训练和验证。

三是启动“应用人工智能战略”，加强人工智能在医疗、制造、公共服务等战略性行业的广泛应用，计划采取以下措施：（1）启动公众咨询，收集利益相关者的意见，识别各行业在采用人工智能技术方面的优先事项和挑战；（2）根据咨询结果，制定具体行动计划，落实提供资金支持、技术指导和政策激励等具体措施，促进人工智能在各行业应用；（3）加强与人工智能工厂和欧洲数字创新中心（EDIHs）的协作，利用现有的人工智能基础设施，支持行业定制化人工智能解决方案的开发和部署等。（来源：欧盟委员会）

2. 英国发布政府部门负责任采购人工智能产品相关指南

4 月 16 日，英国地方政府协会、伦敦技术与创新办公室、平等与人权委员会和信息专员办公室共同发布《如何将平等原则与数据保护融入人工智能委托及采购流程：英格兰各议会指南》。

指南能够帮助相关人员实现：（1）在启动采购或委托流程之前，以及在整个流程中，彻底评估平等影响和数据保护风险，并根据证据做出相关决策；（2）能够自信地向基于人工智能的技术供应商深入询问：在技术开发和测试阶段如何考量平等性及数据保护相关问题；这些考量如何融入后续技术优化过程；以及未来技术迭代中将如何进行持续学习与训练；（3）将平等性原则和数据保护要求系统性地融入招标文件及合同条款设计，确保地方政府在以下三个维度获得必要信息：构建科学合理的采购流程；有效监控技术应用的社会影响；通过合同条款及履约监督机制保障人工智能技术的公平性、合法性和安全性应用；（4）深刻理解相关评估工作具有动态属性。合同存续期间及人工智能技术应用全生命周期内，需持续开展平等性影响及数据保护风险评估。该要求同样适用于合同履行过程中出现技术升级、功能新增或通过合同变更引入人工智能技术等情形。（来源：英国政府）

3. Meta 将使用个人数据训练人工智能，德国监管机构呼吁用户及时行使拒绝权

4 月 15 日，德国汉堡数据保护与信息自由事务专员呼吁 Meta 用户及时对 Meta 行使拒绝权，从而保护其社交平台个人信息不被用于人工智能训练。

近期 Meta 公司宣布，其将自 2025 年 5 月底起，开始使用欧洲地区 Facebook 与 Instagram 成年用户的个人数据训练其人工智能技术。若用户不对此表达反对，则将被视为默认同意 Meta 使用其数据进行人工智能训练。根据相关程序，Meta 将通过 Facebook 与 Instagram 平台通知所有欧洲成年用户，并告知其享有的各项权利。（来源：德国汉堡数据保护与信息自由事务办公室）

4. 特朗普签署行政令，再次推迟执行 TikTok 禁令 75 天

4 月 4 日，美国总统特朗普签署《延长 TikTok 执行推迟》行政令，宣布将此前针对 TikTok 的《保护美国人免受外国敌对方控制的应用程序法》的执行延期宽限至 2025 年 6 月 19 日。

行政令明确，在此期间司法部不得对任何因不遵守该法而产生的行为采取执法行动，也不得对相关企业施加任何处罚。行政令指示司法部长采取一切必要措施，包括发布书面指导以执行本命令并向各相关平台提供书面说明等，确认其在延期期间以及法生效至今的相关行为不构成违法，也无需承担任何责任。

行政令强调，由于 TikTok 案关涉国家安全，《保护美国人免受外国敌对方控制的应用程序法》的执法权归于司法部长，任何州政府或私人团体试图进行执法将构成对联邦行政权的干预。（来源：美国白宫）

5. 英国发布《网络安全与韧性法案》政策声明

4 月 9 日，英国政府发布了《网络安全与韧性法案》的政策声明，介绍法案的立法意图、政策背景，以及拟议的核心措施及适用范围。法案旨在更新 2018 年《网络与信息系统条例》，加强英国关键基础设施和数字服务的网络安全防护能力。法案目前仍处于筹备阶段，计划在 2025 年提交议会审议。

法案将引入以下主要内容：一是将更多实体纳入监管范围，以解决对现代数字基础设施的依赖上升而产生的监管空白问题，确保供应链安全。二是加强监管机构权限，赋予监管机构更强的合规执行能力和可持续监管资源。三是确保法律在面对快速变化的网络安全环境时具备灵活应变的能力。赋予国务大臣新的“授权立法权”，以便政府能快速更新和调整法规，更有效应对新风险、利用技术进步。（来源：英国政府）

6. 美国众议院通过《删除法案》，对“深伪色情”进行监管

4 月 28 日，美国众议院通过《通过阻止网站和网络上技术生成的深度伪造影像来应对已知剥削工具法案》即《删除法案》，并提交美国总统特朗普签署。法案旨在把发布未经同意的私密影像的行为定为犯罪，并要求科技平台在收到删除要求时，48 小时内删除相关内容，否则将被联邦贸易委员会处罚。

法案禁止在满足以下三点的情形下，未经同意发布成年人或未成年人的私密影像：（1）影像在隐私情境下获取；（2）影像是非自愿公开或公众关注内容；（3）意图或实际对成年人造成心理、财务或声誉损害或意图

虐待、性剥削未成年人。此外，对于使用人工智能等技术生成或篡改的私密影像，未经同意发布，且符合上述真实影像条件的行为也被禁止。同时，法案规定以下例外情形：（1）执法或情报机构的合法活动；（2）基于举报、医学用途等的合法目的披露；（3）个人自愿发布（不包括发布包括儿童色情内容）等。

对于违反上述规定的个人主体，最高可被判处 3 年监禁和罚款；未履行相关删除义务的科技平台将被视为“不公平或欺诈行为”,面临调查和处罚。（来源：美国国会）

7. 新加坡网络安全局推出拓展版“网络安全基础”与“网络安全信任”认证标志

4 月 15 日，新加坡网络安全局推出拓展版 “网络安全基础”与“网络安全信任”认证标志，将涵盖云服务、人工智能安全、运营技术安全领域。

此次扩展源于新加坡企业日益广泛地应用超越传统网络安全的数字技术，这也为攻击者开辟更多数字入侵路径。拓展版“网络安全基础”为企业提供针对云服务、人工智能和运营技术安全领域常见网络攻击的防护指南；拓展版“网络安全信任”则在这三个新领域增加了风险评估模板、网络安全准备度审查以及风险处置方案。此举旨在简化新兴技术领域的网络安全要求，助力企业更便捷地落实良好网络安全实践。（来源：新加坡政府）

8. 美国司法部国家安全司主导的“数据安全计划”正式生效

4 月 8 日，美国司法部国家安全司主导的“数据安全计划”正式生效。该计划旨在防止中国、俄罗斯、伊朗和其他外国对手利用商业活动来访问和利用美国政府相关数据和美国人的敏感个人数据，以进行间谍、监视和反间谍活动，并发展人工智能和军事能力或者以其他方式破坏美国国家安全。美国司法部对该计划十分重视，司法部副部长托德·布兰奇强调，对外国对手而言，与其费尽周折发动复杂网络攻击窃取数据，直接从开放市场收购数据或胁迫其管辖企业获取信息显然更具诱惑。数据安全计划将显著提高其获取难度。（来源：美国司法部）

9. 因违反《数字市场法》欧盟对苹果和 Meta 分别处以 5 亿欧元与 2 亿欧元罚款

4 月 23 日，欧盟委员会发布新闻公告，认定美国苹果公司和 Meta 公司违反《数字市场法》的关键条款，对二者分别处以 5 亿欧元和 2 亿欧元罚款。这是欧盟首次就《数字市场法》实施违规裁定，标志着该法的执法进入实质性阶段。根据《数字市场法》规定，所有通过 App Store 分发应用程序的开发者有权向用户告知并引导其访问 App Store 之外的其他优惠购买渠道。然而欧盟委员会调查发现，苹果设置多项限制以阻碍开发者行使此项权利。欧盟委员会认为，这些限制缺乏必要性和比例性，严重妨碍了用户获得更便宜或更合适选择的权利，同时强化了开发者对苹果平台的依赖。

对于 Meta 公司，欧盟委员会调查发现，Meta 自 2023 年 11 月起在欧盟市场实施“同意或付费”广告模式，用户若不同意个性化广告数据使用，需支

付月费以获取无广告版本。欧委会认定此模式未提供“数据最小化的等效选项”，剥夺了用户对个人数据控制的自由选择权。

公告要求苹果与 Meta 需在 60 日内完成整改，否则将面临欧委会每日累计处罚。欧盟委员会表示其将继续与两家公司保持沟通，确保其全面遵守 DMA 的义务与精神。（来源：欧盟委员会）

10. 美中战略竞争特别委员会发布报告，称 DeepSeek 威胁美国

4 月 16 日，美国众议院美中战略竞争特别委员会（Select Committee on the CCP）发布报告《揭露 DeepSeek：暴露中国最新间谍、盗窃和规避美国出口管制工具》，称中国 DeepSeek 模型构成对美国的国家安全威胁。

报告主要内容包括：（1）数据窃取与隐私威胁。DeepSeek 收集美国用户个人数据，包括聊天记录、设备信息及输入习惯，通过后端基础设施传输至中国，受中国《网络安全法》《个人信息保护法》约束；（2）信息操控。DeepSeek 根据中国法律要求，通过自动化过滤和内置偏见，审查输出内容；（3）技术盗用。DeepSeek 通过模型蒸馏技术非法复制美国人工智能模型（如 OpenAI 的模型），以低成本加速其模型开发。OpenAI 向委员会报告，DeepSeek 的 R1 模型表现出与 OpenAI 模型相似的推理结构和短语模式，表明其可能非法复制 OpenAI 技术，违反服务条款；（4）规避出口管制。DeepSeek 使用受美国出口管制限制的英伟达芯片，其中许多通过非法渠道（如新加坡转运）获取。报告批评英伟达设计性能接近管制上限的芯片，以规避出口限制。报告建议加强对中国的出口管制与人工智能风险管

理，跟踪中国人工智能发展动向防止中国人工智能战略突袭。（来源：美国众议院美中战略竞争特别委员会）

行业前沿观察一：高工专栏

导读：全球经济承压，网络空间安全行业却在逆境中崛起。生成式人工智能、低空经济等新兴技术的涌现，为网络安全产业带来新机遇。习近平总书记强调，广大工程技术人员应坚定科技报国理想，推动发展新质生产力。在此背景下，北京网络空间安全协会推出“高工专栏”，以“网络空间安全-新技术、新引擎、新发展”为主题，邀请新晋“网络空间安全专业高级工程师”撰稿。

专栏旨在传播网络安全新技术、新思想和新理念，优秀稿件将在全国范围宣传，并在相关活动中做主题交流。稿件内容可涵盖业务安全、数据安全、信息内容安全及网络与系统安全等方向，需为创新性技术分析文章，字数约 2000 字，个人署名，可配照片。

请于每月 15 日前投稿至 bjcsa@bjcsa.org.cn，审稿通过后，将在本月或下月刊载。

联系人：薛老师

联系方式：17200383428、010-67741727

关键词：人工智能、网络安全、高工专栏、互联网

1. 开源大模型将重塑威胁情报体系和生态——以 DeepSeek 为例阐述大模型对威胁情报的影响

引言：随着随着人工智能技术的快速发展，开源大模型在网络安全领域的应用潜力逐渐显现。DeepSeek 作为一款开源大模型，凭借其强大的自然语言处理、数据理解与推理、内容生成等能力，正在加速威胁情报与大模型的深度融合。其本地化部署能力不仅降低了企业成本，还彻底革新了威胁情报的生产、消费与应用模式。本报告将深入探讨开源大模型如何重塑威胁情报体系与生态，推动威胁情报从“云端集中式”向“云地协同式”转型，并催生新的应用场景与机会。

一、生态重构：从单向消费到参与共建

1.1 传统模式的局限

在传统威胁情报生态中，企业主要作为情报的消费者，依赖情报厂商在云端利用大规模算力进行情报挖掘与加工。尽管这种模式高效，但企业缺乏深度定制能力，难以满足自身特定需求。

1.2 DeepSeek 带来的变革

DeepSeek 的本地化部署为企业提供了低成本、高效率的情报处理能力。企业不再局限于单向消费，而是可以参与情报的二次加工，融入自身业务理解和安全需求，实现情报的深度定制与优化。这种从“消费者”到“共建者”的转变，为威胁情报生态注入了新的活力。

1.3 开源与低门槛的优势

DeepSeek 的开源特性和低硬件门槛使得更多企业能够参与到大模型的情报处理中。企业无需依赖云端的大规模算力与语料支持，即可基于本地业务进行情报加工，推动威胁情报生态向多元化、分布式方向发展。

二、场景进化：从被动防御到智能预防

2.1 传统被动防御的局限

传统本地情报应用主要依赖 IOC（Indicator of Compromise）的机读接入进行自动封堵，属于典型的被动防御模式。这种模式难以应对复杂多变的网络威胁，尤其在未知攻击面前显得捉襟见肘。

2.2 DeepSeek 推动的主动防御

DeepSeek 的自然语言理解和推理能力使得企业能够对情报进行深度分析与预测。通过监测暗网数据泄露、漏洞预警、攻击者技战术分析等多维度情报，企业可以提前发现潜在威胁，主动采取防御措施，实现从“亡羊补牢”到“未雨绸缪”的转变。

2.3 智能预防的新场景

DeepSeek 的引入催生了“半成品情报加工”、“行业定制情报”等新场景。企业可以根据自身需求，对原始情报进行二次加工，生成更具针对性的安全洞察，从而提升防御体系的智能化水平。

三、数据价值更新：从标准化到可塑性强的情报

3.1 传统情报数据的局限

传统情报数据多为标准化、成熟的情报，便于机读与消费，但缺乏灵活性和可塑性。企业在面对复杂威胁时，往往需要更多维度的情报支持，DeepSeek 为首的大模型将彻底改良这一现状。

3.2 DeepSeek 重新定义情报价值

DeepSeek 的本地化应用使得“半成品情报”、“线索情报”等新型数据得以充分利用。例如，专业的技战法分析报告、恶意软件沙箱分析数据等原本难以理解的情报，可以通过 DeepSeek 的智能化处理转化为易用的成品情报，为企业提供更全面的安全洞察。

3.3 情报数据生态的升级

新一代威胁情报平台将支持更多可塑性强的情报数据，如暗网监测情报、勒索组织预警情报、APT 组织技战术情报等。这种升级不仅丰富了情报数据的种类，还提升了其应用价值。

四、精准适配：从通用情报到行业定制

4.1 通用情报的不足

传统威胁情报多为通用化产品，难以满足不同行业的特定需求。企业在使用过程中往往需要花费大量精力进行筛选和适配。

4.2 DeepSeek 驱动的精准化

DeepSeek 的本地化部署使得企业能够根据自身行业特点与业务需求，定制专属情报。例如，从海量情报中自动筛选出与企业相关的内容，实现精准推送与应用。这种精准化不仅提高了情报的易用性，还增强了安全防护的针对性。

4.3 行业定制情报的实践

通过升级新一代威胁情报平台并联动 DeepSeek，企业可以实现智能定制精准适配自身需求的情报，从而有效应对复杂多变的网络安全威胁。

五、理解力升级：从复杂解读到易用洞察

5.1 情报解读的挑战

威胁情报的多维属性往往存在隐含冲突，理解难度较大。例如，一个 CDN IP 地址可能同时具备白名单和恶意域名标识，传统模式下只有经验丰富的分析人员才能解读，DeepSeek 为首的大模型将优化这一现状。

5.2 DeepSeek 提升理解力

DeepSeek 的自然语言处理能力使得复杂情报的解读变得更加简单。企业可以通过本地部署的 DeepSeek，快速理解多维情报数据，降低对专业人员的要求，同时融入行业特色的理解能力。

5.3 情报解读的隐私保障

DeepSeek 的本地化部署还保障了情报查询的隐私性，避免了传统 SaaS 模式下可能存在的信息安全问题。

六、交互革命：人机接口的智能化升级

6.1 传统人机接口的局限

传统情报平台的人机交互方式较为单一，用户需要通过复杂的操作获取所需情报，效率较低。

6.2 DeepSeek 推动的交互革命

DeepSeek 的引入使得情报平台能够实现本地化的情报聊天机器人。用户可以通过自然语言与机器人交互，快速获取所需情报信息，极大地提升了使用便捷性与效率。

6.3 新一代情报平台的特点

新一代情报平台将更加注重人机交互体验，结合 DeepSeek 的能力，提供更智能、更友好的交互方式，满足企业日益增长的情报应用需求。

结论

开源大模型 DeepSeek 的出现为威胁情报领域带来了新的变革机遇。其低成本本地化部署能力推动了威胁情报从“云端集中式”向“云地协同式”转型。通过升级新一代威胁情报平台并联动 DeepSeek，企业可以实现以下目标：

(1)丰富新的情报使用场景；

(2)实现智能提前防御；

(3)应用可塑性强的情报数据；

(4)构建精准适配自身的情报；

(5)提升复杂情报理解能力；

(6)变革情报人机交互接口。

这些变革将大幅提升威胁情报的使用效率与体验，增强企业威胁防御能力，为网络安全生态注入新动力。

展望

未来，随着开源大模型技术的不断进步，威胁情报领域将迎来更多创新与突破。企业应积极拥抱这一趋势，探索大模型在网络安全中的更多应用场景，构建更加智能、灵活的安全防护体系。（作者：郑开发 绿盟科技集团股份有限公司高级工程师）

2. 持续威胁暴露面管理，攻击面管理新范式

前言：全球攻击面正在快速扩大，而且攻击者竭力寻求利用各种安全弱点，尤其当零日弱点被广泛利用的消息传出时，组织通常会感到恐慌，要求 IT 安全团队尽快修补受影响的系统。新的安全形势要求组织将其现有攻击面管理的方法转型为更广泛的持续威胁暴露面管理（CTEM）计划。通过寻找改进的计划和工具、充分利用人工智能技术并采取实施持续威胁暴露面管理 CTEM 计划来降低网络安全风险。要求组织安全管理从简单的安全事件处置转变为更成熟的、具有检测、攻击模拟及响应能力，具备战略规划的预防控制方案。

Gartner 发布的《持续威胁暴露面管理（CTEM）计划》是一种集成的迭代方法，优先考虑潜在的处理方法并不断完善，直到安全态势得以改善。持续开展 CTEM 计划包括五个周期性阶段：确定范围、风险识别、优先级评估、攻击模拟和采取行动，这是一个持续循环的动态过程，组织在 CTEM 计划项目实施中可能会不断重复这五个阶段，以确保不间断地威胁监控与管理，如图 1 所示。

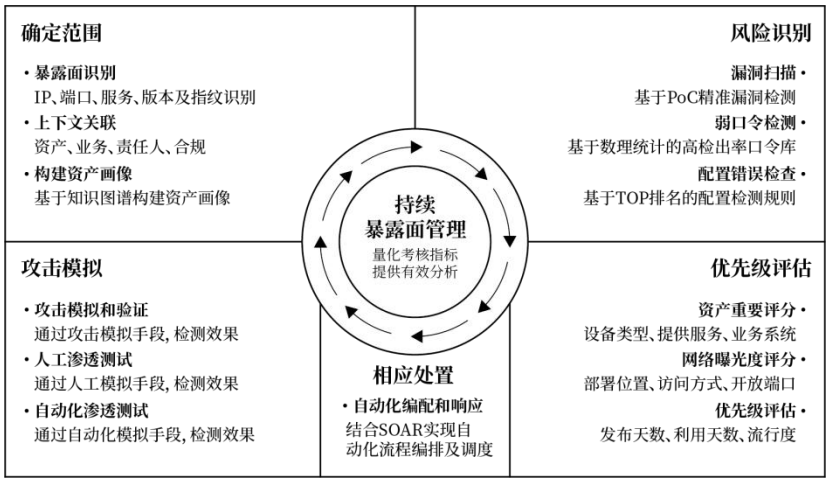


图 1 CTEM 循环

（一）持续威胁暴露面管理概述

传统的方法已无法匹配快速发展的业务需求和不断扩大的攻击面风险。暴露面范围远远超出了传统攻击面覆盖的范围，即便采取基于外部攻击面管理（EASM）、网络资产攻击面管理（CAASM）方案也无法充分覆盖。

新形势下，新的攻击面主要包括如下内容。

1.SaaS 应用程序，作为数字化转型计划的结果，导致组织内攻击面的范围快速增长。员工、组织和客户之间的联系越来越多地通过 SaaS 应用程序和云服务进行，这些应用程序和云服务几乎可以从世界上的任何设备和地点通过互联网进行访问，从而增加了未经授权的用户访问信息或意外发布敏感信息的可能性。

2.另一个增加攻击面风险的因素是物联网设备的使用越来越多。物联网设备可能是家庭和商业应用中增长最快、用途最广泛的技术之一。设备的多样性及其无所不在带来了新安全挑战，例如：用户可以在未经 IT 部门审查或授权的情况下安装它们，这使得维护最新的资产清单变得非常困难。物联网设备导致的暴露面风险包括：固件和软件更新不频繁、设备上运行

的服务不安全、弱密码、不安全的 API、缺乏安全更新机制、使用过时的组件、不安全的信息传输等。

3.影子资产带来的风险，它由用户使用或开发的所有应用程序组成，未经组织的 IT 或安全领域的审查或同意就在网络中使用。用户之所以使用影子 IT 资产，是因为他们认为自己可以更高效地工作，并轻松地与其他员工互动。

“自带或使用自己的设备”等倡议允许员工使用自己的智能手机或电脑；如果没有采取足够的预防措施，就会增加影子 IT 应用程序的使用，这反过来又会增加攻击面，同时也会增加信息泄露和资产管理不一致的可能性。

4.社工信息可在社交网络、深网和暗网资源上获得。泄露的密码和泄露的用户数据可用于有针对地攻击，有针对性地攻击每天都变得越来越频繁。社交媒体上的信息，以及深网和暗网中的数据；使有针对性地攻击对受害者来说更加危险。

总之随着技术环境的复杂化及分散化，无论是在本地还是在云上，并且涉及容器、物联网和网络物理系统，组织攻击面管理的工作压力越来越大；SaaS 应用程序和供应链逐渐形成了新型的攻击面。因此，对于每个组织来讲，需要提高针对内部任何安全体系攻击面威胁可视化，这样才能建立和维持强大的安全态势感知、控制风险的能力。

组织一直在寻找改进的方法论和工具来降低网络安全风险。这包括从单纯的预防方法转变为更成熟的、具有检测及响应能力的战略增强型预防

控制。而现有管理攻击面的方法无法匹配数字化发展速度。CTEM 计划应运而生，它是一种务实且有效的系统化方法论，并可不断优化升级。Gartner 预测，到 2026 年，采用基于 CTEM 计划的组织遭受入侵的可能性将降低 3 倍。CTEM 计划提供了更丰富、更深入的洞察力，可帮助组织主动识别、优先处理和管理意外风险或暴露面。此方法不同于标准威胁风险管理实践，因为它可以响应不断变化的威胁形势。通过这种方式，能够降低攻击的风险，降低攻击者利用弱点的能力，更快地检测和响应攻击，并降低人为错误的风险，最终利用这种新方法来降低攻击的总体风险。

（二）持续威胁暴露面管理计划

Gartner 强调，网络安全的首要目标是降低风险，但预防性工具以及检测和响应解决方案没有跟上数字化转型和不断扩大的攻击面的步伐。尝试修复或补救所有风险是不可行的（近乎不切实际），因此 Gartner 引入了 CTEM 计划作为一种集成方法论，以优先考虑和关注最重要的风险，从而不断完善和改进安全状况。

CTEM 计划是一种集成的迭代方法，优先考虑潜在的处理方法，并不断完善安全态势改进。但是商业风险偏好有时会影响到通过修复和缓解控制的组合来选择网络安全问题的补救措施，将“修复和态势改进”从暴露面管理计划中分离，强调有效改进态势的跨团队要求。同样地，CTEM 计划的运作有特定的时间范围。它遵循治理、风险和合规性的要求，可为长期战略的转变提供参考信息，但在安全运营中心（SOC）团队的威胁检测

和响应活动中，并没有额外的任何限制和要求，日常的安全运营及风险管理计划依旧可以参考图 2。

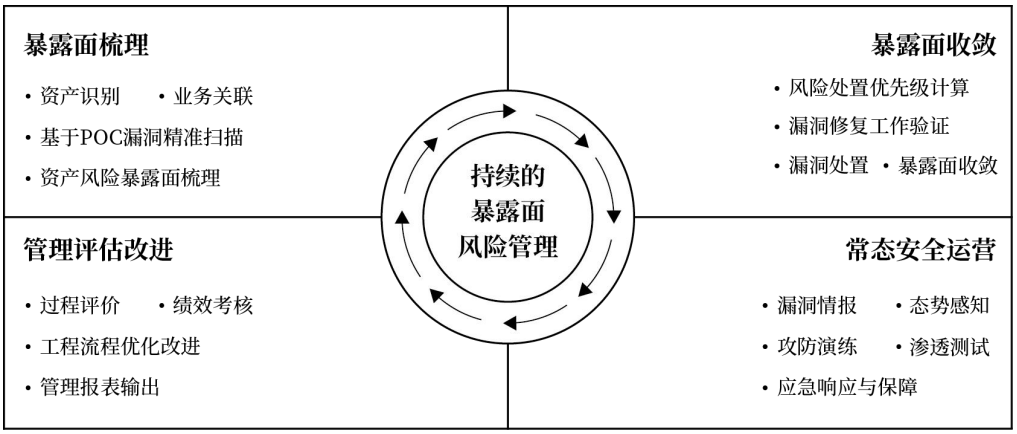


图 2　风险管理

2.1 持续暴露面管理的目标

CTEM 计划是一套流程和方法，使组织能够持续和一致的评估自身数字和物理资产的可访问性、暴露面及可利用性。

CTEM 计划实施周期包括五个步骤：确定范围、发现识别、优先级、攻击模拟和采取行动，这是一个持续的动态循环过程，在 CTEM 计划实施过程中可能会不断重复这五个阶段，以确保不间断地威胁监控与管理，参考图 20-1。

- 确定范围：需要结合业务视角和安全视角，以识别和筛选关键业务资产威胁、高价值资产威胁或敏感资产威胁。
- 发现识别：需要厘清组织的 IT 基础架构、网络、应用程序和敏感数据资产。该阶段旨在发现错误配置、攻击面和缺陷，以便可以根据各自的风险级别进行威胁分类。

- 确定优先级：通过资产和攻击面优先级算法，确定那些最有可能被利用的弱点，并优先处置。低优先级的弱点的修复工作会酌情延后，直到有足够的资源来处置。
- 攻击模拟：主要针对已发现弱点问题进攻攻击模拟测试，以确认风险、检查处置效果。该阶段还用于风险评估。
- 采取行动：是指根据验证阶段的结果对发现的攻击面风险采取纠正措施。采取行动阶段生成有关 CTEM 流程执行的全面数据，促进下一个周期中的流程更高效。

实施 CTEM 计划的组织使用多种弱点扫描工具或攻击面管理平台对资产和攻击面进行清点和分类，通过 BAS 攻击模拟测试工具或自动化渗透测试工具进行评估。实施 CTEM 计划需要为基础设施团队、系统和项目所有者提供有效的、可操作的实践指导，以便对发现的问题采取必要的行动措施。

CTEM 计划是周期性的。各种外部因素，如新的组织结构变更或有时效的攻击技术可能会触发 CTEM 计划流程进入具体操作阶段，但不一定从周期的第一步开始。除了攻击面的优先级和修复外，组织能够在 CTEM 计划阶段中收获正反两方面的教训，从而获得巨大的价值和管理效能提升。

实施 CTEM 计划只是识别和规划解决方案的第一步。它需要进行跨团队的合作并与问责制相结合，需要在参与者间共享评估、跟踪、管理和修复风险的流程。实施 CTEM 计划的优点是可进一步固化可重复的工作流程。

实施 CTEM 计划使修复和安全态势优化超越了传统的利用补丁、签名和安全指导手册的采取行动过程。

2.2 持续暴露面管理的实施准备

实施 CTEM 计划时，主要做如下准备。

1.流程准备：CTEM 计划在组织中的负责团队之间建立了一个持续的流程，以识别风险、确定优先级和验证补救措施，并启用解决方案。

2.数据准备：CTEM 还检查更广泛的暴露面数据，而不是仅依赖于弱点评估工具的输出，还包括 IaaS 环境、SaaS 应用程序和供应链合作伙伴持有的数据等数字资产。这还可以包括一些附加信息，例如成本数据，以确定来自云提供商的未经授权、未知或增加的成本的风险，此外还包括 SaaS 应用程序的安全状况、配置错误、用户权限等。数据准备期间应该细化资产清单，将发现的资产映射到对组织至关重要的服务和资产库中。详细的资产清单中应该包括 IT 管理的基础架构数据以及非直接管理的基础架构数据，如 SaaS 应用程序、影子 IT 应用程序、IoT 设备以及来自外部来源（如深网、暗网）的信息等。

3.改进计划准备：首先需要了解 CTEM 是一项持续实施的改进计划和一种方法论，旨在创建所有组织都能理解的、可操作的安全风险态势改进计划。真正的风险管理计划将系统地、有步骤、可评估的解决关键风险问题（如配置错误或缺少补丁程序），从那些对业务构成最高风险的问题开始。因此，CTEM 计划不是一种具体的技术手段，而是一种运营手段。

2.3 持续暴露面管理的实施流程

CTEM 计划虽然可重复，但受五个核心阶段的制约。为了整体安全态势，每个步骤都执行不同的操作，每个阶段都需要在每次迭代期间重复。CTEM 计划迭代过程是确定资产范围、风险识别、优先级评估、攻击模拟和采取措施，例如实施控制和对策以降低风险和弱点的可能性和影响。计划运行过程中并持续进行风险监控——持续监控组织中可能影响安全态势的变化的因素。

1.确定范围

对于大型组织来说，攻击面的范围超过了传统攻击面管理的范畴，就需要灵活可扩展的数字资产管理功能，包含从传统的设备、应用程序到无形的数字资产（如组织的社交媒体账户、在线代码库和集成供应链系统）。解决这个问题的有效方法是确定初始资产管理范围，并根据项目的进展不断扩展外延。

成熟的攻击面管理项目通常包括对内部、本地、云和自有资产进行初步的初始范围界定。CTEM 计划项目从“攻击者的角度出发”，超越了传统的常见攻击面资产管理平台。

2.风险识别

资产管理范围确定完成后，正确识别资产及风险状概况十分重要，通过安全评估、威胁情报分析和其他手段主动识别风险和弱点。风险识别过程应优先考虑范围界定过程中业务领域的成果。暴露面的发现成果不仅是攻击面，还可以包括资产和安全控制的错误配置及其他缺陷。

为了实现向威胁暴露管理的有效过渡，首先进行风险识别，以确定哪些威胁对您的组织构成最大的风险。一旦知道了这一点，组织就可以制定策略和程序来管理这些威胁的风险，然后实施控制措施来减轻与这些威胁相关的风险，同时采取措施解决任何新的或增加的风险。

3.优先级评估

暴露面管理的目标并不是修复全部已识别问题，而是识别和处理最有可能被利用针对组织进行攻击的威胁因素。组织不能单纯通过预定义的基本严重性评分来对风险进行优先级排序，因为还需考虑补救的紧迫性、暴露程度、资产的关键性、是否有补偿性控制措施、重新计量可能产生的影响和成本等因素。更成熟的组织应该从实施和拓展 CTEM 计划中汲取经验。处理暴露面问题的优先次序需要基于紧迫性、严重性、攻击面的可用性、风险偏好和风险水平进行综合考虑。

识别和修补环境中每个设备和应用程序上的每个漏洞几乎是不可能的，只需要解决正确的问题。漏洞数量惊人，但并不是每个漏洞都是可利用的，并不是每个可利用的漏洞都是威胁参与者的积极目标。专注于重要事项—修补弱点和缓解可能导致重大影响的弱点。实施 CTEM 计划使您将精力和资源集中在减少威胁上。CTEM 利用您现有的基础架构管理和安全工具的强大功能来分析您的环境并自动评估您的风险。通过攻击面管理平台可主动、持续地识别所有攻击路径，以暴露新出现的威胁，并提供优先建议和决策智能，使您能够减轻最严重的风险。

4.攻击模拟

入侵与攻击模拟（Breach and Attack Simulation，BAS）是组织验证潜在攻击者如何实际利用已确定暴露面及安全监测系统进行反应的过程的一部分。攻击模拟是通常在生产环境中使用受控模拟或模仿攻击者的技术。

攻击模拟软件允许您在网络上伪装成坏人，知道坏人如何绕过你的网络工具和安全措施。可以从了解哪些地方容易受到攻击，到实际看到事件响应活动的执行情况。入侵与攻击模拟的好处是，只需点击一个按钮，就可以重放大量攻击。这可以节省渗透测试团队的时间，而不是手动利用活动，手动利用活动必须重复以确认成功的补丁和缓解措施。

入侵与攻击模拟需要实现三个目标：

- 确认攻击者确实可以利用先前发现和优先处理的暴露来评估可能的“攻击成功”数据。
- 分析关键业务资产所有潜在攻击路径，评估“最大潜在影响”。
- 识别响应和修复已识别问题的过程是否足够快，以及是否足以满足业务系统安全需要。

入侵与攻击模拟通常有两种实现方式。

一种是基于代理的方法。安全测试人员会在组织环境中运行数据电脑上安装攻击代理，攻击代理可能会查看它可以泄漏多少未被 DLP 工具阻止的数据。尽管有电子邮件保护解决方案，但攻击代理也可以根据防病毒软件检测到的恶意软件数量、向组织外部发送的敏感电子邮件数量来运行类似的攻击。这些攻击代理也可以放置在服务器上，以确定 Web 应用程序防火墙在阻止攻击方面的有效性。

另外一种基于无代理，主动模拟的方式。模拟软件可以模拟某个人打开包含恶意宏的 Excel 文档，会发生什么情况，记录最初的危害步骤发生后自动执行攻击，可以匹配 ATT&CK 攻击框架，识别每个攻击，查看哪些攻击被捕获，哪些攻击没有被捕获。然后，该模拟工具可以查看组织中应该应用的技术保护措施，分析保护效果，并提供有关如何提高其有效性的建议。比如添加 Windows 组策略来阻止攻击。

5.采取措施

许多成熟的组织缺乏“自动修复”的技术和手段，因为修复处置方案往往仅限于修复、基本威胁检测规则或安全控制的配置变更。完全依赖程序中自动修复的功能存在各种未知因素，因为任何尝试修复的后果，都超出了安全团队的职责范畴，更多要考虑软件业务使用问题。

CTEM 计划中涉及安全工具的建议方案往往是众多解决方案的某一种，建议的解决方案选择，一般只提供部分可用、可阅读、可理解的信息。采取行动的核心工作是确保团队通过减少流程审批、实施过程和缓解部署中的繁琐过程来将 CTEM 计划的调查结果付诸实践。它要求组织定义统一的跨团队审批工作流程，同时还要求组织领导并参与其中。在更高的管理成熟度下，“采取行动”也需要工具的配合，以便更好地整合，使其能够为组织提供更多安全技术支持。

（三）持续威胁暴露面管理的最佳实践

传统理解 IT 基础架构的一种方法是将其想象成一座四周有围墙的城堡，或者是银行的金库，里面有我们想要保护的商品或高价值资产。

针对组织的传统 IT 基础架构，通常会做出以下假设：

- 对基础架构和应用程序进行集中控制。
- 在基础设施的外部和内部资产之间有一个明确定义的边界。
- 必须保护的资产被很好地识别，例如：信息、数据库、内部网络、计算机、应用程序、用户、物理位置。
- 有隔离设备（防火墙、网闸等）或防护设备（WAF、IPS 等），它允许您决定什么进入和离开。
- 有安全区域或网络，在那里你可以放置设备，敏感的数据库等。
- 有定义明确的管理人员，他们可以引入新技术或服务，也可以创建新的应用程序。
- 攻击面可以被视为城墙上的那些薄弱点，这些薄弱点可以从外部被攻击。

现实却大不相同。如今，组织中的攻击面非常复杂，内部和外部资产之间没有明确的界限。资产是不断变化的，并且与服务提供商之间存在相互依赖性。并非 IT 基础架构的所有资产都在 IT 领域的控制之下。仅仅因为一台计算机位于某个网络或网段中，就认为它是安全或可靠的，这是有风险的。

传统的网络安全解决方案强调防御（捕捉和阻止攻击），CTEM 计划则通过强调进攻（发现和修复、缓解问题）来保障安全。CTEM 计划它不是关注攻击类型本身，而是关注攻击路径，像黑客一样思考，想象攻击可能袭击的位置以及它们可能应用的战术和技术。在确定和分析可能的暴露

点后，每个暴露点都会根据其脆弱程度和违规对整个业务造成的损害的严重程度进行风险排名，最后系统地解决关键风险（如配置错误或缺少补丁程序）。组织实施 CTEM 计划时，需要考虑一些最佳实践，以最大限度地减少威胁，并降低安全风险。

最佳实践方法包括以下一些内容：

1.设计并采集更广泛的暴露面的程序，采用更高级的算法，而不是简单地清点和处理来自多个不同攻击面评估工具的评估数据。

2.确保暴露面管理有助于组织安全管理，为安全解决方案设计提供洞察力，丰富安全事件内容提升响应效率，提高组织运营效益，获取高级领导的支持。

3.建立定期的可重复工作流程作为 CTEM 计划的一部分，每个工作流程都遵循五个步骤，从而保证一致的威胁暴露面管理效果。

4.采用攻击面管理和攻击模拟等新兴技术，尤其是攻击模拟（BAS），BAS 是一种主动防御技术，通过模拟攻击者视角，发现攻击者可利用的系统暴露面和渗透路径。使用 BAS 技术，组织可以确认安全防御体系是否正常工作并提供预期的防御力。通过缩小攻击面，解决诸如错误配置、密码/凭证管理和系统弱点等暴露面弱点问题，降低了被攻击的风险。

5.将持续威胁暴露面管理 (CTEM) 与组织级修复和事件工作流程配合，以确保所需的组织内部跨团队协作流程成为标准。

6.充分利用人工智能技术。目前，人工智能技术和自动化技术在检测和管理威胁方面起到了重要作用。人工智能经过训练后，可以迅速检测恶意

软件或恶意网络活动，不仅基于威胁身份来检测，还基于行为模式来检测，可以开发人工智能程序模块来预测潜在攻击。（作者：马维士 北京华云安信息技术有限公司架构师）

3. 基于 Q-learning 的自适应加密算法切换机制研究

摘要：针对传统静态加密技术在动态环境适应性方面存在的策略僵化、上下文感知缺失及密钥管理脆弱性等关键缺陷，本研究提出基于 Q-learning 框架的四层复合状态空间自适应加密决策模型。通过分层整合应用架构层特征参数（包括开发语言范式与加密逻辑植入机制）、网络环境状态变量、安全评估指标及设备资源约束条件，建立覆盖"环境-安全-资源-架构"多维度的状态编码体系，并创新性地引入架构感知因子以优化算法兼容性与工程实施可行性。重点研究构建了基于马尔可夫决策过程的状态空间表征方法与动作空间映射机制，同时针对工程化部署中的性能瓶颈问题，提出了基于动态规划的状态空间压缩策略和基于启发式搜索的动作选择优化方案。

关键词：动态加密体系;Q-learning;自适应数据加密

Abstract: The traditional static encryption techniques suffer from key defects such as rigid strategies, lack of context-awareness, and vulnerabilities in key management, particularly in dynamic environments. To address these issues, this study proposes a four-layer composite state-space adaptive encryption decision model based on the Q-learning framework. By hierarchically integrating application architecture feature parameters (including development language paradigms and encryption logic embedding mechanisms), network environment state variables, security assessment metrics, and device resource constraints, a state encoding system covering the multidimensional perspectives

of "environment-security-resources-architecture" is established. Additionally, an innovative architecture-awareness factor is introduced to optimize algorithm compatibility and engineering implementation feasibility. The study focuses on developing a state-space representation method and an action-space mapping mechanism based on the Markov Decision Process, while also proposing a dynamic programming-based state-space compression strategy and a heuristic search-based action selection optimization solution to address performance bottlenecks in engineering deployment.

Key words: dynamic encryption system;Q-learning; adaptive data encryption

引言

在商用密码应用标准落地实践中[1]，企事业单位通过部署密码设备和应用系统开发调试，以满足身份认证、传输机密性与完整性等基础防护需求；针对在线交易或电子签章等场景下不可否认性要求，则需基于业务特性与数据特征进行深度解析，调用数字签名系统或签章模块实现密码应用的功能闭环。

上述需求及实现已有高可操作性的技术规范和行业实践，但对于数据存储机密性与完整性的实现机制，全行业的技术实现和工程实施仍呈现较高复杂度。其核心症结在于：传统数据加密技术通常需要明确数据来源主体、制定专用加密策略并执行定向加解密操作，本质上属于一种固定参数与预设规则的静态安全范式[2]。该范式看似实现零信任级别的数据防护，然而当面临实时数据处理、动态访问环境及 OLAP 多维分析等复杂应用场景时，静态加密机制与数据高效利用需求之间必然产生结构性矛盾。

针对上述技术挑战，现有研究主要沿着两条技术路径展开：动态加密机制与自适应加密机制。在动态加密框架中，发送方从预置加密算法集合中随机选取加密方案对数据进行加密处理，并通过附加元数据通道传递加密参数，接收端仅需通过合法密钥即可实现数据解密，该机制有效规避了传统固定加密方案的系统脆弱性问题。自适应加密技术则通过实时感知网络安全态势和数据敏感等级，动态优化加密算法的计算复杂度与安全强度，在系统能耗、传输时延与安全需求之间实现多维度均衡。需要指出的是，这两种技术体系最初主要应用于无线传感器网络和移动自组织网络（ad-hoc）的数据传输安全防护。

随着深度强化学习（Deep Reinforcement Learning, DRL）技术在智能决策领域的突破性进展，如何将深度神经网络的上下文感知能力与强化学习的动态策略优化机制相结合，构建情境自适应的智能加密系统，已成为值得深入研究的前沿课题。本研究基于 Q-learning 框架构建了环境感知型数据加密模型，通过严谨定义状态空间 S、动作集合 A 及奖励函数 R，将静态加密策略转换为具备上下文感知能力的动态加密机制。实验结果表明，这种基于人工智能的方法创新不仅显著提升了加密系统的安全鲁棒性，提高密文处理效率，亦为数据全生命周期保护提供了理论依据和可参考的技术实现路径。

相关工作

2.1 AI 在数据加密中的应用

近年来，人工智能技术（特别是深度学习）在数据安全领域展现出显著的应用潜力。Elisa Bertino 等学者系统梳理了该领域主流研究方向，涵盖拒绝服务攻击防御、电子取证优化、入侵检测系统增强、关键基础设施保护、敏感信息防泄漏控制、访问控制机制强化及恶意软件检测技术，同时探讨了人工智能系统自身安全防护问题[3]。Nicolas Guzman Camacho 进一步指出，人工智能在威胁检测、漏洞动态评估、事件响应自动化、安全态势预测分析及主动防御机制构建等方面具有独特技术优势[4]。聚焦于数据加密技术领域，当前研究主要集中于三大方向：加密流量威胁检测、加密协议鲁棒性增强以及自动化加密决策机制。

在加密流量威胁检测方面，机器学习技术已实现创新性应用。IA Alwhbi 等提出四阶段检测框架：通过特征提取获得流量表征，继而引入机器学习模型选择优化及模型训练环节，最终构建具备深度解析能力的加密流量分析系统[5]。Zihao Wang 等突破传统 CNN/RNN/LSTM 模型限制，提出混合特征工程方案——既保留领域专家人工特征设计，又结合机器学习自动特征选择，并创新性引入聚类分析与深度学习融合算法，有效解决复杂网络环境下加密流量特征提取难题[6]。

针对加密协议鲁棒性增强，生成对抗网络（GAN）技术展现出独特价值。Min Li 团队通过构建对抗性密文破解损失函数，将 GAN 集成于加密算法优化过程，不仅提升加密模式复杂度与不可预测性，还实现加密效率的系统性优化[7]。Xingmin Lu 等则创新性融合 GAN 与 Logistic 混沌加密机制，

提出数据特征自适应的动态密钥生成算法，成功在车载网络图像数据加密场景中实现 GPU 加速的高效加密方案[8]。

在自动化加密决策领域，人工智能驱动的动态优化机制成为研究焦点。早期代表性研究如 Hamdy S. Soliman 提出的无线通信安全增强方案，通过密钥回收阶段的向量转换与数据记录重构技术,在 WEP 与 CCMP 协议中实现可证明安全机制[9]。Cao Wanpeng 针对移动通信场景，设计基于用户硬件指纹、个性化特征及伪随机数协同分析的加密策略自适应选择算法，显著提升移动终端敏感数据防护效能[10]。Keke Gai 团队研发的隐私感知自适应加密策略（D2ES）创新引入时序约束下的隐私分级模型，结合动态加密决策（DED）算法，实现数据包级别的智能加密触发机制[11]。Senthilnathan Chidambaranathan 等学者另辟蹊径，从工程实践的角度，探索了人工智能在密文算法模式自动识别方面的应用潜力，为加密策略逆向分析提供新思路[12]。

本研究聚焦于自动化加密决策机制的创新实现，具体提出基于 Q-learning 的加密算法动态切换模型，旨在建立安全性与效率自适应的智能加密系统。

2.2 自适应加密和动态加密

自适应加密在密码学与网络数据安全领域存在概念性差异。其早期研究主要聚焦于加密算法优化，如 P. Krishnadoss 等学者提出的动态字符处理机制：针对数据中特定字符特征，预计算并存储其加密解密参数，显著提升了 RSA 算法的执行效率[13]。

在应用场景研究方面，Jong Min Kim 团队构建了物联网环境下的自适应加密模型，通过动态调整加密强度实现低功耗设备在不同供电条件下的安全效能平衡[14]。Razaq Jinad 等学者则针对云服务场景，提出基于租户安全需求的三维评估模型（数据机密性、数据类型、使用场景），通过分类分级实现加密策略的动态配置[15]。Yongming Feng 进一步拓展至大数据领域，设计分层加密框架：采用去重预处理→哈希密钥生成→非对称密钥保护→对称加密的四阶段架构[16]。本研究主要关注上述三类应用场景导向的研究范式，而非传统算法效率优化范畴。

动态加密与自适应加密存在概念交集，但需明确研究边界：诸如分组密码算法中 S 盒组件的动态替换机制研究，或嵌入式系统密钥动态分配体系，均不属于本文研究范畴。Lars R. Knudsen 提出的动态加密范式具有理论参考价值——在满足 Kerckhoffs 原则前提下，发送方可自主选择加密系统（接收方未知），并基于现有对称密码体系构建，实践中可结合密钥扩展策略强化安全性[17]。本文认为动态加密体系可延伸为系统级密码策略，而自适应加密是实现该体系的重要技术路径。

2.3 深度强化学习与 Q-learning

深度学习（DL）作为一种基于非线性变换的深层神经网络架构，通过多级抽象机制实现特征的自动提取与表征学习，其工作机制模拟人脑皮层对数据的分层解析过程。

强化学习（RL）通过构建价值函数（Value Function）的数学建模框架，评估特定策略的期望累积奖励值，使智能体在马尔可夫决策过程中通过交互式环境探索获得最优策略。

深度强化学习（DRL）通过融合 DL 的特征提取能力与 RL 的决策优化机制，采用深度神经网络对强化学习算法进行参数空间优化。该框架通过环境状态观测-动作执行-奖励反馈的迭代过程，实现策略函数的渐进式优化[18]。

Q 学习（Q-Learning）作为无模型、离策略的强化学习范式，专门用于求解马尔可夫决策过程（MDP）的最优控制问题，其核心在于构建状态-动作对的期望效用函数 Q(s,a)，通过时序差分方法迭代更新动作价值评估矩阵。

Samuel Omokhafe Yusuf 等学者提出的 AI 驱动加密体系，重点论证了机器学习技术在密码学领域的应用范式。该方案通过建立数据敏感性评估模型，实现加密强度的动态自适应调节：对高敏感信息采用增强型加密算法，而对低风险数据实施轻量级加密处理，从而在安全性与计算效率间建立帕累托最优[2]。

Badr Eddine Sabir 等研究者构建了融合公钥基础设施（PKI）、区块链技术与 Q-learning 算法的物联网安全防护模型。该模型通过分布式账本技术保障移动代理的安全迁移路径，并运用强化学习实现恶意节点动态识别。从技术迁移的角度分析，若将该模型中代理机制重构为加密操作控制器，则可基于 Q-learning 框架建立状态空间 S、奖励函数 R 和动作集合 A 的三元组映射关系，实现加密策略的动态优化[19]。SBN Premakumari 团队开发

的强化学习自适应加密框架，通过构建威胁态势感知模型与深度异常检测系统，实现加密强度的动态调控：在低威胁场景下采用能效优先的轻量加密，在高风险环境中切换为安全优先的强加密协议，确保系统在动态网络环境中的安全性与能效平衡[20]。

方案设计

3.1 基本框架

本方案采用状态空间、动作空间与动态奖励函数构成的三元组框架结构，其中状态空间采用复合型状态编码机制进行多维度表征。具体而言，状态空间由以下三个层级构成：

网络环境层：带宽状态（高/中/低）；传输延迟（<50ms/50-200ms/>200ms）；

安全评估层：数据敏感等级（L1-L5 分级制度）；威胁指数（0-100 连续量度）；

设备资源层：CPU 负载水平（<30%/30-70%/>70%）；内存资源占用率（三级离散划分）；

动作空间包含五类标准化加密算法集合，其决策维度涵盖对称加密、非对称加密及混合加密等核心密码学技术。

算法选项	适用场景	性能参数
AES-128-GCM	常规加密	吞吐量 200Mbps
ChaCha20-Poly1305	移动设备	延迟<5ms
RSA-4096	密钥交换	高安全等级要求
SM4	合规要求	国密标准
SM2	合规要求	国密标准
3DES	兼容旧设备	存量适配

AES-256-GCM	静态数据加密	逃生模式

其中，奖励函数设计为：

$$R_t = \alpha \cdot \frac{T_{max}}{T_{enc}} + \beta \cdot S_{level} - \gamma \cdot (C_{cpu} + C_{mem})$$

关键参数设置：

加密耗时权重α=0.3；安全增益β=0.6；资源惩罚γ=0.1，其中安全增益通过攻击面量化模型计算，时延惩罚要动态调整。

在复杂应用架构下，要考虑更多转态的分层融合方式，考虑应用架构编码：开发语言（JAVA/C#/PYTHON/其他）；植入逻辑（类/注解/字节码/数据持久层/其他）。其中开发语言的技术影响主要是算法库支持差异，执行效率差异和内存管理机制差异。其中植入逻辑主要是加密触发时机（编译时/运行时），资源占用位置（CPU/内存/IO）以及安全风险等级（字节码被篡改引发风险）。

奖励函数增强设计时，增加感知因子：

$$R_{new} = R_{original} + \delta \cdot Lib + \theta \cdot Iim$$

关键参数设置：

支持系数δ=0.15；植入成本系数θ=0.1

3.2 算法实现

针对 Q-table 优化策略，采用分层哈希表存储高频状态（出现概率>5%的状态独立存储），对低频状态使用 Bloom Filter 进行概率剪枝。

针对动态调整 ε 的策略

```
def get_epsilon(episode):
base_eps = 0.1
```

```
    decay_factor = 0.98
    return max(0.05, base_eps * (decay_factor ** episode))
```

训练初期保持 30%探索率（保证充分探索），每周期衰减 2%，ε 接近 0.05 时进入部署阶段。

针对状态转移监控，考虑滑动窗口机制检测环境突变：

```
class EnvMonitor:
    def __init__(self, window_size=10):
        self.window = deque(maxlen=window_size)
    def state_changed(self, new_state):
        change_rate = sum([1 for s in self.window if s != new_state])/len(self.window)
        self.window.append(new_state)
        return change_rate > 0.7  # 触发 Q-table 重置条件
```

在 AI 技术应用于数据加密领域，根据文献[5][9]数据集预训练不足，生产级模拟记录需要达到百万。故，可考虑引入在线学习实时采集数据更新。可考虑实现混合训练机制，如连续 20 个 episode 的 Q 值变化方差小于 0.01 时停止训练，进入在线学习模式。

更多地，要考虑安全增强设计连续 3 次选择非最优动作触发人工审查；当置信度低于阈值如 60%时，启用基线加密如 SM4，或当检测到特殊攻击，比如 CC 攻击时强制切换至轻量级算法如 ChaCha20。

方案实践

4.1 AOP 切面数据加密

在方案验证中，利用 Java 生态中的 Spring AOP 或 AspectJ 定义加密切面（Encryption Aspect），拦截和操作数据持久化与传输的关键节点。对于

数据库的拦截，切点限定为自定义仓库接口，避免拦截 Spring Data 内部方法；同时，通过反射和注解标记敏感字段实现字段级加密，避免全对象序列化引发性能损耗。更多，要考虑原始参数类型安全，避免 byte 替换 Object 的错误。对于 HTTP 响应的拦截，使用@ResponseBody 注解匹配（ResponseBodyAdvice 不稳定）；元数据封装应该包含密文、策略版本、算法、IV 值；使用 Caffeine 缓存高频策略，通过 requiresEncryption()方法动态判断数据敏感性。实例如下所示：

```
@Aspect
@Component
public class DataSecurityAspect {
    private static final Logger logger = LoggerFactory.getLogger(DataSecurityAspect.class);
    @Autowired
    private DRLPolicyClient policyClient;
    // 本地策略缓存（示例使用 Caffeine）
    private final Cache<Class<?>, EncryptionPolicy> policyCache =
        Caffeine.newBuilder().expireAfterWrite(5, TimeUnit.MINUTES).build();
    // 1. 修正数据库操作拦截逻辑
    @Around("execution(* com.example.repository.*.save(..))") // 更精确的切点
    public Object securePersistOperation(ProceedingJoinPoint pjp) throws Throwable {
        Object entity = pjp.getArgs()[0];
        // 通过缓存获取策略减少远程调用
```

```
            EncryptionPolicy policy = policyCache.get(entity.getClass(),
                cls -> policyClient.fetchCurrentPolicy(cls));
            // 字段级加密而非全对象序列化
            encryptEntityFields(entity, policy);
            return pjp.proceed(new Object[]{entity});
        }
        // 2. 修正 HTTP 响应拦截逻辑
    @Around("@annotation(org.springframework.web.bind.annotation.ResponseBody)")
        public Object secureApiResponse(ProceedingJoinPoint pjp) throws Throwable {
            Object data = pjp.proceed();
            if (requiresEncryption(data)) {
                EncryptionPolicy policy = policyCache.get(data.getClass(),
                    cls -> policyClient.fetchCurrentPolicy(cls));
                // 构建包含元数据的加密对象
                return new EncryptedPayload(
                    CryptoUtils.encrypt(serialize(data), policy),
                    policy.version(),
                    policy.iv()
                );
            }
            return data;
        }
        // 字段加密实现（需配合实体注解）
        private void encryptEntityFields(Object entity, EncryptionPolicy policy) {
```

```
                Arrays.stream(entity.getClass().getDeclaredFields())
                        .filter(f -> f.isAnnotationPresent(SensitiveField.class))
                        .forEach(field -> {
                            // 反射加密字段内容
                            field.setAccessible(true);
                            Object value = field.get(entity);
                            byte[] encrypted = CryptoUtils.encrypt(value.toString(),
policy);
                            field.set(entity,
Base64.getEncoder().encodeToString(encrypted));
                        });
            }
        }
```

切面通过 DRL 策略客户端（DRLPolicyClient）实时获取当前数据类别的加密规则（如 AES-256-GCM 或 ChaCha20-Poly1305）以实现策略动态注入；加密后的数据附加策略版本号与初始向量（IV）要实现元数据绑定，确保解密时可追溯正确的密钥。本地缓存存储高频策略可以降低 DRL 引擎调用延迟。

4.1.2 自定义序列化实现无感加密

针对结构化数据（如 Protobuf/JSON）与非结构化数据（文件流），设计可插拔式序列化器：

```
public class EncryptedJsonSerializer extends JsonSerializer<Object> {
    @Override
    public void serialize(Object value, JsonGenerator gen,
SerializerProvider provider) throws IOException {
        ByteArrayOutputStream baos = new ByteArrayOutputStream();
```

```
            objectMapper.writeValue(baos, value);
            byte[] encrypted = policyClient.encrypt(baos.toByteArray(),
value.getClass());
            gen.writeBinary(encrypted);
        }
    }
    // 注册自定义序列化器
    module.addSerializer(SensitiveData.class,new EncryptedJsonSerializer());
```

通过替换序列化逻辑，兼容 Thrift、Avro 等多种协议，同时建议根据 @SensitiveField 注解实现字段级加密，减少计算开销。

4.2 配套技术支持

4.2.1 策略推理与实时反馈

基于系统扩展性需求分析，本研究采用 gRPC 微服务架构实现 DRL 引擎的分布式部署。针对业务场景的动态特性需求，系统需构建具备动态惩罚时延调控机制，并确保推理服务在单节点条件下需满足每秒万级策略查询的并发处理能力。技术架构层面特别配置了反馈闭环系统，对加密操作日志（包括服务成功率、故障率及吞吐量等关键性能指标）进行实时采集与分析，通过建立数据流管道将处理结果同步回流至经验回放池，进而驱动策略模型的增量式优化更新。

4.2.2 密文标识与密钥管理

本研究中预见性地指出，在数据存储环节将呈现明文数据、密文数据（多工作密钥）并存的格局。针对该混合存储模式，本研究提出双重解决方案：一方面可基于 Senthilnathan Chidambaranathan 等学者提出的智能识别

机制[12]，实现批量密文数据的自动化检测；另一方面在工程实践层面，需针对不同密码算法参数（包括初始化向量、密码算法类型及工作模式等核心要素）设计专用密文标识符，以建立精确的密码参数映射关系。

4.2.2 性能优化与工程实践

计算卸载策略：实施非对称加密算法（如 RSA/SM2）的运算任务卸载机制，将核心加密操作迁移至专用加密硬件或分布式加密平台，从而有效降低主处理器的计算负载；

异步策略更新机制：采用 Disruptor 无锁环形队列架构处理策略切换事件，构建事件驱动型异步处理模型，确保业务线程的非阻塞运行；

动态密钥管理体系：依托公钥基础设施（PKI）框架，建立策略版本号与密钥版本的动态映射关系，实现基于版本控制的密钥生命周期管理，保障数据解密操作的全生命周期可追溯性；

容灾容错设计：完善系统降级机制，当深度强化学习引擎发生异常或智能体处于无状态场景时，自动触发预置静态安全策略回退机制（例如在“高安全模式”下强制执行 AES-256 加密标准）。

挑战与展望

从宏观的大数字化产业看，一方面是 IPv6 协议、物联网(IoT)技术及第六代移动通信(6G)持续演进，另一方面是数据处理逻辑呈现集中化趋势，同时数据应用呈现边缘化特征，自适应加密技术作为数据动态加密体系的核心支撑技术，已成为数据安全领域的关键性技术演进方向。从网络与数据安全产业看，人工智能安全攻击检测与异常行为识别技术逐步成熟，本技

术模式不仅是攻击检测与异常行为识别的配套方案，更可构建独立的量化评估模型，为实现数据处理效率与数据防护效能的动态平衡提供新的思路。

然而，新技术实施面临多维挑战：首要问题在于与传统密码体系的兼容性冲突，例如在商用密码应用安全性评估体系中，需重新构建数据加密的合规性判定框架；其次，动态加密技术需在技术实现层面预设安全策略覆写接口，具体表现为在加密插件或 SDK 开发过程中，需应用系统整合基于设计加密(Encryption by Design)的技术框架；最后，人工智能技术的集成实质是在加密过程中引入了概率化决策机制，这对从业者的安全认知与风险量化评估能力提出了新的要求。

本研究领域仍存在若干拓展方向：比如，在新技术新业务场景下技术推广，如 5G/6G 网络融合架构中，可基于网络切片技术实施差异化加密策略配置，即针对增强移动宽带(eMBB)切片优化加密算法效率，面向超高可靠低时延通信(uRLLC)切片实施低延迟加密协议；再比如，随着密文威胁检测技术的突破，可建立人工智能驱动的数据安全协同机制，通过加密策略与威胁情报的实时交互，构建"检测-防护(加密)-响应"闭环机制，实现主动式数据安全防护体系。（作者：刘晓光 北京炼石网络技术有限公司）

参考文献

[1] 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.

[2] Yusuf, S. O. (2024). Analyzing the efficiency of AI-powered encryption solutions in safeguarding financial data for SMBs. WJARR. Retrieved from https://wjarr.com/sites/default/files/WJARR-2024-2753.pdf

[3] AI for Security and Security for AI. (2020). ACM Digital Library. Retrieved from https://dl.acm.org/doi/abs/10.1145/3422337.3450357

[4] Camacho, N. G. (2024). The Role of AI in Cybersecurity: Addressing Threats in the Digital Age. Cybersecurity Today Journal. [Publisher information if available].

[5] Alwhbi, I. A. (2024). Encrypted network traffic analysis and classification utilizing machine learning. Journal of Network Security Research, 38(2), 112-130.

[6] Kong, B. (2024). A method of detecting the abnormal encrypted traffic based on machine learning and behavior characteristics. International Journal of Cryptography & Information Security, 16(1), 55-70.

[7] Li, M. (2024). Application of GAN-Based Data Encryption Technology in Computer Communication System. Informatica, 48, 17 – 34.

[8] Lu, X. (2024). Improved trajectory data encryption method for internet of vehicles using GAN-based chaotic logistic algorithm. Journal of Cybersecurity and Communication Networks, 2024, 1-16.

[9] Soliman, H. S., & Omari, M. (2024). Application of synchronous dynamic encryption system in mobile wireless domains. Wireless Communications and Mobile Computing, 23(5), 240-251.

[10] Cao, W., & Bi, W. (2024). Adaptive and dynamic mobile phone data encryption method. China Communications, 11(6), 103-109.

[11] Gai, K., Qiu, M., Zhao, H., & Xiong, J. (2024). Privacy-Aware Adaptive Data Encryption Strategy of Big Data in Cloud Computing. Journal of Cloud Computing and Security, 12(3), 25-40.

[12] Chidambaranathan, S., Santhanaraj, M., Ajitha, E., A S, S. F., B, S., & Kathirvel, T. (2024). Automated Detection of Encryption Algorithms Using AI Techniques. In Proceedings of the 2024 International Conference on IoT Based Control Networks and Intelligent Systems (ICICNIS), 30-35.

[13] Krishnadoss, P., Krishnan, P. T., & Paramasivam, N. (2024). Dynamic Approach for Time Reduction in RSA Algorithm through Adaptive Data Encryption and Decryption. International Journal of Applied Cryptography, 19(2), 123-135.

[14] Kim, J. M., Lee, H. S., Yi, J., & Park, M. (2024). Power Adaptive Data Encryption for Energy-Efficient and Secure Communication in Solar-Powered Wireless Sensor Networks. Journal of Wireless Communications, 18(3), 88-101.

[15] Jinad, R., Akinsowon, T., Ihekweazu, C., & An, M. K. (2024). Enhancing Data Security and Privacy through Classification-Based Adaptive Encryption. International Journal of Cybersecurity, 5(3), 150-164.

[16] Feng, Y., & Wang, J. (2024). Big Data Adaptive Encryption Technology for Remote Network Storage. International Journal of Cloud Data Security, 8(1), 44-58.

[17] Knudsen, L. R. (2024). Dynamic Encryption. Journal of Cryptographic Techniques, 22(4), 76-82.

[18] Sutton, R. S. (2018). Reinforcement learning: An introduction (2nd ed.). Cambridge: MIT Press.

[19] Sabir, B. E. (2024). Q-Learning Based Method to Secure Mobile Agents and Choose the Safest Path in an IoT Environment. Journal of IoT Security, 4(2), 100-112.

[20] Premakumari, S. B. N., Sundaram, G., Rivera, M., Wheeler, P., & Guzmán, R. E. P. (2024). Reinforcement Q-Learning-Based Adaptive Encryption Model for Cyberthreat Mitigation in Wireless Sensor Networks. Wireless Sensor Networks Journal, 13(2), 85-97.

4. 加强体育院校网络安全防护的几点思考

摘要：网络安全是体育院校数字化、智能化转型升级行稳致远的重要保障，已成为体育院校的核心竞争力之一。本文分析了体育院校网络安全面临的挑战和困境，从提升监测预警能力、实施物理空间与网络空间的联合身份认证、加强网络安全宣传教育等方面阐述了加强网络安全防护的对策建议。

关键词：体育院校　网络安全　攻击防护

为加快推进体育强国建设，体育院校正努力实现数字化、智能化转型升级，通过构建一体化的网络安全综合防御体系，用高水平安全保障高质量发展。

一、网络安全已成为体育院校的核心竞争力之一

体育院校承担着高水平运动员甚至国家队运动员的教学、训练以及科技服务保障等重要使命。体育大数据中心汇集了海量的体育数据，包括运动员的运动表现数据、体质监测数据、心理活动数据、环境数据等，这些数据是构建运动大模型的重要基础。一旦高水平运动员的敏感数据遭到泄露或篡改，将造成不可估量的损失。另一方面，体育院校经常举办各类体育赛事，需要利用多个信息系统（平台）进行计时计分、监控仲裁、发布成绩、视频直播等活动，这些信息系统（平台）一旦遭到网络攻击，将严重影响体育赛事的公平公正，甚至造成难以挽回的舆情后果。由此可见，体育院校的数字化、智能化水平越高，对网络安全的要求就越高。网络安全已成为体育院校的核心竞争力之一。

二、体育院校网络安全面临的挑战和困境

体育院校不仅是高水平运动员的训练场和竞技场，也是网络空间攻防对抗的重要战场。当前，体育院校的网络安全工作面临着一些挑战和困境。

（一）智能化的攻击手段

随着人工智能技术的广泛应用，越来越多的智能化攻击手段出现在网络攻防对抗的战场。智能化攻击手段可自动化地开展代码分析、密码破译、逆向工程、漏洞挖掘和自动编程利用漏洞、生成恶意程序等活动。接入校园网的任何一台服务器、PC 终端、手机等设备都将成为智能攻击的对象。智能化的攻击手段难以被传统安全防御系统及时识别和拦截，给网络安全防护带来了巨大挑战[1]。

（二）利用无人机实施网络攻击

攻击者在无人机上搭载网络攻击设备，发射并停落在校园的楼顶上。此类无人机体积小、重量轻，不易被发现。无人机搭载的网络攻击设备可以自动搜索校园的无线网，暴力破解密码，接入校园网实施网络攻击，并将学校的重要敏感数据转发出去。无人机搭载的网络攻击设备也可以对校园内的 LED 显示屏实施控制，造成 LED 显示屏的内容被恶意篡改，从而引发公共舆情事件。

（三）有些深层次安全漏洞难以修复

有些深层次漏洞，修复的代价很大，尤其是当这些漏洞与系统的核心功能或底层架构密切相关时，修复过程中可能会引入新的问题，导致系统崩溃、性能下降、功能异常以至于影响系统的正常运行。由于学校的重要

业务系统需要不间断服务广大师生，系统不允许关停。因此，修复深层次漏洞不得不权衡安全性、稳定性和业务连续性，亟需研究稳妥的解决方案，既要保障系统的正常运行，又要确保漏洞不被利用。

三、加强体育院校网络安全防护的对策建议

体育院校必须构建一体化的网络安全综合防御体系，从组织领导、制度安排、监测预警、溯源追踪、纵深防御、宣传教育等各方面统筹施策，不断提升网络安全防护能力。

（一）提升监测预警能力

网络安全是攻防双方技术能力的较量[2]。只有不断提升网络安全防护能力，才能从根本上保护好学校的信息资产以及师生的数据安全。通过统一全网流量和异构日志数据，融合威胁情报实时分析、智能决策，实现资产和漏洞的全周期管控，为校园网络安全运营提供有效支撑，实现全域安全态势感知和事件回溯分析追踪，打造数据流动风险识别与可视、多场景数据保护的网络安全运营机制，加强数据分类分级管理，建立常态化网络安全风险监测预警，促进学校网络安全综合防御体系的建立。对全校的信息资产采取周密的监测手段，对接入校园网的所有服务器和终端实施7×24小时监测，发现网络威胁后立即告警。接到告警之后，快速开展溯源分析，确保安全隐患定位到具体人、具体设备，及时通知相关部门和单位采取处置措施，防范化解安全风险。

（二）实施物理空间与网络空间的联合身份认证

物理空间身份认证是指对进入学校物理空间人员的真实身份进行认证。所有人员进入学校大门以及进入场馆时都要进行人脸识别，在校园内活动时也要进行人脸抓拍，实时记录每一名在校人员的大致位置。对于非本校师生进入学校时的认证，要与公安部门对接，比对人脸特征。

网络空间身份认证是指对访问校园网的实体进行权限合法性的认证。当进校人员的电脑、手机等设备接入校园网时，从技术上强制采用多因素身份认证的方式进行认证，之后实时记录设备使用校园网的大致位置，并与上网账号对应人员的物理空间位置进行对比，如果两者的时空位置有较大差别，应立即向学校有关部门推送告警信息，并快速进行溯源取证，确认人员的身份以及校园网账号是否为本人使用。如果证据显示某账号被攻击者利用，立即禁用该账号并采取进一步的措施。

（三）加强网络安全宣传教育

网络安全需要全体师生共同参与。开展网络安全宣传教育要覆盖到所有师生。大力宣传国家网络安全工作取得的重大成就，深入宣传贯彻《网络安全法》《数据安全法》《个人信息保护法》及相关配套法规，普及网络安全防护的技术和方法，提升广大师生的网络安全素养和网络安全防护技能，营造清朗网络空间[3]。通过举行网络安全主题讲座、开设网络安全课程、发放网络安全宣传材料、推送微信公众号文章等多种形式对学校师生特别是对新入学的大学生开展网络安全宣传教育，使大家深刻认识到网络空间是国家主权的“第五疆域”，网络安全是推进中国式现代化行稳致

远的重要保障。通过组织网络安全防护应急演练，实现“人人讲安全，个个会应急”的目标。（作者：郑成文 北京体育大学 高级工程师）

参考文献：

1.朱俊涛,人工智能在新型网络安全体系中的应用探究[J],中国信息界，2025（02）

2.胡春卉，陈剑锋，网络安全前沿技术演进机理与发展策略[J]，国防科技，2024（01）

3.刘坤峰，刘欣慧，大学生网络安全素养培养研究[J]，网络安全技术与应用，2022（12）

行业前沿观察二：2024 广东、广州网民网络安全感满意度调查统计报告发布；网信部门公开曝光网络谣言典型案例、开展“清朗·整治 AI 技术滥用”专项行动；移动互联网未成年人模式正式发布

导读：2024 网民网络安全感满意度调查活动《广东区域报告》、《广州区域报告》（以下均称为“报告”）在广州成功发布。报告数据显示，广东、广州网民网络安全感大幅度提升，对数字政府服务的满意度持续走高；与全国数据相比，广东地区网民在网络社会发展成就中的安全感、获得感和幸福感程度更高，均达到七成以上。

近日，中央网信办印发通知，在全国范围内部署开展为期 3 个月的“清朗·整治 AI 技术滥用”专项行动。近期，一些网络账号以滥用 AI 技术、嫁接拼凑等方式虚构突发案事件、编造公共政策、捏造社会民生领域谣言，误导网民认知，造成公众恐慌，扰乱社会秩序。在网信部门指导下，网站平台持续加大监测和处置曝光力度，将部分典型案例通报给广大网民。

4 月 29 日上午，移动互联网未成年人模式在第八届数字中国建设峰会主论坛上正式发布。立足未成年人网络保护现实需要、回应社会各界期待关切，国家网信办持续指导国内软硬件企业共同推进移动互联网未成年人模式建设工作。

关键词：互联网、AI、网络安全、网信办、未成年

1. 安全感和满意度同步提升！2024 广东、广州网民网络安全感满意度调查统计报告发布

4 月 29 日，2024 网民网络安全感满意度调查活动《广东区域报告》、《广州区域报告》（以下均称为“报告”）在广州成功发布。报告数据显示，广东、广州网民网络安全感大幅度提升，对数字政府服务的满意度持续走高；与全国数据相比，广东地区网民在网络社会发展成就中的安全感、获得感和幸福感程度更高，均达到七成以上。

报告发布会由网民网络安全感满意度调查活动组委会指导，广东省网络空间安全协会、广州网络空间安全协会主办。广东省网络空间安全协会副会长、调查活动承办单位广东新兴国家网络安全和信息化发展研究院总工程师高宁出席会议并作报告说明和解读，调查活动组委会常务副秘书长、广东省网络空间安全协会秘书长周贵招主持会议。广东新兴国家网络安全和信息化发展研究院助理研究员毛翠芳、吴娱分别发布广东调查报告、广州调查报告。发布会由虎牙直播面向全国观众全程线上同步直播。

报告围绕网络安全综合治理效果、网络法治建设成果、网络违法治理、网络诚信建设成效、个人信息保护与数据安全、网络购物安全及权益保障、互联网平台监管与企业自律、特殊人群网络权益保护、数字政府服务与治理、网络社会发展的变化与冲击、等级保护实施与企业合规、行业发展与科技创新、新技术挑战与网络安全等方面内容进行分析研究，并通过全国、广东省、广州市三个行政层级的情况进行对比，全面反映 2024 年度广东（含广州）网络安全态势及网民关注的网络安全焦点和痛点问题。

一、广东网民对网络安全感的正面评价率持续上升

报告显示，2024 年广东省公众网民对网络安全感的正面评价率为 63.10%，和 2023 年相比上升了 6.97 个百分点，说明网络安全治理的针对性措施初见成效，公众对风险防控的信任度有所提升。在满意度方面，调查发现 64.90%广东网民对我国网络安全治理的状况是满意为主。

二、网络法治建设成果突出，新法律法规的普法有待加强

报告显示，超过六成半广东网民对网络空间领域的立法建设效果表示满意。在网络安全法律法规认知方面，《国家安全法》、《网络安全法》和《个人信息保护法》知晓率较高且超全国水平，显示出普法宣传成效显著。但在新兴网络犯罪如 “帮信罪” 的认识仍有不足，反映在新法律法规的普法上仍有不足。

此外，网民最关注未成年人上网保护、互联网络平台安全责任监管细则、以及数据安全保护实施细则，需求强度显著高于全国，凸显立法优化方向。

三、广东网民对跨境诈骗打击力度满意度较高，但网络诈骗形势依然严峻

报告指出，参加调查的广东网民感受到的网络诈骗活跃度仍处在较高的位置。和全国数据相比，排名前三的常遇网络诈骗中，前两位都是“电话欠费、积分兑换、中奖诈骗”和“贷款金融诈骗”，不同的是第三位，广东地区的网民更常遇到“网络购物诈骗”。

此外，公众网民关于政府对跨境诈骗打击力度的满意度评价较高，认为满意的接近六成。而加强执法力度打击网络罪犯、加强宣传教育、加强制定和完善相关法律法规等是广东网民期望政府应对跨境诈骗时加强的内容。

四、超过六成半网民满意当前个人信息保护状况，但仍需加强保护力度

在对我国当前个人信息保护状况满意度评价方面，参与调查的广东、广州网民中表示满意的均超过六成半，和上一年相比，公众网民对个人信息保护状况正面评价有明显提升。

需要特别关注的是，调查显示近七成广东网民不了解个人信息保护公益诉讼制度。推行个人信息保护公益诉讼面临诉讼过程漫长、维权意识不足、判决执行困难等困境。公众建议扩大检察机关获取侵权线索途径、加强惩罚措施、完善配套制度。

五、网络诚信建设成效改善，电商、社交平台成广东网民网络诚信建设治理焦点

在网络诚信建设方面，调查发现广东省网民对网络诚信状况总体得分为 7.41 分，好评率为 69.13%，和上一年相比有较大提升。

此外，参与调查的公众网民遭遇不诚信行为的概率超过四成半。其中最常遭遇不诚信行为的互联网行业或领域是电商平台、社交平台、新闻媒体网站平台。

六、广东网民网络购物维权意识较强，处罚不足成维权瓶颈

报告显示，广东、广州网民的网络购物安全满意度均超七成，但刷单与直播问题待解。在网络维权的难点方面，参与调查的公众网民认为排在第一位的是“对侵权消费者权益的行为处罚力度不够”，占52.65%。数据显示对侵权消费者权益的行为处罚力度不够，导致侵权行为不受到足够的制约是消费者维权难的主要原因。

七、特殊人群权益保护渐显，消除数字鸿沟仍需努力

参与调查的广东网民对未成年人网络权益保护状况满意度评价中，认为满意以上的占49.48%。数据显示，广东省未成年人互联网普及率高于全国平均水平。在认为未成年在网络空间中面临的主要风险的选择中，广东、广州网民选择率排名前三位都是网络沉迷、接触不良信息、个人隐私泄露。在网络应用适老化改造方面，广东网民对改造效果认为满意以上的占45.53%，负面评价占比6.59%。和上一年相比，正面评价的选择率上涨5.54个百分点。此外，数据显示老人使用网络困难的主要原因集中在技术操作复杂性与隐私问题。

八、五成网民对互联网平台自律满意，不良信息与执行短板仍待突破

报告显示，超过五成参与调查的广东网民（50.55%）对互联网平台自律评价为满意，广州网民中认为满意的则接近五成（49.39%）。

调查显示，网络环境问题依旧严峻。过去的一年来，传播色情、暴力、赌博等不良信息在网民中的接触率较高，超五成广东网民认为网络欺凌情况严重。

九、超七成广东网民认为政府网上服务便利或非常便利

调查发现，广东网民对数字政府服务评价较高，便利性和安全性评价均高于全国平均水平。71.76%公众网民认为政府网上服务便利或非常便利，70.25%公众网民认为政府网上服务安全和非常安全。但不足之处在于办理时效、资料提交、结果反馈等。

十、广东网民对网络强国战略成效的认可度高，正面评价居全国前列

报告显示，超过六成半的广东网民对网络强国战略在网络空间治理中的成效表示了充分的肯定。

同时，超七成的广东网民对我国网络社会发展现状表示满意，显示出网民对网络社会快速发展的高度认可与肯定。与全国数据相比，广东地区网民在网络社会发展成就中的安全感、获得感和幸福感程度更高，均达到七成以上。

此外，调查显示网络社会的快速发展在带来便利的同时，也对公众的心理健康提出了新的挑战。调查数据显示，网络社会对公众的心理健康产生了显著影响，接近半数（47.05%）的广东网民表示感受到了不同程度的心理压力或焦虑，其中，个人信息得不到保护、网络暴力、不实谣言、网络成瘾、网络诈骗威胁等问题是影响部分网民的心理状态的主要因素。

2.网信部门公开曝光第六批涉公共政策、突发案事件、社会民生领域网络谣言典型案例

近期，一些网络账号以滥用AI技术、嫁接拼凑等方式虚构突发案事件、编造公共政策、捏造社会民生领域谣言，误导网民认知，造成公众恐慌，扰乱社会秩序。网信部门指导网站平台持续加大监测和处置曝光力度，及

时溯源并关闭谣言首发账号，累计处置相关违法违规账号2210个。现将部分典型案例通报如下。

1.“AI预测彩票号码百分百中奖”谣言。一则“AI预测彩票号码，百分百中奖”的消息在网络上流传。中国福彩发文提醒，所谓AI预测彩票号码均为骗局，请务必警惕。快手平台“落寞人生”、小红书平台“快来带我吃饭”等账号已被依法依约关闭。

2.“广东冰雹比鸡蛋还大”等谣言。近期，有网民借广东冰雹天气，发布“冰雹比鸡蛋还大”“冰雹砸坏汽车”等图片。经广东省互联网举报中心核实，相关图片均为通过AI制作生成的虚假图片，画面明显夸大灾情。百度平台“童生在此”、小红书平台“遥遥雪中客”、今日头条平台“小糖热搜”等账号已被依法依约关闭。

3.“杭州滨江发生恶性刑事案件”谣言。网上有消息称“滨江区发生恶性刑事案，嫌疑人已被刑拘”，引发关注。经当地公安机关查证，该信息纯属虚构，系造谣者为博取流量，利用AI生成工具捏造虚假案情，经深度编辑后发布于社交平台，已依法对造谣者作出行政处罚。百度平台“小娱游游”、微信平台“憨憨小魔王”等账号已被依法依约关闭。

4.“扫码领取‘五险一金补贴’”谣言。近日，有网民反映收到“扫码领取‘五险一金补贴’”的通知。人力资源和社会保障部表示，通知信息不实且涉嫌诈骗，从未面向普通群众发放过所谓的“五险一金补贴”。微信平台“尼吉特”等账号已被依法依约关闭。

5.“故意捏造并传播虚假‘死亡率’”系列谣言。近期，“截至2024年末，80后死亡率突破5.2%”“70后死亡率却低于80后”等信息在网上流传。经公安机关查证，上述信息系个别网民为挑拨情绪、售卖保健品而借机编造的谣言，已对造谣者依法予以行政处罚。知乎平台“江南”、哔哩哔哩平台“晶晶说-”等账号已被依法依约关闭。

6.“重庆一工业园区着火10人遇难上百人失联”谣言。近日，有网民散播“10人遇难，16人受伤，上百人失联，重庆一工业园区着火”的信息，引发关注。经重庆市互联网违法和不良信息举报中心向重庆市应急管理局和重庆市消防救援总队核实，重庆近期未发生此类事故，网传信息系谣言。抖音平台“霞姐”、微博平台“官疯雨”等账号已被依法依约关闭。

7.“云南德宏芒市发生5.8级地震”谣言。近日，有网民发布视频称“云南芒市发生5.8级地震”。经芒市委网信办核实，相关视频系造谣者为蹭流量，将缅甸地震视频标注为“云南芒市地震废墟”的不实信息。抖音平台“爱一个人要好好的对她”、快手平台“相识是缘033”等账号已被依法依约关闭。

8.“中国残疾人联合会宣传文化部开展APP线上试点”谣言。有网络传言称“中国残疾人联合会宣传文化部开展APP线上试点”，中国残联宣文部严正声明，从未授权任何组织或个人成立所谓“中国残联线上试点线下工作室”，从未组织开展过所谓“APP线上试点精准扶贫助残”等活动。微信平台“然然的”等账号已被依法依约关闭。

中央网信办相关部门负责人表示，将持续加大网络谣言监测打击力度，从严查处发布谣言的账号，及时曝光违法违规典型案例，形成有力警示震慑效应。同时欢迎网民积极参与监督举报，广泛凝聚各方力量，合力铲除网络谣言生存土壤，共同营造清朗网络空间。

3.中央网信办部署开展“清朗·整治AI技术滥用”专项行动

为规范AI服务和应用，促进行业健康有序发展，保障公民合法权益，近日，中央网信办印发通知，在全国范围内部署开展为期3个月的“清朗·整治AI技术滥用”专项行动。

中央网信办有关负责人表示，本次专项行动分两个阶段开展。第一阶段强化AI技术源头治理，清理整治违规AI应用程序，加强AI生成合成技术和内容标识管理，推动网站平台提升检测鉴伪能力。第二阶段聚焦利用AI技术制作发布谣言、不实信息、色情低俗内容，假冒他人、从事网络水军活动等突出问题，集中清理相关违法不良信息，处置处罚违规账号、MCN机构和网站平台。

第一阶段重点整治6类突出问题：一是违规AI产品。利用生成式人工智能技术向公众提供内容服务，但未履行大模型备案或登记程序。提供“一键脱衣”等违背法律、伦理的功能。在未经授权同意情况下，克隆、编辑他人声音、人脸等生物特征信息，侵犯他人隐私。二是传授、售卖违规AI产品教程和商品。传授利用违规AI产品伪造换脸视频、换声音频等教程信息。售卖违规“语音合成器”“换脸工具”等商品信息。营销、炒作、推广违规AI产品信息。三是训练语料管理不严。使用侵犯他人知识产权、隐

私权等权益的信息。使用网上爬取的虚假、无效、不实内容。使用非法来源数据。未建立训练语料管理机制，未定期排查清理违规语料。四是安全管理措施薄弱。未建立与业务规模相适应的内容审核、意图识别等安全措施。未建立有效的违规账号管理机制。未定期开展安全自评估。社交平台对通过API接口接入的AI自动回复等服务底数不清、把关不严。五是未落实内容标识要求。服务提供者未对深度合成内容添加隐式、显式内容标识，未向使用者提供或提示显式内容标识功能。内容传播平台未开展生成合成内容监测甄别，导致虚假信息误导公众。六是重点领域安全风险。已备案AI产品提供医疗、金融、未成年人等重点领域问答服务的，未针对性设置行业领域安全审核和控制措施，出现“AI开处方”“诱导投资”“AI幻觉”等问题，误导学生、患者，扰乱金融市场秩序。

第二阶段重点整治7类突出问题：一是利用AI制作发布谣言。无中生有、凭空捏造涉时事政治、公共政策、社会民生、国际关系、突发事件等各类谣言信息，或擅自妄测、恶意解读重大方针政策。借突发案事件、灾难事故等，编造、捏造原因、进展、细节等。冒充官方新闻发布会或新闻报道，发布谣言信息。利用AI认知偏差生成的内容进行恶意引导。二是利用AI制作发布不实信息。将无关图文、视频拼凑剪辑，生成虚实混杂、半真半假的信息。模糊修改事件发生的时间、地点、人物等要素，翻炒旧闻。制作发布涉财经、教育、司法、医疗卫生等专业领域的夸大、伪科学等不实内容。借助AI算命、AI占卜等误导欺骗网民，传播迷信思想。三是利用AI制作发布色情低俗内容。利用AI脱衣、AI绘图等功能生成合成色情内

容或他人不雅图片、视频，衣着暴露、搔首弄姿等软色情、二次元擦边形象，或扮丑风等导向不良内容。制作发布血腥暴力场景，人体扭曲变形、超现实怪物等恐怖诡谲画面。生成合成“小黄文”“荤段子”等性暗示意味明显的小说、帖文、笔记。四是利用AI假冒他人实施侵权违法行为。通过AI换脸、声音克隆等深度伪造技术，假冒专家、企业家、明星等公众人物，欺骗网民，甚至营销牟利。借AI对公众人物或历史人物进行恶搞、抹黑、歪曲、异化。利用AI冒充亲友，从事网络诈骗等违法活动。不当使用AI“复活逝者”，滥用逝者信息。五是利用AI从事网络水军活动。利用AI技术“养号”，模拟真人批量注册、运营社交账号。利用AI内容农场或AI洗稿，批量生成发布低质同质化文案，博取流量。使用AI群控软件、社交机器人批量点赞跟帖评论，刷量控评，制造热点话题上榜。六是AI产品服务和应用程序违规。制作和传播仿冒、套壳AI网站和应用程序。AI应用程序提供违规功能服务，例如创作类工具提供“热搜热榜热点扩写成文”等功能，AI社交、陪聊软件等提供低俗软色情对话服务等。提供违规AI应用程序、生成合成服务或课程的售卖、推广引流等。七是侵害未成年人权益。AI应用程序诱导未成年人沉迷、在未成年人模式下存在影响未成年人身心健康的内容等。

中央网信办有关负责人强调，各地网信部门要充分认识专项行动对于防范AI技术滥用风险，维护网民合法权益的重要意义。切实履行属地管理责任，督导网站平台对照专项行动有关要求，健全AI生成合成内容审核机制，提升技术检测能力，做好整改落实。加强人工智能相关政策的宣传推

广和人工智能素养的科普教育，引导各方正确认识和应用人工智能技术，不断凝聚治理共识。

4. 移动互联网未成年人模式正式发布

4 月 29 日上午，移动互联网未成年人模式在第八届数字中国建设峰会主论坛上正式发布。

立足未成年人网络保护现实需要、回应社会各界期待关切，国家网信办持续指导国内软硬件企业共同推进移动互联网未成年人模式（以下简称“未成年人模式”）建设工作。今年 4 月，未成年人模式突破一系列技术瓶颈，实现了全方位优化和系统性升级。

发布仪式全面展示了未成年人模式的特色亮点和主要功能。从操作方式看，移动智能终端、应用程序、应用程序分发平台实现三方联动，大大降低了模式的使用门槛。家长可在手机端显著位置点击图标，“一键启动”未成年人模式，所有应用程序同步切换，形成一个相对独立、安全可控的上网环境。从内容生态看，适合未成年人的优质内容得到大幅扩充，重点平台依托儿童内容创作者、版权资源、权威机构等，筛选海量内容纳入未成年人模式，并建立年龄分层、内容分类、推荐分众的梯度化内容体系，更好满足未成年人的精神文化需求。从功能服务看，未成年人模式可以提供每日上网总时长控制、使用时段设置、休息提醒、应用管理、使用情况统计等功能，家长可根据实际情况调整各项设置，实现对未成年人上网行为的合理引导。从覆盖范围看，华为、OPPO 和中兴在手机系统更新后提供未成年人模式，小米、荣耀和 vivo 在发布的新机上搭载未成年人模式，应

用商店建立未成年人专区，短视频、社交、电商、教育、工具等领域重点应用程序全面升级未成年人模式。后续模式的覆盖范围还将持续扩大，满足未成年人日常使用需求、提供丰富多元服务。

国家网信办相关负责人表示，充分发挥未成年人模式保护作用，离不开各方面的共同努力。一方面，将持续指导和支持鼓励平台优化未成年人模式，让这一技术工具更易用更好用。另一方面，希望广大家长和未成年人主动开启未成年人模式，提出宝贵意见，共同营造安全健康、清朗向上的网络环境。

行业前沿观察三：各地协会动态

导读：各地协会活动精彩纷呈，开展主题当日活动，开设大讲堂，举行培训会等。广东省网络空间安全协会党支部举行“全民国家安全教育 走深走实十周年”主题党日活动；2025 第九届丝绸之路网络安全论坛将于 5 月在西安举办；湖南省网络空间安全协会举办 2025 年第 1 期网络与信息安全管理员高级研修班；2025 年湖北卫生健康行业网络安全攻防培训在汉举行；苏州市互联网协会举办 AI 赋能高效办公与职场进阶培训活动；上海市信息网络安全管理协会举办四届四次会员大会暨新耀东方大讲堂；湖南省网络空间安全协会数据合规实践（研究）基地首期活动圆满收官；上海市信息安全行业协会数据安全官、数据安全评估师私享会（上海站）圆满举行；湖北省网络和数据安全协会牵头举办“应急通信与大数据应用论坛”；重庆信息安全产业技术创新联盟举办“拥抱 AI，拥有未来”DeepSeek 技术沙龙；广东省网络空间安全协会和广州网络空间安全协会举行 2024 年度广东省及广州市网络空间安全工程职称申报医疗系统专场培训会等。

关键词：年会、会长会议、团体标准、网络安全、信息安全

1. 广东省网络空间安全协会党支部举行“全民国家安全教育 走深走实十周年”主题党日活动

4 月 15 日是第十个全民国家安全日。为深入学习贯彻总体国家安全观，推动开展全民国家安全教育走深走实，4 月 27 日，广东省网络空间安全协会党支部组织开展“全民国家安全教育走深走实十周年”主题党日活动。活动期间举行学习会，回放新闻联播《习近平主持二十届中共中央政治局第十九次集体学习并发表重要讲话》短视频，深入学习习近平总书记在中央政治局第十九次集体学习时的重要讲话精神。活动以线下线上形式举行。协会党支部书记、会长林勇忠在线出席活动。协会常务副会长方满意、秘书长周贵招、支部委员黎明瑶与协会党员、发展对象、入党积极分子参加活动。协会党支部专职副书记、执行秘书长黄汝锡主持活动。

学习会结合网络空间安全领域实际，探讨了如何进一步发挥行业优势，聚焦网络安全，筑牢网络安全防线，为维护国家安全贡献力量。大家表示要深刻领会把握平安中国建设只能加强、不能削弱的重要要求，持续强化维护国家安全的政治自觉、思想自觉、行动自觉，一起努力践行守护网络空间安全，共同筑牢网络安全防线，让数字时代的国家安全坚如磐石，围绕实现好、维护好、发展好最广大人民根本利益，坚持和发展新时代“枫桥经验”，助力建设人人有责、人人尽责、人人享有的社会治理共同体，坚定不移贯彻总体国家安全观，积极为建设更高水平平安中国做贡献。

2. 2025 第九届丝绸之路网络安全论坛将于 5 月在西安举办

在数字化浪潮席卷全球的当下，网络安全已成为数字经济稳健前行的关键保障。据悉，备受瞩目的 2025 第九届丝绸之路网络安全论坛，暂定于 5 月 29 日在西安隆重举办。此次论坛将以“AI 赋能安全，共筑数字未来”为主题，汇聚行业顶尖智慧，深入探讨人工智能时代的网络安全新趋势与新挑战。

论坛由陕西省信息网络安全协会主办，获得了陕西省委网信办、陕西省公安厅、陕西省国家密码管理局、陕西省工业和信息化厅、陕西省网络社会组织联合会等多方大力指导与支持，历经八届的沉淀与发展，丝绸之路网络安全论坛已成为国内极具影响力的网络安全交流盛会，为推动我国网络信息安全领域 “产、学、研、用” 的深度融合及国际交流合作搭建了重要平台。

3. 湖南省网络空间安全协会举办 2025 年第 1 期网络与信息安全管理员高级研修班

近日，湖南省网络空间安全协会（以下简称“协会”）2025 年第一期网络与信息安全管理员高级研修班在协会网络空间安全人才培训专委会主任单位湖南云畔网络科技有限公司正式开班，20 余名来自企业从事网络安全从业者、行业精英进阶者、网络安全部门负责人、技术总监等人才参加培训。培训结束后开展职业技能等级认定。

本次培训为期 2 天，采用“理论+实操”相结合的教学模式，围绕当前网络安全面临的问题与挑战、我国大力推进网络安全建设的重要性、网络

安全的防范与建设等内容进行了重点讲述。培训内容针对性强，指导性高，有效帮助学员进一步规范网络安全行为、安全防范意识，为创建安全、和谐、稳定的工作环境打下了坚实的基础。

4. 2025 年湖北卫生健康行业网络安全攻防培训在汉举行

5 月 6 日，由湖北省卫健委指导、省网络和数据安全协会医卫分会承办的 2025 年湖北卫生健康行业网络安全攻防培训，在省网络和数据安全协会顺利开展，省内卫生健康行业专业人士参训。

此次培训通过“理论+实战”模式，为湖北卫生健康行业网络安全人才培养奠定基础，也为全国攻防储备了人才。下一步，协会及医卫分会将开展常态化技术培训与攻防演练，推动形成“主动防御、协同共治”的安全防护格局，为群众健康信息安全提供坚实保障。

5. 苏州市互联网协会举办 AI 赋能高效办公与职场进阶培训活动

4 月 30 日，苏州市互联网企业行业党建专委会、苏州市商务楼宇行业党建专委会联合市互联网协会在国际大厦开展 AI 赋能高效办公与职场进阶培训活动，50 余家楼宇、互联网企业超 60 人参与。

此次活动以 “党建 + 技术” 模式精准匹配企业需求，助力提升企业职工 AI 应用水平，推动楼宇与互联网企业探索 “人工智能 +” 高质量发展新路径。

6. 上海市信息网络安全管理协会举办四届四次会员大会暨新耀东方大讲堂

4 月 25 日，上海市信息网络安全管理协会四届四次会员大会暨新耀东方大讲堂在普陀区图书馆举办。协会成立至今已 15 周年了，本次会员大会不仅是对过往成绩的回顾与总结，更是对未来发展的展望与规划。

大会以举手表决的方式通过了理事会的工作报告和财务报告、监事会工作报告等事宜。

大会还汇报了新耀东方-2025 第四届上海网络安全博览会筹备情况。前三届新耀东方上安会通过展示前沿技术、探讨热点话题，有力地推动了上海市乃至全国网络安全产业的发展。新耀东方上安会将于 2025 年 6 月 5 日—7 日在上海新国际博览中心举办。

7. 湖南省网络空间安全协会数据合规实践（研究）基地首期活动圆满收官

4 月 25 日，由湖南省网络空间安全协会主办、北京浩天（长沙）律师事务所承办的数据合规实践（研究）基地第一期主题分享活动成功举办。

活动聚焦《生成式人工智能极速发展面临的法律风险和合规实践》主题，众多金融、科技、新媒体、教育等行业专家、协会各会员单位代表齐聚一堂，展开深度研讨与思想碰撞，为人工智能领域的合规发展提供新思路。活动的成功举办，不仅为行业搭建了一个高质量的交流平台，也为数据合规实践（研究）基地后续工作的开展奠定了良好基础。

8.上海市信息安全行业协会数据安全官、数据安全评估师私享会（上海站）圆满举行

4月25日，由众研社、上海市信息安全行业协会、上海金融信息行业协会主办的“第六期-DSO/DSA私享交流会（上海站）”圆满举行。活动现场，来自全国各地40多位学员热情满满，积极交流。深度剖析AI全生命周期风险管控与数据安全实践。

活动中，参会学员分为6组聚焦“AI客服数据泄露”“医疗影像误诊诉讼”“自动驾驶数据跨境违规”三大议题，展开沉浸式AI危机模拟数据安全攻防演练。活动期间还进行了《AI技术在金融行业数据保护中的应用和实践》《AI融合数据治理与安全保障，探寻医药智造与创新变革》《金融科技风险数据安全ABC解决方案》演讲分享。

9.湖北省网络和数据安全协会牵头举办“应急通信与大数据应用论坛”

4月25日，作为2025世界大安全博览会暨第五届武汉国际安全应急博览会同期“应急大家谈”系列活动的重磅环节，由湖北省网络和数据安全协会联合湖北省应急救援协会、中国电信湖北分公司主办的“应急通信与大数据应用论坛”在武汉国际博览中心成功举办。

来自政府、企业、科研机构的权威专家及行业代表齐聚一堂，围绕深化应急管理领域科技创新，推动大数据、北斗导航、空天地一体化等前沿技术与应急管理深度融合展开深入探讨。

10.重庆信息安全产业技术创新联盟举办“拥抱 AI，拥有未来”DeepSeek 技术沙龙

近日，由重庆信息安全产业技术创新联盟主办，联通（重庆）产业互联网有限公司、重庆奇安信科技有限公司承办的 “拥抱 AI，拥有未来”DeepSeek 技术沙龙圆满落幕。

会议上发表了《人工智能大模型的发展与变革》主题演讲，由浅到深剖析了人工智能大模型发展趋势，为参会者清晰勾勒出大模型的变革脉络，并详细介绍了联通大模型在办公、政务、医疗、公共安全等领域的应用成果。发表了《探索人工智能时代下的网络安全》主题演讲，针对人工智能时代下网络安全面临的新挑战，分享了 AI 技术在网络安全领域的应用成果与实践经验，探讨如何借助 AI 提升网络安全防护水平，为行业筑牢安全防线。

11.广东省网络空间安全协会和广州网络空间安全协会举行 2024 年度广东省及广州市网络空间安全工程职称申报医疗系统专场培训会

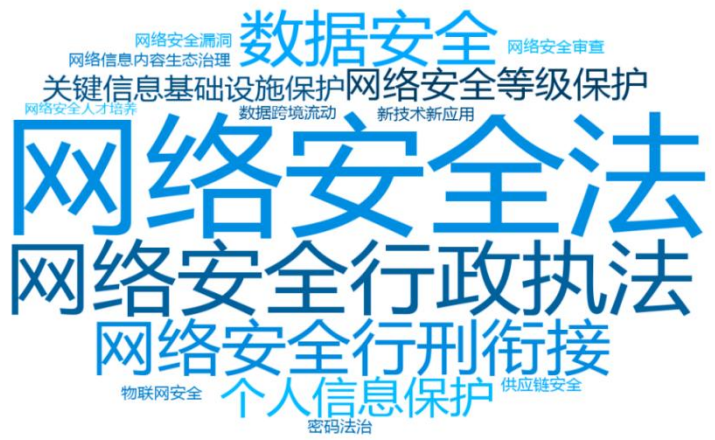
为帮助广大专业技术人员准确把握职称评审政策动态，提升申报竞争力，4 月 8 日，由广东省网络空间安全协会和广州网络空间安全协会主办的网安联•南粤网安系列活动（2025 年第 2 期）——“2024 年度广东省及广州市网络空间安全工程职称申报医疗系统专场培训会”在广州医科大学附属第一医院(大坦沙院区)学术交流中心召开。协会副会长黄志豪、高宁等人

员出席培训会。来自省、市各医疗系统单位有意申报职称评审的多名专业技术人员参加培训会。

公安部第三研究所网络安全法律研究中心

2016年2月，公安部第三研究所正式成立“网络安全法律研究中心”。 中心成立以来，聚焦前瞻性研究，切实践行理论研究与立法实践深度结合，跟踪研判国内外网络安全事件，深度分析国外网络安全战略、政策和立法动向，动态关注新技术新应用发展及安全风险，并持续推动科研成果应用于网络安全相关立法活动，在国内网络安全法律方面的影响力逐步提升。同时投身警务实践活动和公安一线服务，为公安部门提供立法动态研判和决策研究支撑。

基础性	专业性	针对性



推动立法、服务实务、智库支撑

联系方式

电子邮箱：cslaw@gass.ac.cn　　咨询电话：王老师 18817309169

网络与数据安全法律合规咨询服务

提供《网络安全法》《数据安全法》《密码法》《个人信息保护法》及配套制度为核心的数据安全保护合规体系建设，包括但不限于帮助企业落实网络安全等级保护、关键信息基础设施安全保护、网络安全审查、数据出境安全风险评估、数据交易安全保障、安全事件应急处置等要求。
开展个人信息、重要数据、核心数据等数据安全合规自查、合规差距性分析，发现、识别、分析、研判、控制数据收集、存储、使用、加工、传输、提供、公开等全生命周期的法律风险，提供法律意见和整改建议。

数据安全合规体系构建

为企业提供网络安全漏洞发现与披露、漏洞扫描与渗透测试等安全测试、“白帽子”与众测等业务场景下的合规体系构建，帮助企业厘清行为边界，避免经营风险。

安全测试法律合规体系构建

开展情况调研，评估拟出境活动风险，发现安全风险并提供整改建议，根据客户整改落实情况，出具数据出境安全风险评估报告。

数据出境安全风险评估咨询服务

帮助企业构建事先防范网络安全、数据安全行政与刑事风险框架，指导企业如何正确配合监督检查、理解执法要求等。

网络安全、数据安全执法调查与刑事风险的防范与处置意见

针对《个人信息保护法》第五十五条规定的个人信息处理情形，帮助企业开展个人信息保护影响评估，履行个人信息保护义务。

个人信息保护影响评估/合规审计咨询服务

结合行业特点，为企业提供个性化、专业化网络安全、数据安全法律法规专业培训，结合案例帮助企业正确理解与适用现有法律法规。

网络安全、数据安全法律法规专业培训

数据出境安全风险评估咨询服务

近年来，我国在国家数据安全和个人信息保护的顶层设计布局下，加快数据出境相关立法，数据出境规则体系不断完善，数据出境安全评估成为数据出境的重要路径。2022年7月7日，国家互联网信息办公室发布《数据出境安全评估办法》，落实《网络安全法》《数据安全法》《个人信息保护法》上位法要求，明确数据出境安全评估相关规定。在此形势下，企业普遍面临出境数据识别难、出境风险评估难、申报材料填报难等难题。为帮助企业解决以上难题，及时履行数据出境安全评估申报义务，公安部第三研究所网络安全法律研究中心特推出**数据出境安全风险评估咨询服务。**

数据出境活动

1 境内运营中收集和产生的数据传输、存储至境外

2 数据存储在境内，境外的机构、组织或者个人可以访问或者调用

数据出境安全风险评估咨询服务流程

01 情况调研 — 1 - 3 周

- 开展合规差距分析
- 识别安全风险并划定风险等级
- 针对安全风险提供整改建议

02 风险评估 — 3 - 5 周

03 指导落实整改 — 周期视情况而定

04 出具风险评估报告 — 1 - 2 周

- 结合客户落实整改情况，出具《数据出境风险评估报告》

合规咨询服务项目

中心已为互联网、银行、服装、签证、传统制造业等分属不同行业类别的企业提供APP合规咨询、个人信息保护（隐私政策）评估、个人信息保护合规整改、数据出境安全风险自评估等方面的合规咨询服务，合规咨询服务能力得到客户一致认可。

典型项目

- 某互联网公司APP合规咨询
- 某银行个人信息保护（隐私政策）评估
- 某跨国服装零售企业个人信息保护合规整改
- 某签证跨国集团数据出境安全风险评估咨询
- 某传统制造业跨国集团数据出境安全风险评估咨询

……