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10月第10期（总第27期）

2025年10月15日

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：政策立法

导读：9 月，网络安全保护、数据跨境流动、网络平台治理、公共数据登记管理等方面是国家和地方政策立法重点关注内容，在配套规章、制度层面规定更加细致。

国家层面，网络安全法修正草案首次提请全国人大常委会会议审议。此次修改重点强化网络安全法律责任，加大对违法行为处罚力度，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，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。

部委层面，国家互联网信息办公室发布《国家网络安全事件报告管理办法》，对网络安全事件的报告主体、报告流程、报告时限等提出规范要求，明确涉及关键信息基础设施的网络安全事件，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。平台治理方面，国家互联网信息办公室先后发布两项征求意见稿，其中《大型网络平台设立个人信息保护监督委员会规定（征求意见稿）》明确个人信息保护监督委员会的组成模式、成员职责等；《未成年人用户数量巨大和对未成年人群体具有显著影响的网络平台服务提供者认定办法（征求意见稿）》明确未成年人用户数量巨大和对未成年人群体具有显著影响的网络平台服务提供者的认定标准、程序启动、论证与决定等内容。此外，商务部等九部门印发《关于促进服务出口的若干政策措施》，要求促进和规范数据跨境流

动，提出优化调整和动态更新自由贸易试验区数据出境负面清单，研究探索形成全国自由贸易试验区数据出境负面清单。

地方层面，浙江省通过《浙江省实施〈中华人民共和国反电信网络诈骗法〉办法》，是全国范围内第一部反诈领域的地方性法规。宁夏回族自治区、云南省主要围绕公共数据资源登记管理推进政策立法。《宁夏回族自治区公共数据管理办法（试行）》印发，规定公共数据采集、资源登记、汇聚治理、共享开放等内容。云南省数据局发布《云南省公共数据资源登记实施细则（试行）（公开征求意见稿）》，明确责任分工、登记管理、登记程序等内容。

关键词：网安法修正、网络安全事件报告；平台治理；数据跨境流动

（一）国家层面动向

1. 网络安全法修正草案首次提请全国人大常委会会议审议，审议后再次公开征求意见

9月8日，网络安全法修正草案首次提请全国人大常委会会议审议。此次修改重点强化网络安全法律责任，加大对违法行为处罚力度，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，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。

全国人大常委会法制工作委员会副主任王瑞贺在向常委会会议作说明时表示，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。为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。

在完善不依法履行网络运行安全保护义务行为的法律责任方面，修正草案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。

在完善不依法履行违法信息处置义务行为的法律责任方面，修正草案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。

9 月 12 日，中国人大网公布网络安全法（修正草案）征求意见，征求意见时间为 2025 年 9 月 12 日至 2025 年 10 月 11 日。（来源：中国网信网、中国人大网）

2. 中国发布《携手构建中非网络空间命运共同体行动计划（2025-2026）》

9 月 28 日消息，中国近日发布《携手构建中非网络空间命运共同体行动计划（2025-2026）》，提出五项行动计划，包括数字经济发展行动、网络安全保障行动、人工智能治理行动等。

网络安全保障行动方面，《计划》提出，加强网络安全应急响应合作。支持鼓励中国国家计算机网络应急技术处理协调中心（CNCERT）与更多的非洲国家级应急响应组织（CERT）建立联系，开展跨境事件处置和经验交流，签署合作文件。

人工智能治理行动方面，《计划》提出，深化人工智能对话合作、交流互鉴，探讨推动人工智能在公共领域发挥更大作用，促进智能技术造福于人类，推动构建中非网络空间命运共同体，携手迈进更加美好的“数字未来”。（来源：网信中国）

（二）部委层面动向

1. 国家密码管理局发布《国家密码管理局商用密码行政检查事项清单》

9月2日，国家密码管理局发布《国家密码管理局商用密码行政检查事项清单》，明确九项行政检查事项，分别是：

一是依据《商用密码管理条例》第九条、第四十三条，对法律、行政法规和国家有关规定要求使用商用密码进行保护的网络与信息系统所使用的密码算法、密码协议、密钥管理机制等商用密码技术的监督检查。

二是依据《密码法》第二十四条和《商用密码管理条例》第十条、第十一条、第四十三条，对商用密码标准实施的监督检查。

三是依据《密码法》第二十五条和《商用密码管理条例》第十三条、第四十三条、第五十条等，对向社会开展商用密码检测活动的机构是否具备商用密码检测机构资质的监督检查。

四是依据《密码法》第二十五条、第三十五条和《商用密码管理条例》第十四条、第十六条、第四十三条、第四十七条、第五十一条，对商用密码检测机构开展商用密码检测的监督检查。

五是依据《电子签名法》第十七条和《商用密码管理条例》第二十二条、第二十三条、第四十三条、第五十四条，对电子认证服务机构使用密码的监督检查。

六是依据《密码法》第二十九条、第三十九条和《商用密码管理条例》第二十四条、第四十三条、第五十条，对从事电子政务电子认证服务的机构是否具备电子政务电子认证服务机构资质的监督检查。

七是依据《密码法》第二十九条和《商用密码管理条例》第二十五条、第二十八条、第四十三条、第四十七条、第五十五条，对电子政务电子认证服务机构开展电子政务电子认证服务的监督检查。

八是依据《密码法》第二十九条和《商用密码管理条例》第三十条、第四十三条、第五十七条，对政务活动中电子签名、电子印章、电子证照等涉及的电子认证服务使用的监督检查。

九是依据《密码法》第二十七条、第三十七条和《商用密码管理条例》第三十八条、第三十九条、第四十一条、第四十三条、第六十条、第六十二条、第六十四条，对法律、行政法规和国家有关规定要求使用商用密码进行保护的网络与信息系统商用密码使用的监督检查。（来源：国家密码管理局）

2. 国家发展改革委等六部门印发《关于加强数字经济创新型企业培育的若干措施》

9 月 4 日，国家发展改革委、国家数据局、财政部等六部门印发《关于加强数字经济创新型企业培育的若干措施》。文件指出，数字经济创新型企业是以数据为关键生产要素，以数字技术创新、应用场景创新、数据价值创新为核心驱动力，具备高敏捷性和高成长性的企业，是发展新质生产力的重要实践主体。

为加强数创企业培育，文件提出健全数创企业源头发现机制、强化多维用数保障、强化算力资源供给支撑、强化企业出海服务、建立开放包容审慎的创新环境等十项措施。

强化多维用数保障方面，文件提出，在保障数据安全合规前提下，支持数创企业公平参与公共数据资源开发利用，探索以成本共担、收益共享等方式，保障数创企业开展公共数据资源开发利用创新实践早期用数需求。

建立开放包容审慎的创新环境方面，文件提出，结合企业行业特点，稳慎探索推行“沙盒监管”模式，分级分类制定“沙盒监管”规则，鼓励在风险可控的前提下开展先行先试。规范涉企检查，推进精准检查，防止重复检查、多头检查，探索推行非现场监管，最大限度减少对企业生产经营的不必要干扰。引导数创企业守法自律经营，探索柔性执法机制，对首次轻微违规问题依法优先采取引导协商、行政指导、信用承诺等方式处理。（来源：中国政府网）

3. 国家能源局综合司发布《能源行业数据安全管理办法（试行）（征求意见稿）》

9 月 10 日，国家能源局综合司发布《能源行业数据安全管理办法（试行）（征求意见稿）》。征求意见稿共六章三十六条，涉及能源行业数据安全基本职责、能源行业数据保护要求、能源行业数据安全监测预警和应急处置等内容。

征求意见稿规定，存储处理能源行业重要数据的信息网络应落实三级及以上网络安全等级保护要求；存储处理能源行业核心数据的信息网络，

如涉及关键信息基础设施，应在网络安全等级保护制度的基础上，落实关键信息基础设施安全保护要求；不涉及关键信息基础设施的，应落实四级网络安全等级保护要求。

征求意见稿明确核心数据保护义务，要求能源行业核心数据的处理者在落实以上能源行业重要数据保护要求的基础上，可以采取以下措施加强对能源行业核心数据的保护：（1）优先使用商用密码进行保护；（2）优先使用安全可信的产品和服务；（3）优先使用第三方评估机构开展风险评估；（4）涉及核心数据安全事件处置、溯源的相关日志，留存时间不少于三年；（5）对相关关键岗位人员、涉及核心数据信息系统建设和运维单位等，依法依规提交公安机关、国家安全机关进行国家安全背景审查。（来源：国家能源局）

4. 国家互联网信息办公室发布《国家网络安全事件报告管理办法》

9 月 11 日，国家互联网信息办公室发布《国家网络安全事件报告管理办法》，自 2025 年 11 月 1 日起施行。《办法》共十四条，主要对网络安全事件报告的报告主体、报告流程、报告时限等提出规范要求。

《办法》规定，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》进行研判，属于较大以上网络安全事件的，按程序报告：

（1）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。

（2）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。

（3）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。

《办法》提出，报告网络安全事件时，应当包括：（1）涉事单位名称及涉事系统或设施基本情况；（2）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；（3）事态发展趋势及可能造成的进一步影响和危害；（4）网络安全事件原因初步分析意见；（5）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；（6）拟进一步采取的应对措施以及请求支援事项；（7）网络安全事件现场保护情况；（8）其他应当报告的情况。（来源：国家互联网信息办公室）

5. 国家互联网信息办公室发布《大型网络平台设立个人信息保护监督委员会规定（征求意见稿）》

9 月 12 日，国家互联网信息办公室发布《大型网络平台设立个人信息保护监督委员会规定（征求意见稿）》，共三十一条。

征求意见稿指出，个人信息保护监督委员会是指由大型网络平台服务提供者成立的，主要由外部成员组成的，对大型网络平台个人信息保护情况进行监督的独立机构。其中，个人信息保护监督委员会外部成员，是指具备个人信息保护专业知识和技能，不在受聘大型网络平台担任除监督委员会成员外的其他职务的人员。

征求意见稿规定，监督委员会重点对大型网络平台下列事项进行监督：（1）个人信息保护合规制度体系建设情况；（2）平台或产品个人信息保护规则制修订情况；（3）敏感个人信息保护情况；（4）个人信息保护影响评估开展情况；（5）个人信息保护合规审计开展情况；（6）落实监管机构提出的整改要求情况；（7）个人信息安全事件处理情况；（8）个人行使个人信息权益保障情况；（9）向境外提供个人信息合规情况；（10）个人信息保护社会责任履行及报告发布情况；（11）个人信息保护负责人履行职责情况；（12）利用个人信息进行自动化决策等情况；（13）与个人信息保护相关的其他重大事项；（14）法律、行政法规规定的其他监督事项。

征求意见稿明确，监督委员会成员在履行职责过程中发现大型网络平台个人信息处理活动存在风险或违法违规收集处理个人信息等问题的，应

当向监督委员会和大型网络平台服务提供者提出书面建议。监督委员会和大型网络平台服务提供者未处理的，或成员对处理结果有异议的，成员应当向所在地省级网信部门报告。（来源：网信中国）

6. 国家互联网信息办公室发布《促进和规范电子单证应用规定（征求意见稿）》

9 月 13 日，国家互联网信息办公室发布《促进和规范电子单证应用规定（征求意见稿）》。征求意见稿共五章二十五条，包括电子单证应用的促进、电子单证系统的可靠性、安全性等内容。

征求意见稿指出，电子单证是指采用数据电文形式，能够证明当事人之间存在货物运输、仓储、货物保险等法律关系的单证，包括电子提单、电子多式联运单证、电子海运单、电子铁路货运单、电子航空货运单、电子仓单、电子货物保险单等。电子单证包括可转让电子单证和不可转让电子单证。电子单证系统是指基于网络信息技术，为接收、存储和发送电子单证信息提供技术服务的信息系统。

征求意见稿提出，鼓励相关机构、组织和个人通过可靠的电子单证系统从事电子单证的签发、存储、变更、转换、转让、质押、流转等活动。可靠的电子单证系统应实现以下功能：（1）确保电子单证信息全程可追溯，不可篡改；（2）能够识别电子单证的签发人；（3）若支持电子单证和纸质单证相互转换，应确保转换前后的信息一致，并在单证中体现相关转换信息。

征求意见稿规定，向境外提供与电子单证有关的数据，应当符合国家关于数据出境的相关规定。国际贸易、跨境运输过程中收集和产生的与电子单证相关的数据向境外提供，如果不包含个人信息或重要数据，或者所涉个人信息仅为签发、转让、质押电子单证或行使电子单证权利所必需的，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。（来源：网信中国）

7. 国家互联网信息办公室发布《未成年人用户数量巨大和对未成年人群体具有显著影响的网络平台服务提供者认定办法（征求意见稿）》

9 月 16 日，国家互联网信息办公室发布《未成年人用户数量巨大和对未成年人群体具有显著影响的网络平台服务提供者认定办法（征求意见稿）》。征求意见稿共六章十九条，包括认定标准、程序启动、论证与决定等内容。

征求意见稿规定，网络平台提供的产品或者服务专门以未成年人为服务对象，注册用户在 1000 万以上或者月活跃用户在 100 万以上，或者服务对象不局限于未成年人，但未成年人注册用户数量在 1000 万以上或者月活跃未成年人用户在 100 万以上的，应当认定为未成年人用户数量巨大的网络平台服务提供者。

征求意见稿提出，认定对未成年人群体具有显著影响的网络平台服务提供者，应当综合考虑：（1）该网络平台下载量、注册用户数量、月活跃用户数量规模较大，或网络产品的销售额、交易量等较大；（2）该网络平

台未成年人登录频次、使用时长、喜爱程度、消费金额等指标较高；（3）该网络平台涵盖大量涉及或面向未成年人的信息内容；（4）该网络平台在3年内存在较多涉未成年人突出情况，违法违规问题较为突出，受到社会广泛关注；（5）该网络平台在相关垂直领域排名靠前；（6）其他对未成年人群体具有显著影响的因素。（来源：网信中国）

8. 商务部等九部门印发《关于促进服务出口的若干政策措施》，提出促进和规范数据跨境流动

9月22日，商务部、中央网信办、财政部等九部门印发《关于促进服务出口的若干政策措施》，提出十三项措施，其中包括促进和规范数据跨境流动。

《措施》提出，制订重要数据目录，出台更具操作性的重要数据识别指南。优化调整和动态更新自由贸易试验区数据出境负面清单，研究探索形成全国自由贸易试验区数据出境负面清单。支持具备条件的地区探索跨国公司内部个人信息跨境传输便捷化安排，允许通过评估或认证的跨国公司内部自由跨境流动个人信息。在遵守国家网络管理制度前提下，支持相关企业、科研机构更便利地使用网络开展国际贸易和学术研究，参与国际竞争。（来源：商务部）

9. 《数据安全国家标准体系（2025 版）》《个人信息保护国家标准体系（2025 版）》印发

9 月 15 日，全国网安标委印发《数据安全国家标准体系（2025 版）》《个人信息保护国家标准体系（2025 版）》。

其中，数据安全国家标准体系以数据为核心，以数据分类分级保护为基础，覆盖数据收集、存储、使用、加工、传输、提供、公开、删除等全流程数据处理活动，标准化对象涉及与数据紧密相关的组织、产品、服务、系统、技术、管理、活动等。数据安全国家标准体系由基础共性、数据安全技术和产品、数据安全管理、数据安全服务、产品和服务数据安全、行业与应用数据安全六大类标准组成。

个人信息保护国家标准体系在数据安全国家标准体系的基础上，以个人信息权益保护为核心，涉及与个人信息紧密相关的组织、产品、服务、系统、活动、技术、管理等标准化对象，涵盖个人信息收集、存储、使用、加工、传输、提供、公开、删除等处理活动，保障个人信息的知情权、决定权、限制处理、拒绝处理等权利。个人信息保护国家标准体系由基础共性、个人信息保护技术、个人信息保护管理与权益保障、个人信息保护测评和认证、产品和服务个人信息保护、行业与应用个人信息保护六大类标准组成。（来源：全国网安标委）

10. 2 项网络安全国家标准和 4 项网络安全标准实践指南发布

9月,由全国网络安全标准化技术委员会归口的2项国家标准正式发布，分别是：（1）GB/T 46068-2025《数据安全技术 个人信息跨境处理活动安

全认证要求》；（2）GB/T 46071-2025《数据安全技术 数据安全和个人信息保护社会责任指南》。

此外，4 项网络安全标准实践指南发布，分别是：（1）《网络安全标准实践指南——学术科技服务平台数据安全要求》；（2）《网络安全标准实践指南——扫码点餐个人信息保护要求》；（3）《网络安全标准实践指南——互联网平台停服数据处理安全要求》；（4）《网络安全标准实践指南——生成式人工智能服务安全应急响应指南》。（来源：全国网安标委）

（三）地方层面动向

1. 宁夏回族自治区印发《宁夏回族自治区公共数据管理办法（试行）》

9 月 21 日，宁夏回族自治区发展改革委印发《宁夏回族自治区公共数据管理办法（试行）》，自 2025 年 11 月 1 日施行，有效期至 2027 年 10 月 31 日。《办法》共十章四十五条，包括公共数据采集、公共数据资源登记、公共数据汇聚治理、公共数据共享开放等内容。

《办法》规定，公共数据采集实行统一目录管理。公共数据目录应当包括数据来源、采集方式、更新频率、数据类型、共享开放属性等内容，并明确能否授权运营。自治区数据管理部门统筹推进全区公共数据资源目录一体化建设，会同数据中心等相关部门制定公共数据资源目录编制指南。市、县（区）数据管理部门应当按照统一标准，组织编制本级公共数据资源目录，并报上级数据管理部门审核。公共管理和服务机构应当按照公共

数据资源目录编制指南，编制本部门公共数据资源目录，并报同级数据管理部门审核。

《办法》提出，公共数据按照开放属性分为无条件开放、有条件开放和不予开放3种类型。属于有条件开放类的，申请使用单位或个人可按程序提出申请，明确用途、使用期限以及应用场景等内容，经公共管理和服务机构审核同意后开放，并承诺合法、安全使用获得的数据，不得以任何形式提供给第三方使用，不得用于其他用途或者场景。不予开放类公共数据通过脱密、脱敏等技术处理后，经相关权利人同意的，可以列入无条件开放或者有条件开放类。（来源：宁夏回族自治区发改委）

2. 福建省印发《福建省促进数据产业高质量发展行动计划（2025—2027年）》

9月24日，福建省发展和改革委员会、福建省数据管理局印发《福建省促进数据产业高质量发展行动计划（2025—2027年）》，围绕“数产集聚”行动、“数企繁荣”行动、“数据赋智”行动等七方面提出二十一项措施。

实施“数值释放”行动，加速数据要素价值释放方面，《计划》提出深化公共数据开发利用。推进公共数据汇聚治理，建设福建省“一数一源”标准，推动公共数据“一本账”管理、“一平台”运营、“一体化”应用。健全省市一体开发机制，优化公共数据资源授权运营机制，探索完善价格形成机制。

实施“数据筑基”行动，全面提升基础核心能力方面，《计划》提出提高数据安全保障能力。加强数据脱敏、数据水印、数据安全态势感知等数据安全技术应用，推进隐私保护计算、区块链等数据流通利用技术部署。培育壮大适应数据流通特征的安全服务业态，支持企业创新数据分类分级、隐私保护、安全监测、应急处置、流通安全检测评估、安全审计、数据托管等数据安全产品和服务。（来源：福建省发展和改革委员会）

3. 《浙江省实施〈中华人民共和国反电信网络诈骗法〉办法》通过，系全国首部反诈领域地方性法规

9 月 26 日，浙江省第十四届人民代表大会常务委员会第十九次会议审议通过《浙江省实施〈中华人民共和国反电信网络诈骗法〉办法》，自 2025 年 12 月 1 日起施行。《办法》是全国范围内第一部反诈领域的地方性法规。

据围绕《办法》通过召开的新闻发布会介绍，近年来，电信网络诈骗犯罪已经成为发案最高、案损最大、群众反映最强烈的突出犯罪。从浙江省情况来看，案件高发态势得到一定程度遏制，但涉及浙江的整体案件数和案损价值仍处高位，打击治理电信网络诈骗形势依然严峻。制定实施办法，不仅是贯彻实施国家法的必然要求，更是积极回应反诈工作实践需要、维护人民群众合法权益的重要举措。

《办法》分别明确政府组织领导、公安机关牵头负责、金融电信等部门行业监管以及相关经营主体风险防控等方面责任，并要求有关部门和单位加强工作协作，规定浙江省公安机关应当推动省际合作，并会同有关部门建立和完善“96110”运行机制。

互联网治理方面，《办法》要求有关部门督促互联网服务提供者履行涉诈信息监测和处置等义务，指导开展电话卡与互联网账号关联的安全风险防范，并在上位法规定基础上，将涉案和涉诈异常互联网账号所关联注册的互联网账号也纳入到重新进行核验的范围。对于涉诈信息，要求互联网服务提供者加强动态监测，并明确对涉诈互联网账号、网站访问链接和应用程序的处置措施。（来源：中国新闻网、浙江人大）

4. 湖南省公布《湖南省数据条例》

9 月 26 日，湖南省第十四届人民代表大会常务委员会第十八次会议通过《湖南省数据条例》，自 2025 年 12 月 1 日起施行。《条例》共九章五十六条，包括数据权益、数据资源、数据流通等内容。

《条例》涵盖公共数据、非公共数据和衍生数据。其中，非公共数据是指公共管理和服务机构以外的自然人、法人和非法人组织依法开展活动所产生、获取或者加工处理的各类数据；衍生数据是指数据处理者对其享有使用权的数据，在保护各方合法权益前提下，通过利用专业知识加工、建模分析、关键信息提取等方式实现数据内容、形式、结构等实质改变，从而显著提升数据价值形成的数据。

《条例》规定，数据处理者对其合法取得的数据，依法享有数据持有权益，可以自主管控其持有的数据；对其合法持有的数据，依法或者按照约定享有数据使用权益，可以进行开发利用；对其合法持有的数据以及通过加工、分析等形成的数据产品和服务，包括在此过程中所形成的衍生数据，依法或者按照约定享有数据经营权益。（来源：湖南人大网）

5. 云南省发布《云南省公共数据资源登记实施细则（试行）（公开征求意见稿）》

9月26日，云南省数据局发布《云南省公共数据资源登记实施细则（试行）（公开征求意见稿）》。公开征求意见稿共六章二十四条，包括责任分工、登记管理、登记程序等内容。

公开征求意见稿指出，公共数据资源是指各级党政机关、企事业单位依法履职或提供公共服务过程中产生的具有利用价值的数据集合；登记主体是指根据工作职责直接持有或管理公共数据资源的单位，以及依法依规对授权范围的公共数据资源进行开发运营的法人组织；登记机构是指由数据管理部门设立或指定的、提供公共数据资源登记服务的事业单位；登记平台是指支撑公共数据资源登记全流程服务管理的信息化系统。

公开征求意见稿提出，直接持有或管理公共数据资源的党政机关和企事业单位，应对纳入授权运营范围的公共数据资源进行登记，鼓励对未纳入授权运营范围的公共数据资源进行登记。经授权开展运营活动的法人组织，应对利用被授权的公共数据资源加工形成的数据产品和服务进行登记。

公开征求意见稿规定，登记结果有效期为三年，自赋码之日起计算。对授权运营范围内的公共数据产品和服务登记，根据授权协议运营期限不超过三年的，登记结果有效期以实际授权运营期限为准。登记结果可作为数据交易、数据要素型企业认定等的可信依据。登记主体可在登记结果有效期满前60日内按照规定续展。每次续展期最长为三年，自上一届有效期

满次日起计算。期满未按规定续展的，由登记机构予以注销。（来源：云南省发改委）

6. 重庆市公布《重庆市互联网信息办公室涉企行政检查事项清单》

9 月 26 日，重庆市网信办公布《重庆市互联网信息办公室涉企行政检查事项清单》。清单明确七项行政检查事项，分别是：（1）对互联网新闻信息服务活动的检查；（2）对网站平台落实信息内容管理主体责任情况的监督检查；（3）对履行预防未成年人沉迷网络义务情况开展监督检查；（4）对重要信息系统安全风险进行检查；（5）对个人信息处理活动实施监督检查；（6）对网络数据安全进行监督检查；（7）对互联网新技术新应用进行安全评估和监督检查。（来源：网信重庆）

境内前沿观察二：治理实践

导读：9 月，公安、网信、通信管理部门等机构持续发力，持续强化网络安全、数据安全、个人信息保护监督检查力度，公布一批刑事打击和行政执法典型案例，提升网络和数据安全水平，构建天朗气清的网络空间。

公安网安部门依法查处迪奥（上海）公司未依法履行个人信息保护义务案。这是自《个人信息保护法》生效以来，目前公开披露信息中为数不多的国际知名品牌因违法出境数据、违规个人信息处理等行为受到行政处罚的案件，具有非常典型的警示意义。此外，公安部及辽宁、山西等地网警公布“净网—2025”“护网—2025”等专项行动工作成效。

中央网信办部署开展“清朗·整治恶意挑动负面情绪问题”专项行动，全面排查话题、榜单、推荐、弹幕、评论等重点环节，着力整治挑动群体极端对立情绪、宣扬恐慌焦虑情绪、挑起网络暴力戾气、过度渲染消极悲观情绪四方面问题。网信部门针对快手、微博、UC、今日头条、小红书破坏网络生态的行为依法作出行政处罚。

工信部等六部门联合部署开展汽车行业网络乱象专项整治行动，将集中整治非法牟利、夸大和虚假宣传、恶意诋毁攻击等网络乱象。工信部通信管理局以及山东、浙江等地通信管理局发布侵害用户权益 APP 名单。

关键词：净网行动；护网行动；网络生态治理

（一）公安机关治理实践

1. 公安部公布三起非法破解无人机飞行控制系统黑客违法犯罪典型案例

9 月 1 日，公安部公布 3 起非法破解无人机飞行控制系统黑客违法犯罪典型案例。

案例一：浙江衢州公安机关侦破陈某强非法破解无人机飞行控制系统案。浙江衢州公安网安部门查明，2020 年 2 月以来，陈某强非法提供无人机禁飞破解服务，谋取非法利益。2024 年 6 月，浙江衢州公安机关将陈某强抓获，查获作案电脑 1 台、无人机 10 余台，查明其非法破解无人机 200 余台，非法获利共计 10 万余元。

案例二：山东临沂公安机关侦破张某玲非法破解无人机飞行控制系统案。山东临沂公安网安部门查明，2023 年 1 月以来，张某玲利用非法获取的无人机破解程序，破坏无人机飞行控制系统，谋取非法利益。2024 年 4 月，山东临沂公安机关将张某玲抓获，查明其非法破解无人机 10 余台，非法获利共计 6000 余元。

案例三：四川成都公安机关侦破陈某平非法破解无人机飞行控制系统案。四川成都公安网安部门查明，2023 年 9 月以来，陈某平多次向无人机生产公司谎报无人机丢失，利用有关服务条款漏洞获取新机后，将因报丢而被锁定的无人机的飞行控制系统进行非法破解并销售，谋取非法利益。

2024 年 9 月，四川成都公安机关将陈某平抓获，查明其非法破解无人机 5 台，非法获利共计 3 万余元。（来源：公安部网安局）

2. 公安部公布“净网—2025”专项工作十起典型案例

9 月 18 日，公安部网安局公布十起打击整治网络违法犯罪典型案例。

案例一：江苏公安机关侦破曹某某利用 AI 工具编造“泰州姜堰政府干部因食用方便面被通报”网络谣言案

江苏公安机关网安部门查明，2025 年 6 月 17 日，泰州网民曹某某为蹭热点、博眼球、吸引流量，利用 AI 工具炮制内容为“泰州姜堰顾高镇政府办公室两名干部张某某、李某某在三令五申严禁违规吃喝、厉行节约反对浪费的纪律要求下，未能严于律己、以身作则，在镇政府周边一便利店消费方便面 2 份，行为逾越了公职人员的廉洁规范，造成了不良影响，予以通报批评”的谣言信息，并在互联网平台发布，引发大量网民关注、讨论，严重扰乱公共秩序。公安机关已依法对曹某某采取刑事强制措施，并对其造谣网络账号采取关停措施。

案例二：四川公安机关侦破以“保护大熊猫”名义实施系列网络暴力案

四川公安机关网安部门查明，以陕西白某某、黑龙江周某某、四川唐某等 3 人为首的违法犯罪团伙，以“保护大熊猫”名义，长期在网上炮制炒作“大熊猫遭受虐待”“买卖熊猫皮”等谣言信息，恶意抹黑大熊猫保护国际合作成效，煽动网民对大熊猫保护工作人员实施网络暴力，并串联

实施线下滋扰活动。2025 年 4 月至 6 月，白某某、周某某、唐某分别被判处一年至一年六个月不等有期徒刑。

案例三：上海公安机关侦破跳水运动员被实施网络暴力案

2025 年 5 月，部分网民侮辱诽谤跳水运动员，引发舆论关注。上海公安机关网安部门立即对网上信息进行全面排查梳理，查明犯罪嫌疑人王某使用某短视频平台账号发布关于“某运动员被禁赛”等谣言信息和“拉踩”视频；犯罪嫌疑人韩某为博取眼球，借助 AI 编辑制作发布“某运动员向裁判长行贿”等谣言视频；犯罪嫌疑人马某某为吸粉引流，长期使用多个平台账号发布侮辱和诽谤跳水运动员视频，并公开发布多组侮辱性词汇。公安机关已依法对王某、韩某、马某某采取刑事强制措施。

案例四：北京公安机关侦破“开盒”网暴检察官案

2025 年 4 月，《央视新闻》公开报道一起恶意“开盒”案件，2 名出镜接受采访的办案检察官身份信息随即被“开盒”。北京公安机关网安部门查明上述“开盒”活动由林某某、王某某实施。经进一步深挖，查明一个以王某为首的“查档”“开盒”违法犯罪团伙。公安机关已对其中 7 人依法采取刑事强制措施，对其中 1 人依法予以教育训诫。

案例五：甘肃公安机关侦破卢某等人侵犯公民个人信息案

甘肃兰州公安机关网安部门查明，卢某等人在老旧小区、学校等区域，利用车载伪基站设备截取周边居民手机号及短信验证码从事网络账号注册贩卖活动。2025 年 4 月，公安机关抓获卢某等违法犯罪嫌疑人 12 名，查扣车载伪基站设备 7 套、作案车辆 5 台，配件 1000 余件。卢某等人因涉嫌侵犯公民个人信息罪等，已被依法移送起诉。

案例六：四川公安机关侦破张某等人侵犯公民个人信息案

四川内江公安机关网安部门查明，犯罪嫌疑人张某等人利用在某保险公司从事线上外包工作的职务之便，非法获取大量客户的公民个人信息，并通过网络兜售获利，涉案金额16万余元。张某等3人因涉嫌侵犯公民个人信息罪，已被依法移送起诉。

案例七：四川公安机关侦破王某破坏计算机信息系统案

四川德阳公安机关网安部门查明，王某利用系统漏洞非法登录某单位系统后台，执行恶意指令，上传自制勒索病毒，并自动生成匿名勒索信，牟取非法利益10余万元。王某因涉嫌破坏计算机信息系统罪，已被公安机关依法采取刑事强制措施。

案例八：安徽公安机关侦破郝某等人非法利用信息网络案

2025年3月，安徽阜阳公安机关网安部门成功破获一起利用AI仿冒银行APP并伪造交易凭证案件，查明郝某等人通过开发假冒银行APP，伪造银行交易流水、公积金流水账单、贷款结清证明等交易凭证，从中非法牟利。郝某等12人因涉嫌非法利用信息网络罪，已被公安机关依法采取刑事强制措施。

案例九：甘肃公安机关侦破罗某某非法利用信息网络案

2025年3月，甘肃天水公安机关网安部门查明，罗某某等人与多个色情网站勾连，在视频素材内加入色情网站域名水印，并组织人员通过某短视频平台发布相关视频，为色情网站推广引流，从中牟取非法利益。罗某某等3人因犯非法利用信息网络罪，分别被判处六个月至八个月不等有期徒刑。

案例十：湖北公安机关侦破徐某某等人帮助信息网络犯罪活动案

2024 年 9 月，湖北宜昌公安机关网安部门查明，徐某某等人大量购买、注册短视频平台账号，在各类短视频平台上通过伪装炒股机构专业顾问、撰写投资理财文案、编造虚假股票走势图、剪辑金融股票视频等方式发展粉丝，并将粉丝信息推送至境外诈骗集团，从中牟取非法利益。公安机关抓获徐某某等 4 名犯罪嫌疑人，现场查获作案电脑 5 台、手机 24 部，查获各类社交账号 200 余个，查明非法获利金额 180 余万元。徐某某等 4 人因犯帮助信息网络犯罪活动罪，分别被判处六个月至两年六个月不等有期徒刑。（来源：公安部网安局）

3. 公安部公布“护网—2025”专项工作六起典型案例

9 月 18 日，公安部网安局公布六起不履行网络安全、数据安全、个人信息保护义务的行政执法典型案例。

案例一：贵州公安机关侦办的某政务服务系统未采取技术防护措施被网络攻击案

2025 年 5 月，贵州某单位政务服务系统遭网络攻击，被涉诈犯罪嫌疑人利用，造成群众财产损失 400 余万元。贵州公安机关网安部门查明该系统运营者、承建方、运维方等未落实网络安全主体责任，未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，未采取监测、记录网络运行状态、网络安全事件的技术措施，未按规定留存网络日志，未及时处置系统漏洞等安全风险，造成严重后果。当地政府部门已依法对该单位直接负责的主管人员和其他直接责任人给予处分，当地公安机

关已依法对系统承建方、运维方等予以行政处罚并责令限期改正。犯罪嫌疑人已依法另案处理。

案例二：江苏公安机关侦办的某短信平台未采取技术防护措施被网络攻击案

2025 年 5 月，江苏苏州吴江某公司建设的短信群发系统被攻击冒用，并发送诈骗短信 27000 余条。江苏公安机关网安部门查明因相关短信群发平台未进行等保备案测评，未采取技术防护措施，导致被犯罪嫌疑人攻击控制，短信服务被冒用滥发。当地公安机关已依法对该系统建设运维方予以行政处罚并责令限期改正。犯罪嫌疑人已依法另案处理。

案例三：河南公安机关侦办的某学校系统遭攻击导致数据泄露案

2025 年 3 月，不法分子在境外网上兜售舞钢市某学校个人信息数据。河南公安机关网安部门查明，相关数据泄露源头为该校智慧刷卡计费系统。由于该系统存在高危漏洞且数据未采取加密存储，系统未设置访问控制、安全认证等技术措施，导致系统数据被犯罪嫌疑人网络攻击窃取，且该校在委托第三方公司处理业务数据和个人信息时，未在合同中明确接收方的数据安全保护义务并监督其履约。当地公安机关已依法对该校予以行政处罚并责令限期改正。犯罪嫌疑人已依法另案处理。

案例四：安徽公安机关侦办的某电子商务公司旅客购票信息泄露案

2025 年 5 月，安徽合肥某电子商务有限公司旗下网站内的旅客购票信息遭泄露。安徽公安机关网安部门查明，由于该公司网络和数据安全保护意识薄弱，未制定网络安全管理制度和个人信息保护制度，未开展等级保护工作，未按规定要求留存网络日志数据，未采取技术防护措施，未及时

处置系统漏洞风险，导致相关数据被犯罪嫌疑人批量爬取。当地公安机关已依法对该公司予以行政处罚并责令限期改正。犯罪嫌疑人已依法另案处理。

案例五：云南公安机关侦办的某科技公司 APP 数据泄露案

2025 年 4 月，云南公安机关网安部门集中开展侵犯公民个人信息打击整治工作，打掉一批侵犯公民信息的犯罪团伙，查明部分公民个人信息数据泄露源头为云南某科技有限公司开发的“通讯录”APP。经查，该公司因内部管理混乱，缺乏用户身份信息核对机制，对公民信息数据未尽到保护责任，保护措施不力，导致大量公民个人信息泄露，被犯罪嫌疑人非法获取并贩卖。当地公安机关已依法对该公司和实际负责人予以行政处罚并责令限期改正。犯罪嫌疑人已依法另案处理。

案例六：上海公安机关办理的某跨国公司不履行个人信息保护义务案

2025 年 5 月，多家媒体报道境外某时尚消费品牌发生数据泄露事件，中国大陆地区用户也陆续收到该公司警示短信。上海公安机关网安部门查明，该品牌中国公司未通过数据出境安全评估、订立个人信息出境标准合同或通过个人信息保护认证，违规向境外总部传输用户个人信息，未向用户充分告知其个人信息境外接收方的处理方式，未取得用户“单独同意”，未对收集的个人信息采取加密、去标识化等安全技术措施。当地公安机关已依法对该公司予以行政处罚并责令限期改正。（来源：公安部网安局）

4. 湖北公安部门侦破一起提供侵入、非法控制计算机信息系统程序、工具案

9月6日消息，湖北武汉网警近日接上海某科技公司报案：2月起，其旗下社交平台突然涌现1.7万余个“僵尸”账号，涌入大量群组疯狂推送涉黄、涉赌等非法引流广告，严重污染网络环境，威胁用户财产安全。

武汉网警调查发现一款名为“某助手”的恶意软件及其开发者袁某。经查，袁某为牟取不法利益，开发“某助手”软件，绕过平台的登录验证机制，自动化、批量登录海量账号，进行评论、点赞、群发私信等操作。目前，袁某已被依法刑事拘留。（来源：公安部网安局）

5. 公安网安部门依法查处迪奥（上海）公司未依法履行个人信息保护义务案

9月9日，国家网络与信息安全信息通报中心通报称，2025年5月，多家媒体报道法国时尚消费品牌迪奥发生数据泄露事件，中国大陆地区用户也陆续收到迪奥官方警示短信。

对此，公安网安部门组织对迪奥（上海）公司依法开展行政调查。经查，迪奥（上海）公司存在三项违法事实：一是未通过数据出境安全评估、订立个人信息出境标准合同或通过个人信息保护认证，违规向法国迪奥总部传输用户个人信息；二是向法国迪奥总部提供用户个人信息前，未向用户充分告知其个人信息境外接收方的处理方式，未取得用户“单独同意”；三是未对收集的个人信息采取加密、去标识化等安全技术措施。属地公安

机关依据《个人信息保护法》规定，对迪奥（上海）公司依法予以行政处罚。（来源：公安部网安局）

6. 新疆维吾尔自治区公安部门侦破一起侵犯公民个人信息案

9 月 10 日消息，新疆乌鲁木齐市公安网安部门近日发现有人频繁致电小初高学生家长，精准推销“私人订制”补习班，能清晰说出学生具体信息，疑似存在个人信息泄露情况。

对此，乌鲁木齐市公安机关成立专案组，迅速开展侦查工作，发现天山区两家机构存在非法购买公民个人信息的违法行为。专案组立即对涉案人员开展调查。经查，犯罪嫌疑人刘某非法收集学生个人信息，并向某机构工作人员冯某出售，冯某又将信息转卖给另一家机构工作人员邵某。目前，乌鲁木齐市公安机关已依法对刘某、冯某、邵某 3 人采取刑事强制措施，案件正在进一步侦办中。（来源：公安部网安局）

7. 安徽省公安部门打击一起利用 AI 工具编造涉企谣言案

9 月 11 日消息，安徽合肥公安网安部门近日查处一起利用网络平台故意散布涉企业不实信息的案件。

8 月 26 日，某著名食品股份有限公司向合肥市公安局经开分局报案称，近期多个网络平台上集中出现大量虚假、带有诱导性的负面文章，恶意攻击公司品牌及产品品质，导致大量消费者产生误解。公安机关调查发现，多个平台关于该品牌“二氧化硫残留”“霉变”等内容的文章 200 余篇，且内容高度雷同。经公安机关核实，上述内容均为虚假信息。

公安机关依法传唤信息发布者陈某（男，29 岁）接受调查。据陈某交代，8 月，陈某在网上看到该食品公司的相关信息后，为博取流量，使用 AI 工具编造内容，生成多篇虚假负面文章，在多个平台集中发布，造成恶劣社会影响。目前，陈某已被依法行政拘留。（来源：公安部网安局）

8. 上海市公安部门侦破一起房产公司职工出售客户信息案

9 月 12 日消息，上海市公安局奉贤分局近日在“净网 2025”专项行动中，全链条捣毁一房产交易领域侵犯公民个人信息的犯罪团伙。

2024 年 11 月 26 日，奉贤警方收到辖区一房地产经纪公司负责人报案，称其公司独家房源信息疑似遭到“泄露”，有数名业主反映屡遭不明身份的房产中介来电，干扰业主正常生活。接到报案后，奉贤警方迅速抽调网安、属地派出所等多部门警力，组成专案组展开全面侦查。

经初步调查研判，专案组很快锁定公司内部客服任某培存在重大作案嫌疑。为进一步还原犯罪事实，专案组对接公司技术团队，深入企业内部开展溯源调查，查明任某培利用职务便利，在网络平台发布所谓“可查询房源业主手机号码”的广告吸引买家，待买家明确需求房源后，任某培即通过内部工作账号调取房东电话号码，以“独家房源”为噱头，以每条 100 元至 500 元的高价出售公民个人信息。

截至案发，任某培已累计非法获取、出售公民个人信息超 1 万条，涉案资金达 300 余万元。专案组继续循线深挖，依托“科技+人力”，发现由任某培发展的周某、田某鹏、路某等 10 余名代理销售人员，层层转卖相关信息非法牟利。

2025 年 1 月，奉贤警方在全国多地公安机关配合下，开展同步收网行动，成功抓获任某培、周某等 13 名犯罪嫌疑人。经审讯，所有到案嫌疑人均有房地产销售中介从业经历，已形成信息获取、代理分销、购买使用的完整犯罪链条。2025 年 3 月至 5 月，上海警方再次组织警力前往多地实施抓捕，先后抓获 18 名下游犯罪嫌疑人。截至目前，该案共抓获犯罪嫌疑人 31 名，所有涉案人员因涉嫌侵犯公民个人信息罪，均已被依法移送检察机关审查起诉，案件后续办理工作正有序推进中。（来源：公安部网安局）

9. 陕西省公安部门侦破一起特大侵犯公民个人信息案

9 月 17 日消息，陕西公安网安部门近日成功侦破一起特大侵犯公民个人信息案，抓获 2 名主要犯罪嫌疑人，移交属地处理 260 人，查获一批涉案公民个人信息数据。

2025 年 5 月，陕西岚皋公安网安部门在工作中掌握一条涉及侵犯公民个人信息犯罪的线索。经查，该团伙组织人员在全国各类展会现场大量搜集参展商名片，并将包含姓名、电话、公司名称、职务等敏感信息整理成电子表格，数量极为庞大。

在全面掌握该团伙组织架构、作案手法、活动区域及核心证据后，网警分赴上海、广东等地同步开展收网行动，成功抓获何某等 2 名主要犯罪嫌疑人，现场查获电脑、手机、硬盘等涉案电子设备数十台。涉案公民个人信息涵盖多个行业领域。目前，该案已移送检察机关审查起诉。（来源：公安部网安局）

10. 公安网安部门依法对某人工智能服务科技有限公司予以行政处罚

9 月 17 日消息，国家网络与信息安全信息通报中心近日通报，公安网安部门在“护网—2025”专项工作中发现，某主营业务为对外提供人工智能模型训练基础数据（算料）的科技有限公司，在处理人脸等生物识别类敏感个人信息前，未按《个人信息保护法》有关规定进行个人信息保护影响评估。属地公安机关依据《个人信息保护法》规定，对该公司依法予以行政处罚，并责令整改。（来源：公安部网安局）

11. 湖北省公安部门侦破一起通过“AI 换脸”非法侵入计算机信息系统案

9 月 20 日消息，湖北武汉网警近日侦破一起利用“AI 换脸”技术非法侵入计算机信息系统的案件，抓获阿成（化名）等 4 名犯罪嫌疑人。

6 月 10 日，某机构工作人员发现运营的公众号密码以及公司法人代表信息被篡改。武汉网警通过技术分析研判查证属实，并锁定犯罪嫌疑人阿成。7 月 17 日，民警赴潍坊实施抓捕，对其住所搜查时，办案民警发现大量 AI 换脸视频素材，同时发现其账户内价值 40 余万元来自 AI 换脸“接单”的非法获利。经查，阿成负责完成 AI 换脸验证操作，而阿明（化名）、阿斌（化名）、阿华（化名）等 3 名上线则负责承接“人脸代过”需求、转交人员信息，并从中牟利。

目前，4 人均被依法采取刑事强制措施，案件正进一步侦办中。（来源：公安部网安局）

12. 浙江省公安部门侦破一起非法获取计算机信息系统数据案

9 月 22 日消息，浙江绍兴诸暨公安机关近日侦破一起非法获取计算机信息系统数据案。

2022 年，兰某某在某电商平台开设了四家店铺，以“专业解锁”“不成功不收费”等噱头招揽生意。接到订单后，兰某某在明知客户非手机机主的情况下，仍将搜集到的信息提供给其上家，由上家通过非法手段进行手机解锁，解锁成功后，兰某某根据手机新旧程度向客户收取 500 至 900 元不等的费用，再从中抽取 100 至 200 元作为自己的“中介费”。

兰某某通过充当非法解锁链条的“掮客”，截止被公安机关抓获时已非法牟利超 10 万余元。案件正在进一步侦办中。（来源：公安部网安局）

13. 重庆市公安部门打击“跑马机”黑灰产工作取得成效

9 月 26 日消息，重庆公安部门近日在工作中发现，一些驾校学员无需实际练车即可刷满学时。经查，犯罪嫌疑人使用“跑马机”并结合 AI 技术实施作弊。犯罪嫌疑人利用汽车脉冲信号原理制作的设备，通过侵入并篡改驾培计时系统，并运用 AI 技术模拟学员动态人像，达成伪造培训记录目的。目前，重庆警方已打掉涉案违法犯罪团伙 2 个，抓获犯罪嫌疑人 70 名，查扣“跑马机”设备 384 台，查处涉案驾校 34 家。（来源：公安部网安局）

14. 内蒙古自治区公安厅通报2025年“净网”“护网”等专项行动成果

9月27日，内蒙古自治区公安厅通报2025年以来“净网”“护网”等专项行动成果。

2025年以来，全区公安机关共发现网络谣言线索2029条，查处网络谣言案事件1400余起，关停违法违规账号17个。其中，侦办刑事案件8起，办理行政案件160起，对8人采取了刑事强制措施，对161人进行了行政处罚，对违法情节较轻微的1300余人进行了批评教育。全区三级公安机关累计开展网络安全监督检查3653家（次），办理行政案件421起，下达责令限期整改通知书1158份，公安风险提示函2118份，保障了全区网络和数据安全。（来源：公安部网安局）

15. 山东公安部门侦破一起非法“刷机”案

9月30日消息，在“净网—2025”专项行动中，山东威海网安部门近日成功侦破一起提供非法侵入、控制计算机信息系统工具的案件，抓获犯罪嫌疑人连某某，查获9套“刷机”工具及139部已被非法“刷机”的手机设备。

涉案人员非法获得具有绕过手机官方系统限制、破解安全防护功能的非法“刷机”程序，以此为工具，大肆开展非法“刷机”业务，为大量非法来源的手机提供系统重装、破解激活锁等服务，并为下游的盗窃、诈骗等犯罪活动提供技术支持。

该案中，犯罪嫌疑人线上招揽“客户”，通过邮寄手机或使用远程桌面控制软件，实现“非接触式”为非法来源的手机进行“刷机”。此外，犯罪嫌疑人还将购得的非法“刷机”程序通过网络以租借或售卖的方式提供给他人使用，以此牟取非法利益。（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·整治恶意挑动负面情绪问题”专项行动

9月22日消息，中央网信办近日部署开展为期2个月的“清朗·整治恶意挑动负面情绪问题”专项行动。本次专项行动聚焦社交、短视频、直播等平台，全面排查话题、榜单、推荐、弹幕、评论等重点环节，着力整治四个方面问题，分别是：

一是挑动群体极端对立情绪。借社会热点事件强行关联身份、地域、性别等信息标签化、污名化炒作，挑动群体间矛盾。借影视作品、脱口秀、体育赛事等话题，鼓动“饭圈”粉丝群体恶意拉踩、攻击、谩骂或者组织批量举报投诉等行为。部分二次元群体、“喷系少年”组织煽动对立甚至“开盒”，或者教授买卖“开盒”技巧等。

二是宣扬恐慌焦虑情绪。恶意虚构散布灾情、险情、警情等可能影响公共安全的突发事件，伪造发布政府部门公告。以“内幕消息”等方式，拼凑剪辑或者利用矩阵账号炮制传播经济金融、社会民生、公共政策等谣言信息。虚构歪曲事件原因、细节、进展等，发布“阴谋论”等耸人听闻

的信息。编造“大师”“专家”等虚假身份、人设，围绕就业、婚恋、教育等领域“贩卖”焦虑带货卖课。

三是挑起网络暴力戾气。策划、演绎打架斗殴、恶意刁难等剧本，宣扬“以暴制暴”。传播未经处理直接展示的血腥恐怖现场画面，或发布含有虐待动物、自残自伤等极端行为的刺激图片视频。利用 AI 合成、视频剪辑、图片拼凑等手段，渲染美化暴力行为，制造猎奇惊悚氛围。直播中以自残自虐、“打人挑战”、持械恐吓等噱头吸粉引流，组织线上约架，并实时直播双方线下侮辱谩骂、打架斗殴等场景。

四是过度渲染消极悲观情绪。集中发布、片面鼓吹“努力无用论”“读书无用论”等绝对化、消极化论调。恶意解读社会现象，片面放大负面个案，借机宣扬厌世等负面人生观。通过炮制所谓热搜词、热门梗、表情包、语录段子等，过度自我矮化或者渲染颓丧消极负面情绪，引起跟风效仿。（来源：网信中国）

2. 国家网信办发布整治违规开展互联网新闻信息服务典型案例

9 月 10 日，国家网信办发布整治违规开展互联网新闻信息服务典型案例。

案例一：假冒仿冒新闻单位。新浪微博账号“黑龙江新闻观察网”“互联网新闻网”、微信视频号“直播忻州”、百度百家号“上游皖观察”、今日头条号“时代之声”等 1200 余个账号，在名称、头像、简介等账号信息中使用与新闻单位相同或相似内容，违规发布新闻信息。相关账号已被依法依约关闭或禁言。

案例二：违规开展新闻采编。某文化传媒有限公司未取得互联网新闻信息服务许可，在微信、微博等平台注册“瞭新社”矩阵账号，以“通讯员”“记者”名义进行新闻采访报道，违规开展互联网新闻信息采编发布服务。相关账号已被依法依约关闭。

案例三：冒用新闻栏目照片。微信公众号“天津百晓圈子”“天津老刘”等20余个账号长期发布有关社会突发事件的“标题党”文章，在文中冒用央视“新闻联播”“新闻直播间”等栏目主持人照片，混淆公众视听，扰乱网上传播秩序。相关账号已被依法依约关闭。

案例四：发布虚假不实信息。“金融界”“中访网”“全球财说”等46个公众账号，使用“标题党”、夸张词汇发布涉企虚假不实新闻，集纳企业负面信息，恶意诋毁抹黑企业，干扰企业正常生产经营。相关账号已被依法依约禁言。（来源：网信中国）

3. 国家网信办通报“清朗·优化营商网络环境—整治涉企网络‘黑嘴’”专项行动第二批典型案例

9月11日，国家网信办通报“清朗·优化营商网络环境—整治涉企网络‘黑嘴’”专项行动第二批典型案例。

案例一：“通信圈”等账号胁迫企业进行“商业合作”，谋取非法利益。微信公众号“通信圈”，抖音、微博、微信等平台账号“券业行家”“煤文化”等，长期集纳发布涉企负面信息，以“茶水费”“商业合作”等名义，向企业索取高额费用，并在合作到期前持续发布虚假不实信息威

胁企业续签合同。涉及的账号已被依法依约关闭，账号主体被纳入平台黑名单管理。

案例二：“国际投行研究报告”等账号歪曲解读涉企公开信息，诋毁企业形象声誉。微信公众号“国际投行研究报告”“IPO超级情报局”、百度百家号“博望财经”等，为博取流量，长期恶意集纳炒作上市公司、拟上市公司负面信息，发布“业绩真实性存疑”“营业收入骤然下滑”等虚假不实信息，歪曲解读企业财务报表，恶意唱衰企业经营状况。涉及的账号已被依法依约采取禁言处置。

案例三：“固收嘚啵李”等账号捏造不实信息，恶意诋毁金融机构声誉。微信公众号“固收嘚啵李”“钞票不睡觉”、今日头条、百度、微博等平台账号“首席商业智慧”“九号财经”等，以“标题党”“小作文”等形式长期发布炒作银行、信托等金融机构“业绩爆雷”“产品兑付大规模逾期”等虚假不实信息，干扰企业正常经营，影响金融市场稳定。涉及的账号已被依法依约采取关闭或禁言处置。

案例四：“大嘴博士”等账号发布炒作测评信息，影响市场竞争秩序。抖音、小红书、微博、哔哩哔哩等平台账号“大嘴博士”运营主体与某美妆产品企业存在商业利益关系。上述账号多次针对同领域竞争对手产品发布炒作没有法律效力的测评信息，误导消费者，干扰正常市场秩序。涉及的账号已被依法依约采取禁言措施。（来源：网信中国）

4. 国家网信办发布网络安全、数据安全、个人信息保护相关执法典型案例

9 月 16 日，国家网信办发布网络安全、数据安全、个人信息保护相关执法典型案例。

案例一：广东某科技股份有限公司网页篡改案

网信部门工作发现，该企业用于业务审批等的办公协作平台登录页面被篡改为违法有害内容。经查，该企业涉事系统存在任意文件上传漏洞，遭受勒索软件攻击，该企业当天发现后仅重装系统，未修复系统漏洞。其后，攻击者利用该漏洞上传远程控制木马，将登录页面篡改为违法有害内容。该企业未依法履行网络安全保护义务，未采取必要技术措施保障网络安全，未及时修复系统漏洞，造成网页篡改后果，违反《网络安全法》相关规定。属地网信办已依法责令其改正，并予以警告、罚款处罚。

案例二：新疆某互联网科技有限公司网页篡改案

网信部门工作发现，该企业门户网站及开发运维的 8 个网站子页面被篡改为涉赌违法信息。经查，该企业上述网站存在安全缺陷和漏洞，相关网页源代码 php 文件被恶意篡改，出现涉赌违法信息。事件发生时，网站管理员休假不在岗，网站处于无人管理状态。该企业作为网络产品、服务提供者，未及时发现其开发的网站存在安全缺陷和漏洞，未立即采取补救措施，未按照规定及时告知用户并向主管部门报告，违反《网络安全法》相关规定，属地网信办已依法责令其改正，并予以警告处罚。

案例三：山东某医学检验有限公司数据泄露案

网信部门工作发现，该企业某系统相关数据被搜索引擎爬虫爬取。经查，涉事系统开启目录浏览功能，存在目录遍历和未授权访问漏洞，未正确配置防火墙入侵防护策略，未按照规定留存相关网络日志。相关搜索引擎爬虫通过遍历请求爬取了网站组织架构和文件，导致系统相关数据泄露。该企业未依法履行网络安全、数据安全保护义务，涉事系统未依法留存相关网络日志，未采取技术措施和其他必要措施保障数据安全，造成数据泄露后果，违反《网络安全法》《数据安全法》《网络数据安全管理条例》等法律法规规定。属地网信办已依法责令其改正，并予以警告、罚款处罚。

案例四：浙江某科技股份有限公司数据被窃取案

网信部门工作发现，该企业 FTP 系统相关数据被窃取。经查，该企业为方便共享、打印系统文件，将涉事系统设置为允许匿名访问，并设置云服务器安全组规则不生效，长期存在未授权访问漏洞，导致涉事系统相关数据被窃取。该企业未依法履行网络安全、数据安全保护义务，涉事系统未采取技术措施和其他必要措施保障数据安全，造成数据被窃取后果，违反《网络安全法》《数据安全法》《网络数据安全管理条例》等法律法规规定。属地网信办已依法责令其改正，并予以警告、罚款处罚。

案例五：重庆某科技公司数据被窃取案

网信部门工作发现，该企业用于汽车租赁服务的“OA 信息系统”相关数据被窃取。经查，该企业涉事系统 3306 端口开放 MySQL 数据库服务，未设置用户密码，存在弱口令漏洞，导致涉事系统相关数据被先后窃取 159 次。该企业未依法履行网络安全、数据安全保护义务，涉事系统未采取技术措施和其他必要措施保障数据安全，造成数据被窃取后果，违反《网络

安全法》《数据安全法》《网络数据安全管理条例》等法律法规规定。属地网信办已依法责令其改正，并予以警告、罚款处罚。

案例六：广东某保险代理有限公司数据被窃取案

网信部门工作发现，该企业提供保险代理服务的后台系统相关数据被窃取。经查，该企业涉事系统存在越权遍历访问漏洞，攻击者可通过遍历URL ID 的方式批量获取数据，且该企业购买的云防火墙服务已过期，未按照规定留存相关网络日志，导致涉事系统相关数据被窃取。该企业未依法履行网络安全、数据安全保护义务，涉事系统未依法留存相关网络日志，未采取技术措施和其他必要措施保障数据安全，造成数据被窃取后果，违反《网络安全法》《数据安全法》《网络数据安全管理条例》等法律法规规定。属地网信办已依法责令其改正，并予以警告、罚款处罚。

案例七：湖南某科技股份有限公司数据存在泄露安全风险案

网信部门工作发现，该企业内网数据库相关数据存在泄露安全风险。经查，该企业内网数据库存在未授权访问漏洞和弱口令漏洞，某软件研发工程师为工作便利，将合作项目中掌握的大量用户数据拷贝至企业内网数据库，并打开企业内网的公共互联网访问端口，导致内网数据库相关数据暴露在互联网上。该企业未依法履行网络安全、数据安全保护义务，未建立网络安全和数据安全管理制度，涉事系统未采取技术措施和其他必要措施保障数据安全，存在数据泄露安全风险，违反《网络安全法》《数据安全法》《网络数据安全管理条例》等法律法规规定。属地网信办已依法责令其改正，并予以警告、罚款处罚。

案例八：北京某科技有限公司运营的 App 超范围收集个人信息案

网信部门工作发现，该企业运营的App违反必要原则，收集与其提供的服务无关的个人信息。经查，该企业开发的App在用户未使用任何功能情况下，后台运行时收集上传用户应用程序安装、卸载信息。用户使用上传AI头像等功能时，调用非必要存储权限。相关行为超出了实现个人信息处理目的最小必要范围，违反《网络安全法》《个人信息保护法》《网络数据安全管理条例》等法律法规。属地网信办已依法责令其改正，并予以警告、罚款处罚。

案例九：上海某科技有限公司违法违规收集人脸信息案

网信部门工作发现，该企业运营的自动售货机存在违法违规收集人脸信息等问题。经查，该企业运营的自动售货机在用户支付环节存在未经同意收集人脸信息等问题，同时该企业存在未建立个人信息保护影响评估制度、相关系统存在SQL注入高危漏洞等问题，违反《网络安全法》《个人信息保护法》《网络数据安全管理条例》等法律法规规定。属地网信办已依法责令其改正，并予以警告处罚。

案例十：浙江某科技有限责任公司运营的App提供深度合成服务未按规定进行安全评估案

网信部门工作发现，该企业运营的App提供AI换脸服务未按规定进行安全评估。经查，该企业运营的App是一款深度合成类服务产品，提供视频换脸、图片换脸、照片舞动配音等图片处理功能，用户可对上传图片、视频中的人物进行换脸，但未按规定落实安全评估要求，相关深度合成内容也未作显著标识，存在较大安全风险，违反《互联网信息服务深度合成管理规定》《生成式人工智能服务管理暂行办法》《互联网信息服务算法

推荐管理规定》《具有舆论属性或社会动员能力的互联网信息服务安全评估规定》等规定。网信部门已依法责令移动应用程序分发平台依规依约对该 App 予以下架处置。（来源：网信中国）

5. 网信部门依法查处快手、UC、今日头条等平台

9 月，国家网信办先后公布一批网信部门针对快手、微博、UC、今日头条、小红书破坏网络生态的行为依法作出的行政处罚案件。

一是小红书平台破坏网络生态案件。小红书平台未落实信息内容管理主体责任，在热搜榜单重点环节频繁呈现多条炒作明星个人动态和琐事类词条等不良信息内容，破坏网络生态问题，国家网信办指导上海市网信办，依据《网络信息内容生态治理规定》等有关规定，对小红书平台采取约谈、责令限期改正、警告、从严处理责任人等处置处罚措施。

二是快手平台破坏网络生态案件。快手平台未落实信息内容管理主体责任，在热搜榜单主榜扎堆呈现炒作明星个人动态和琐事类词条等不良信息内容，存在泛娱乐化倾向问题，国家网信办指导北京市网信办，依据《网络信息内容生态治理规定》等有关规定，对快手平台采取约谈、责令限期改正、警告、从严处理责任人等处置处罚措施。

三是微博平台破坏网络生态案件。微博平台未落实信息内容管理主体责任，在热搜榜单主榜高位呈现大量炒作明星个人动态和琐事类词条等不良信息内容，破坏网络生态的问题，国家网信办指导北京市网信办，依据《网络信息内容生态治理规定》等有关规定，对微博平台采取约谈、责令限期改正、警告、从严处理责任人等处置处罚措施。

四是UC平台破坏网络生态案件。UC平台未落实信息内容管理主体责任，在热搜榜单主榜扎堆呈现极端敏感恶性案事件词条等非权威部门、权威媒体发布的信息，涉及网络暴力、未成年人隐私等相关话题，破坏网络生态秩序的问题，国家网信办指导广东省网信办，依据《网络信息内容生态治理规定》等有关规定，对UC平台采取约谈、责令限期改正、警告、从严处理责任人等处置处罚措施。

五是今日头条平台破坏网络生态案件。今日头条平台未落实信息内容管理主体责任，不仅在热搜榜单主榜呈现不良信息内容，还在落地页面置顶呈现相关话题，破坏网络生态的问题，国家网信办指导北京市网信办，依据《网络信息内容生态治理规定》等有关规定，对今日头条平台采取约谈、责令限期改正、警告、从严处理责任人等处置处罚措施。（来源：网信中国）

6. 海南省互联网信息办公室通报28款移动应用程序违法违规收集使用个人信息情况

9月11日，海南省互联网信息办公室发布通报，指出针对群众反映强烈的移动应用程序（包含App、小程序等）非法获取、超范围收集、过度索取权限等侵害公民个人信息的违法违规现象，海南省互联网信息办公室近期组织对省内用户量大的移动应用程序收集使用个人信息情况进行了技术检测，检测结果显示28款移动应用程序均存在不同程度违法违规收集使用个人信息的行为。

所涉问题包括未提供有效的更正、删除个人信息及注销用户账号功能；在申请打开可收集个人信息的权限，或申请收集用户身份证号、银行账号、行踪轨迹等个人敏感信息时，未同步告知用户其目的，或者目的不明确、难以理解等。

通报要求上述移动应用程序运营主体强化守法意识、压实主体责任、按时落实整改。（来源：网信海南）

7. 湖南怀化网信部门查处一企业及九所学校违法收集使用人脸等个人信息案件

9 月 29 日消息，根据湖南省网信办、省教育厅等部门开展的 2025 年度“亮剑湖湘·民生领域个人信息权益保护”专项执法行动工作部署，湖南怀化市网信部门近日对一家企业及九所学校违法收集使用人脸等个人信息的行为进行立案查处。

经查，某云科技有限公司在推广使用其“智慧校园系统”时，未经学生或家长单独同意收集学生姓名、人脸图像等个人信息，且未对相关个人信息进行加密存储，相关系统存在未授权访问漏洞。怀化市网信办依据《个人信息保护法》对其作出行政警告处罚，并责令整改。

“**第一中学”等 9 所学校在使用该“智慧校园系统”时，将学生姓名、人脸图像等数据，教师姓名、联系方式、头像等数据，以及家长联系方式等数据在未经过本人及监护人同意的情况下，违规提供给该云科技有限公司。属地县级网信部门依据《个人信息保护法》，对上述 9 所学校处以警告的行政处罚，并要求立即撤回相关个人信息。（来源：网信湖南）

（三）通信管理部门治理实践

1. 工信部等六部门联合部署开展汽车行业网络乱象专项整治行动

9 月 10 日消息，工业和信息化部、中央社会工作部、中央网信办、国家发展改革委、公安部、市场监管总局等六部门近日联合印发《关于开展汽车行业网络乱象专项整治行动的通知》，决定在全国范围内开展为期 3 个月的汽车行业网络乱象专项整治行动。专项整治行动将集中整治非法牟利、夸大和虚假宣传、恶意诋毁攻击等网络乱象。

《通知》要求，各地工业和信息化、社会工作、网信、发展改革、公安、市场监管等部门要加强组织领导和协调联动。网络平台企业要深入开展自查自纠，加强对采用生成式人工智能技术等的网络水军、“黑嘴”的甄别管控，健全平台涉企侵权信息投诉举报、争议标签、一键关联辟谣内容等产品功能，防止虚假信息误导公众。行业协会要引导行业加强自律建设。汽车企业要深入开展自查，自觉抵制网络水军、“黑公关”“黑嘴”及“饭圈”粉丝等网络乱象。要形成合力，持续净化汽车行业网络舆论环境。（来源：工信部）

2. 工信部以及山东、浙江等地通信管理局发布侵害用户权益 APP 名单

（1）工信部

9 月 18 日消息，工信部近日组织第三方检测机构进行抽查，共发现 29 款 APP 存在侵害用户权益行为。29 款 APP 所涉问题主要包括违规收集个

人信息，APP 强制、频繁、过度索取权限，APP 频繁自启动和关联启动，强制用户使用定向推送功能等。上述 APP 应按有关规定进行整改，整改落实不到位的，工信部将依法依规组织开展相关处置工作。

（2）山东省

9 月 8 日，山东省通信管理局发布 2025 年第 5 批不合格 APP 整改情况通报。

一是逾期未完成整改的 14 款 APP，予以通报。截至 9 月 8 日，有 14 款存在问题并被山东省通信管理局通知限期整改的 APP 未按要求在限期内完成整改反馈。9 月 15 日前，上述 14 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等措施。

二是通报后仍未完成整改的 2 款 APP，予以下架。截至 9 月 8 日，有 2 款存在问题的 APP 经书面要求整改、通报再次要求整改后，仍未在规定时限内完成整改反馈，现予以下架。相关应用商店应立即对有关 APP 进行下架处理，并举一反三，排查反复出现问题的 APP 开发运营者，严格落实分发平台主体责任，把好上架审核关。山东省通信管理局将对下架情况进行持续跟踪。

（3）上海市

9 月 16 日消息，上海市通信管理局近日向社会公示了一批存在侵害用户权益行为的应用。在规定的整改期限内，经核查复检，尚有 42 款 APP（SDK）未按照要求落实整改，现对上述 APP（SDK）采取下架处理。上海市通信

管理局将对上述应用持续跟踪，视情况进一步采取停止接入、行政处罚、纳入电信业务经营不良名单等后续处理措施。

（4）江苏省

9 月 17 日消息，江苏省通信管理局近日组织第三方检测机构对省内金融理财、实用工具等类型的 APP、小程序进行检查，并通报相关单位限期整改。截至通报，尚有 7 款 APP 未完成整改。请相关单位于 9 月 29 日前完成整改并反馈，整改落实不到位的，江苏省通信管理局将依法依规组织开展相关处置工作。

（5）广东省

9 月 26 日，广东省通信管理局通报 14 款未按要求完成整改 APP 名单，以及下架的 2 款 APP 名单。

通报指出，广东省通信管理局持续开展移动应用程序专项治理工作，发出《APP 整改通知书》责令 APP 运营者限期整改，并通知相关应用商店协助督促 APP 运营者整改。截至通报，尚有 14 款 APP 未完成整改。被通报的 APP 主办者应在 2025 年 9 月 29 日前完成整改及反馈工作。逾期不整改的，广东省通信管理局将依法依规采取下一步处置措施。

通报指出，广东省通信管理局持续开展移动应用程序专项治理工作。截至通报规定时限，经核查复检，尚有 2 款 APP 未按照要求完成整改反馈。为严肃处理上述 APP 的违规行为，广东省通信管理局决定对该 APP 予以下架/禁搜。相关应用商店应立即组织对该 APP 进行下架/禁搜处理，并举一反三，排查反复出现问题的 APP 开发运营者，严格落实分发平台主体责任，

把好上架审核关。广东省通信管理局将对通报 APP 持续跟踪，视情况进一步采取断开网络、行政处罚、纳入电信业务经营不良名单等后续处理措施。

（6）浙江省

9 月 26 日消息，浙江省通信管理局发布通报，指出前期公开通报存在侵害用户权益行为的 App，要求限期整改。经核查复检，尚有 9 款 APP 未按要求完成整改，现对上述 APP 采取下架处理。浙江省通信管理局将对上述 APP 持续跟踪，视企业整改情况进一步采取断开网络、行政处罚、纳入电信业务经营不良名单等后续处理措施。（来源：工信部、山东省通信管理局、上海通信圈、浙江省通信管理局等）

境内观察三：人工智能安全专题

导读：9 月，人工智能政策立法主要关注人工智能安全治理、“人工智能+”和数据知识产权登记方面。

《人工智能安全治理框架》2.0 版正式发布，涉及人工智能安全风险分类、技术应对措施、综合治理措施等内容。《框架》2.0 版在 2024 年《框架》基础上，结合人工智能技术发展和应用实践，持续跟踪风险变化，完善优化风险分类，研究探索风险分级，动态调整更新防范治理措施。《国家发展改革委 国家能源局关于推进“人工智能+”能源高质量发展的实施意见》发布，从加快能源应用场景赋能、加大关键技术供给两方面提出要求，并从强化组织实施、推动协同创新、加强标准规范建设等方面加强保障措施。

浙江省知识产权局印发《浙江省人工智能领域数据知识产权登记申请指引（2025）》，明确人工智能领域数据知识产权登记对象、登记前存证公证、登记申请、集合申请、登记审查等要求。

关键词：人工智能安全治理；人工智能+；数据知识产权登记

1. 《国家发展改革委 国家能源局关于推进“人工智能+”能源高质量发展的实施意见》印发，要求加大关键技术供给

9月4日，国家发展改革委、国家能源局印发《国家发展改革委 国家能源局关于推进“人工智能+”能源高质量发展的实施意见》。《意见》从加快能源应用场景赋能、加大关键技术供给两方面提出要求，并从强化组织实施、推动协同创新、加强标准规范建设等方面加强保障措施。

其中，加大关键技术供给方面，《意见》提出，聚焦能源领域数据孤岛化、算力碎片化、算法黑盒化、算力高耗能等技术瓶颈，推动开展适用能源领域的数据、算力、算法等共性关键技术攻关。具体包括夯实数据基础、强化算力支撑、提升模型基础能力。夯实数据基础方面，《意见》要求针对能源领域高质量数据集构建和数据安全需求，推动数据智能标注、智能增强、数据合成等技术应用，推进能源数据分类分级技术、隐私计算技术以及智能数据动态加密和跨域可信溯源等技术研发，优化数据分享机制，加快形成能源领域高质量数据集，确保能源数据全流程安全可靠。（来源：中国政府网）

2. 《人工智能安全治理框架》2.0版正式发布

9月15日，《人工智能安全治理框架》2.0版正式发布。《框架》2.0版是在国家网信办指导下，由国家互联网应急中心牵头组织人工智能专业机构、科研院所、行业企业联合制定。作为全国网安标委技术文件，《框架》2.0版在2024年《框架》基础上，结合人工智能技术发展和应用实践，持续跟踪风险变化，完善优化风险分类，研究探索风险分级，动态调整更

新防范治理措施。《框架》2.0 版包括人工智能安全风险分类、技术应对措施、综合治理措施等内容。

人工智能安全风险分类方面，《框架》2.0 版指出，人工智能既存在模型算法缺陷、数据语料质量问题等技术内生安全风险，也存在技术整合交付应用时的网络系统、信息内容等方面应用安全风险，还面临技术误用、滥用、恶用冲击现实社会环境、人类认知伦理的衍生安全风险。

技术应对措施方面，《框架》2.0 版指出，针对上述风险，模型算法研发者、服务提供者、系统使用者等需从训练数据、模型算法、算力设施、产品服务、应用场景各方面采取技术措施予以防范。

综合治理措施方面，《框架》2.0 版提出，在采取技术应对措施的同时，建立完善技术研发机构、服务提供者、用户、政府部门、社会组织等多方参与的人工智能安全风险综合治理制度规范。（来源：国家互联网信息办公室）

3. 浙江省知识产权局印发《浙江省人工智能领域数据知识产权登记申请指引（2025）》

9 月 14 日，浙江省知识产权局印发《浙江省人工智能领域数据知识产权登记申请指引（2025）》。

《指引》所指人工智能领域数据知识产权登记对象包括：（1）基于人工智能大模型，通过预训练等方式形成适配专项能力或特定任务解决能力要求，所形成的算法、参数、模型等数据处理规则和数据集合，符合数据知识产权登记要件的；（2）基于人工智能相关技术，通过智能体、脑机接

口、具身智能、生物启发等应用创新技术，所形成的算法、参数、模型等数据处理规则和数据集合，符合数据知识产权登记要件的。

《指引》明确登记前存证公证、登记申请、集合申请、登记审查等要求。（来源：浙江省知识产权局）

境外前沿观察：月度速览十则

导读：9 月，境外国家和地区持续推动网络安全领域政策法律，重点关注人工智能、数据安全等方面。

人工智能方面，美国与英国签署《美国与英国政府关于技术繁荣协定的谅解备忘录》，双方拟在共同建设人工智能基础设施，促进研究界获取算力资源，支持创建新型科学数据集，并利用双方在计量与评估领域的优势推动技术应用与安全提升等方面深化合作。意大利议会通过《关于人工智能领域的政府授权及相关规定》法案，使其成为首个拥有与欧盟《人工智能法》接轨的人工智能全面监管法规的欧盟国家。欧盟委员会为落实《人工智能法》第 73 条的规定，发布《人工智能严重事件报告指南》草案，明确高风险人工智能系统在发生严重事件时的报告义务和流程。

数据安全方面，欧盟《数据法》开始施行，主要内容包括：赋予用户在各云数据处理服务提供者之间切换的能力；构建公共机构访问和使用私营部门所持数据的机制；制定使联网设备用户能够访问联网设备和相关服务所产生的数据的措施等。

此外，美国总统特朗普签署一项行政命令，使 TikTok 免于被禁。特朗普总统认定，在一份拟定的框架协议中概述的业务剥离，即由一家新的、设在美国境内的合资公司运营 TikTok 在美国的应用程序，是一种“合格的业务剥离”。

关键词：人工智能；数据安全；TikTok

1. 英国 DSIT 发布《可信第三方人工智能保障路线图》

9 月 3 日，英国科学、创新与技术部（DSIT）发布《可信第三方人工智能保障路线图》，旨在培育可信的第三方人工智能保障市场，确保人工智能技术的安全开发与部署。

路线图指出构建可信第三方人工智能保障市场需突破四大关键障碍：一是保障质量存疑：尽管技术标准为质量保障奠定基础，但人工智能系统及其保障机制仍处于发展阶段，相关标准尚不明确。现有人工智能认证体系未获英国认可服务局（UKAS）授权；二是人才短缺：保障服务商普遍反映难以招募合格人才，亟需人工智能/机器学习、法律伦理、数据治理及技术标准等复合型技能；三是信息获取受限：企业因商业机密、安全顾虑或对审计需求认知不足，往往拒绝向保障机构开放训练数据、模型细节及治理文档等核心信息；四是创新动力不足：缺乏协作研究平台，持续保障技术与工具研发滞后于人工智能技术演进速度。

针对上述挑战，路线图提出系列举措：一是建设专业体系：组建多方参与的英国联盟，制定自愿性道德准则，建立人工智能保障人员能力框架及认证体系；二是人才培育计划：完善学术与职业培训路径，评估现有课程设置，明确人工智能保障岗位的知识技能要求，通过职业前景宣传提升行业多样性；三是信息共享机制：制定最佳实践指南，规范人工智能开发初期的数据披露标准；四是创新激励措施：设立 1100 万英镑人工智能保障创新基金，支持新型保障工具与方法的研发试点，构建持续创新的治理技术管道等。（来源：英国政府）

2. 欧洲数据保护监督局发布《关于签署及缔结〈联合国打击网络犯罪公约〉两项理事会决定提案的意见》

9 月 4 日，欧洲数据保护监督局（EDPS）发布《关于签署及缔结〈联合国打击网络犯罪公约〉两项理事会决定提案的意见》。

EDPS 强调联合国成员国数量庞大，其法律体系在基本权利与自由（包括隐私权与数据保护权）的保障方面存在显著差异。在此背景下，EDPS 认为至关重要的是确保公约框架下与第三国的合作不会削弱或损害欧盟法律对自然人基本权利与自由的保护水平，特别是数据保护权与隐私权。

EDPS 注意到公约明确规定：若个人数据传输行为不符合缔约国关于数据保护的现行法律要求，则无需履行该义务。因此，成员国在实施和适用公约时，应在每个具体案例中将个人数据转移至第三国前，严格评估是否符合欧盟《执法数据保护指令》第五章规定的条件。成员国主管部门还须审慎考量向公约缔约第三国传输个人数据的行为是否完全符合其在国际人权法下的义务，以及是否充分尊重相关个人的基本权利与自由。

EDPS 还表示，成员国主管部门在适当时机应援引拒绝合作条款。例如：针对本国法律体系中未认定的犯罪行为，或依据欧盟法院相关判例，当类似案件在本国司法管辖范围内不允许执行相关调查措施时，应拒绝合作请求。若决定开展合作，则应选择数据保护措施最完善的国际协作机制等。（来源：欧盟数据保护监督局）

3. 美国总统特朗普签署《执行〈美日协定〉》行政令

9 月 4 日，美国总统特朗普签署第 14345 号《执行〈美日协定〉》行政令，正式落实今年 7 月 22 日与日本达成的美日贸易框架协议的相关措施。根据协议内容，日本政府承诺向美国投资 5500 亿美元，由美国政府选择项目方向。这些投资将集中于半导体、人工智能和量子计算等领域。

行政令要求美国商务部长会同贸易代表、国土安全部部长和国际贸易委员会主席监督日本履约进展，并在必要时调整关税安排或修改相关法规。如日本未能履行承诺，总统可以重新调整行政措施，以应对贸易失衡和国家安全威胁。行政令同时授权商务部和国土安全部采取一切必要行动，包括发布公告、修改法规、发布实施指南等，以确保行政令顺利执行。

特朗普强调，这项行政令标志着美日经济关系进入“以互惠原则和共同的国家利益为基础的新时代”。协定不仅将推动美国出口和制造业发展，还将强化供应链韧性和产业竞争力。（来源：美国白宫）

4. 欧盟《数据法》开始施行

9 月 12 日，欧盟《数据法》开始施行。该法是一项综合举措，旨在应对欧盟数据带来的挑战，强调公平访问和用户权利，同时确保对个人数据的保护。

该法主要内容包括：（1）赋予用户在各云数据处理服务提供者之间切换的能力；（2）构建公共机构访问和使用私营部门所持数据的机制；（3）制定使联网设备用户能够访问联网设备和相关服务所产生的数据的措施；

（4）制定防止非法数据传输的保障措施；（5）为各部门之间重复使用数据制定互操作性标准。（来源：欧盟委员会）

5. 意大利议会通过《关于人工智能领域的政府授权及相关规定》法案

9 月 17 日，意大利议会通过《关于人工智能领域的政府授权及相关规定法案》，使其成为首个拥有与欧盟《人工智能法》接轨的人工智能全面监管法规的欧盟国家。该法案确立以人为本、透明和安全的人工智能使用核心原则，同时注重创新、网络安全和隐私保护。法案制定覆盖医疗健康、劳动就业、公共行政、司法审判、教育体育等领域的跨行业规则，要求对人工智能决策进行溯源追踪和人工监督。

法案主要内容包括：（1）14 岁以下未成年人使用人工智能需获得父母同意；（2）针对非法传播人工智能生成内容（如深度伪造内容）的行为，若造成危害将被处以 1 至 5 年监禁。非法使用人工智能还将加重身份盗窃和诈骗等犯罪的量刑；（3）在版权领域，经人工智能介入创作的作品若体现智力劳动成果将受到保护。

法案授权从政府支持的风险投资基金中拨付最多 10 亿欧元，用于对人工智能、网络安全、量子技术和电信领域的中小企业和大型企业进行股权投资。（来源：路透社）

6. 美国与英国签署《美国与英国政府关于技术繁荣协定的谅解备忘录》

9 月 18 日，美国与英国签署《美国与英国政府关于技术繁荣协定的谅解备忘录》，旨在推动双方在战略科技领域的合作，共同把握人工智能、量子技术等前沿领域的重大发展机遇。合作内容主要包括：

一是加速人工智能创新。人工智能作为时代的标志性技术，为改善人类生活提供无限可能。双方拟在以下方面深化合作：共同建设人工智能基础设施，促进研究界获取算力资源，支持新型科学数据集创建，并利用双方在计量与评估领域的优势推动技术应用与安全提升。在此基础上，双方希望联合科研与产业力量，将人工智能塑造为引领经济社会变革的驱动力。

二是确保量子优势。双方计划构建变革国防、金融与医疗的量子计算机器，保护公民安全并创造高技能岗位。重点合作领域包括：（1）设立美英量子基准测试工作组，加速量子硬件、软件及算法全链条评测突破；（2）启动跨大西洋量子代码挑战赛，动员科研人员研发并部署解决实际痛点的革命性量子算法；（3）通过协调研发合作，利用人工智能与高性能计算加速量子算法开发及系统成熟度；（4）通过多边与双边互补的预标准化活动，推进量子计算、传感及网络的可信互操作标准等。

该备忘录将在《美英经济繁荣协定》正式签署与实施后同步生效。根据安排，备忘录生效六个月内将成立部长级工作组，作为战略论坛指导合作、设定优先事项并监督执行；生效十二个月后（此后每年）举行正式评

估会议，以技术机遇、政策发展和战略利益为依据，动态调整合作方向。（来源：美国白宫）

7. 美国总统特朗普发布《在保护国家安全的同时拯救 TikTok》行政令

9 月 25 日，美国总统特朗普发布《在保护国家安全的同时拯救 TikTok》行政令。行政令基于《保护美国人免受外国对手控制的应用程序法》（简称“该法”）。该法授权总统通过跨机构程序认定“合格剥离”，从而解除对外国对手控制的应用程序的限制。行政令指出，现已提交一份框架协议，拟对 TikTok 的美国业务进行合格剥离。根据该框架协议，将设立一家总部在美国的新合资企业，运营 TikTok 美国业务；美国投资方持有和控制大多数股份，字节跳动及其关联方持股低于 20%；新董事会独立管理，受制于保障国家安全和用户数据保护的规则。

行政令认为，根据该法，总统必须通过“跨机构程序”认定框架协议的剥离是否构成“合格剥离”。根据总统的授权和指示，跨机构程序由副总统牵头，联合国家安全委员会、财政部、司法部、商务部、国家情报总监办公室等部门。该程序包括大量跨机构审议与磋商、多次由专家及国家安全官员提供的简报，以及与外部各方的深入谈判。该跨机构程序已就拟议剥离的各个方面向总统提出建议。

在完成该法所要求的跨机构程序后，总统作出如下认定：一是 TikTok 在美用户约 1.7 亿，平台对内容创作者和广告业务具有重要作用；二是国会立法是基于 TikTok 受外国对手控制的国家安全担忧；三是框架协议中拟议

的剥离解决国家安全担忧；四是该剥离安排符合“合格剥离”标准，适用于 TikTok、Lemon8、CapCut 及未来由新合资企业合法运营的其他应用。

此外，行政令指出，自行政令发布之日起 120 日内，司法部不得采取行动执行该法，以便完成剥离。（来源：美国白宫）

8. 欧盟委员会发布《人工智能严重事件报告指南》草案

9 月 26 日，欧盟委员会为落实《人工智能法》第 73 条的规定，发布《人工智能严重事件报告指南》草案，明确高风险人工智能系统在发生严重事件时的报告义务和流程。该指南旨在建立早期预警机制，确保人工智能技术在安全、透明和可控的框架下运行。

指南指出，严重事件包括但不限于：因人工智能系统运行引发人员死亡或健康严重受损、关键基础设施发生严重且不可逆转的中断、侵害欧盟法律所保护的基本权利以及对财产或环境造成严重损害。若事件涉及跨境大规模侵害，亦需即时报告。根据第 73 条规定，高风险人工智能系统的提供者须在获知事件后最迟 15 天内上报，若涉及跨境大规模侵害或关键基础设施中断，则需在 2 天内报告；如有人死亡，报告期限不得超过 10 天。部署者一旦发现严重事件，也须在 24 小时内通知提供者和主管机关。

除及时上报外，提供者还必须立即展开调查和风险评估，采取必要的纠正措施，并在调查过程中与主管部门保持合作。市场监管机构需在收到报告后 7 日内采取措施，成员国主管机构亦应第一时间通报欧盟委员会，以便建立跨境预警系统等。（来源：欧盟委员会）

9. 联合国启动全球人工智能治理对话

9月25日消息,联合国秘书长安东尼奥·古特雷斯近日在纽约举行的“全球人工智能治理多方利益攸关方高级别非正式会议”上发表讲话，宣布正式启动“全球人工智能治理对话”。该对话平台的建立旨在构建能够跟上人类历史上发展最快技术步伐的全球人工智能治理体系，为建立安全、可信、公正的人工智能生态奠定基础。

古特雷斯指出,自一年前通过《全球数字契约》(Global Digital Compact)以来，国际社会已从原则性共识迈向实际行动。本次全球对话的目标是通过联合国这一具有普遍代表性的平台，为全球各国提供平等参与的机会，共同讨论人工智能在社会、经济、伦理、技术、文化和语言等多方面的影响，并推动三大支柱性工作：政策、科学和能力建设。

在政策方面，全球人工智能对话将致力于帮助各方构建安全、可信、可监督的人工智能系统，使其根植于国际法、人权原则和有效监管之上；促进不同治理体系之间的互操作性，通过规则对接、减少壁垒、促进经济合作来推动协同发展；同时鼓励开放创新，支持开放源代码工具和共享资源的开发与使用，让创新成果为所有国家和社会所用。古特雷斯强调，问题已不在于人工智能是否将改变世界，而在于人类能否共同治理这一变革，而不是被它所主导。（来源：联合国）

10. 韩国将举行2025年人工智能攻防大赛

9月29日，韩国互联网振兴院（KISA）宣布将于今年下半年举办全球首个涵盖人工智能安全三大核心方向的“2025年人工智能攻防大赛”。

比赛题目将围绕人工智能安全的三个核心方向展开，包括“基于人工智能的安全”、“人工智能系统安全”和“人工智能平台安全”。这一设计旨在全面考察参赛者在人工智能与网络安全融合领域的技术能力和创新思维。参赛对象为对人工智能和网络安全有兴趣的韩国公民，年龄需在 19 岁以上。

本次大赛分为线上预选赛、线下决赛和颁奖典礼三个阶段。线上预选赛将于 2025 年 10 月 31 日至 11 月 1 日举行，决赛定于 12 月 1 日进行，颁奖仪式将于 12 月 2 日举行。（来源：韩国互联网振兴院）

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.印巴局势升级：军事行动与 DDoS 攻击双重“定点打击”

引言：2025 年 5 月 7 日，随着印巴局势进一步升级，绿盟科技伏影实验室全球威胁狩猎系统持续监测针到印方的 DDoS 活动更加剧烈，进一步印证了现实世界冲突与网络空间对抗存在明显的平行演进特征。攻击者不仅公开宣称攻击行动，还实施“定点打击”策略，将攻击目标升级为政府机构、军事设施及关键信息基础设施等高价值目标。同时，攻击时长也在不断增长，针对印度总统办公室网站的 DDoS 攻击持续时间创下新高，时长达 19 小时。在现实世界层面，2025 年 5 月 7 日后印巴冲突转入空中较量，5 月 8 日、9 日巴基斯坦相继摧毁印度 77 架无人机；5 月 10 日。巴基斯坦正式采取军事行动，命名“铜墙铁壁”，定点袭击印 26 个军事目标，并伴随网络攻击，巴方宣称网络攻击致使印度约 70%电网瘫痪。

随着国家间冲突的不断升级，网络空间的对抗模式已从传统的隐蔽行动转变为公开宣示的“作战”行为。甚至国家行为体开始直接参与网络攻击行动——巴基斯坦官方宣称网络攻击在本次冲突中颇具成效。从而形成了"现实军事-网络空间"双线联动的混合作战新形态。

关键词：印巴冲突；DDoS 攻击；

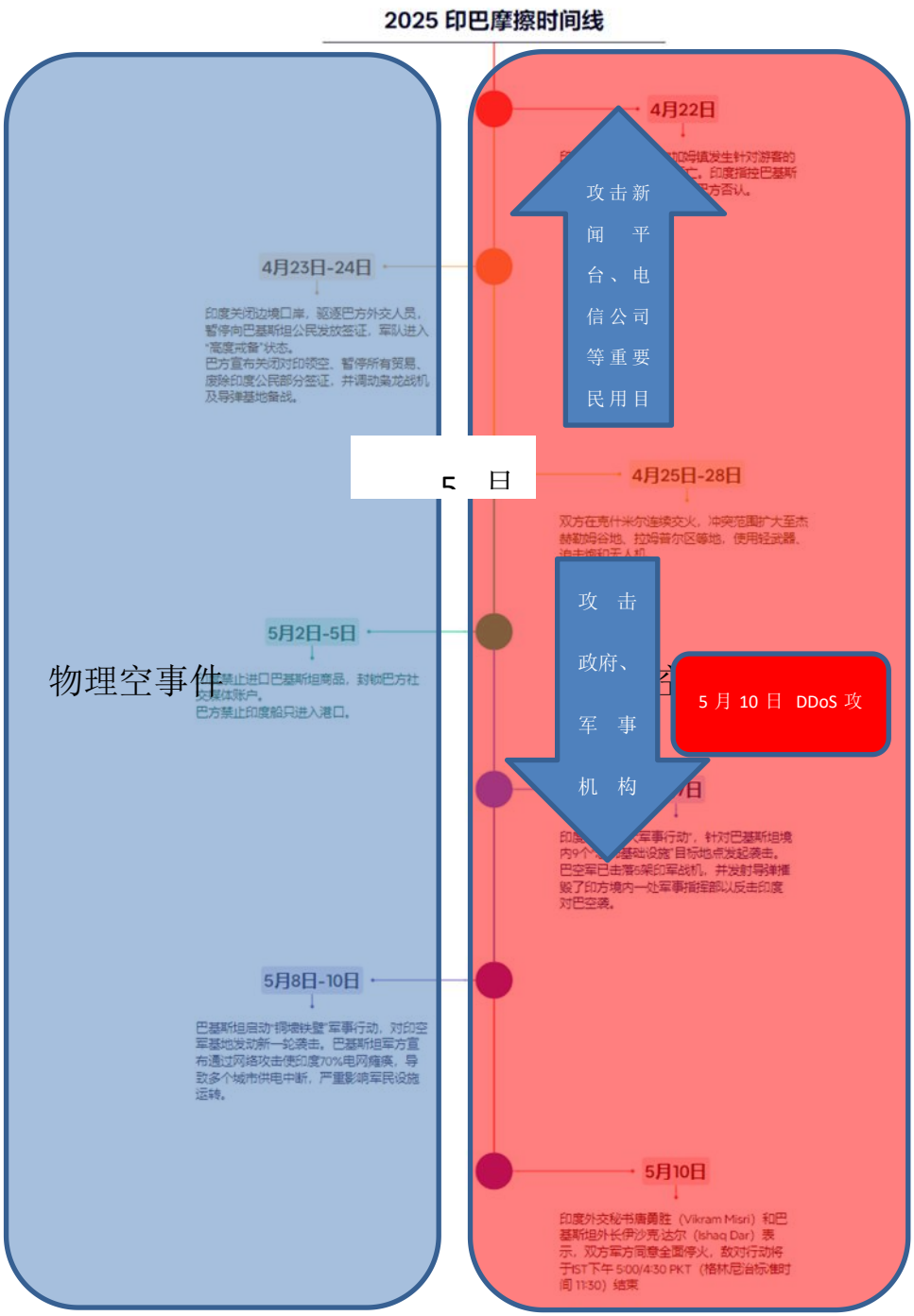


图 1　2025 印巴摩擦时间线

一、针对印度 DDoS 攻击活动总览

自 5 月 7 日起，印度发起“重大军事行动”，印巴冲突升级为空中对抗，印方首先采取战机导弹打击。伴随实体战事的演进，针对印度的 DDoS 攻击量也呈现显著增长，从 5 月 7 日持续上升，到 5 月 10 日达到顶峰，较

4 月 22 日摩擦前激增 97 倍（9700%），相较于 4 月 25 日至 28 日双方交火期间，涨幅亦高达 14 倍（1400%）。同日，巴基斯坦也启动“铜墙铁壁”军事行动，并宣称进行网络空间导致印度 70%电网瘫痪。5 月 11 日，双方同意全面停火后，DDoS 攻击强度虽有所回落，但整体攻击态势并未完全消退。

图 2　针对印度 DDoS 攻击趋势

在 5 月 7 日前，DDoS 攻击主要针对电信、新闻等行业。然而，随着局势升级，攻击目标发生了显著转移，政府机构、军事设施等关键部门成为首要攻击对象，且持续时长也逐步提升，这或与国家行为体支持的组织的直接参与有关，这些组织往往拥有的资源更多，能力更强，所造成的攻击效果及影响更大。

图 3　5 月 7 日前后重点攻击目标对比

二、重点攻击事件

2.1 针对印度国防部网站的网络攻击

2025 年 5 月 10 日 15:39，印度国防部（Ministry of Defence，MoD）官方网站（mod.gov.in）遭到长达 3 小时 56 分 57 秒的 DDoS 攻击。监测数据显示，攻击使用 NTP 反射放大手段。

印度国防部是印度政府的关键行政部门，负责统筹国家军事防务，特别是在与巴基斯坦爆发武装冲突期间，国防部更是作为最重要、最权威的统筹部门。其官方网站是印度国防事务的权威信息发布平台，承担公布政策文件、军事教育、征兵宣传、国家形象维护等多重作用。截至 5 月 12 日，印度国防部官方网站或为减少 DDoS 攻击影响，已经屏蔽来自境外的网络请求，国防部官网的外宣职能属于瘫痪状态。

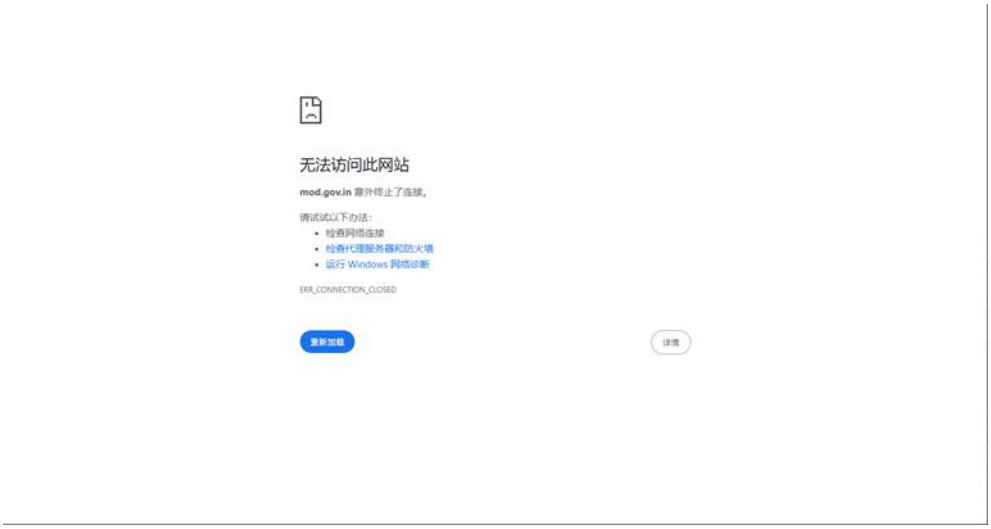


图 4　印度国防部屏蔽境外网络请求

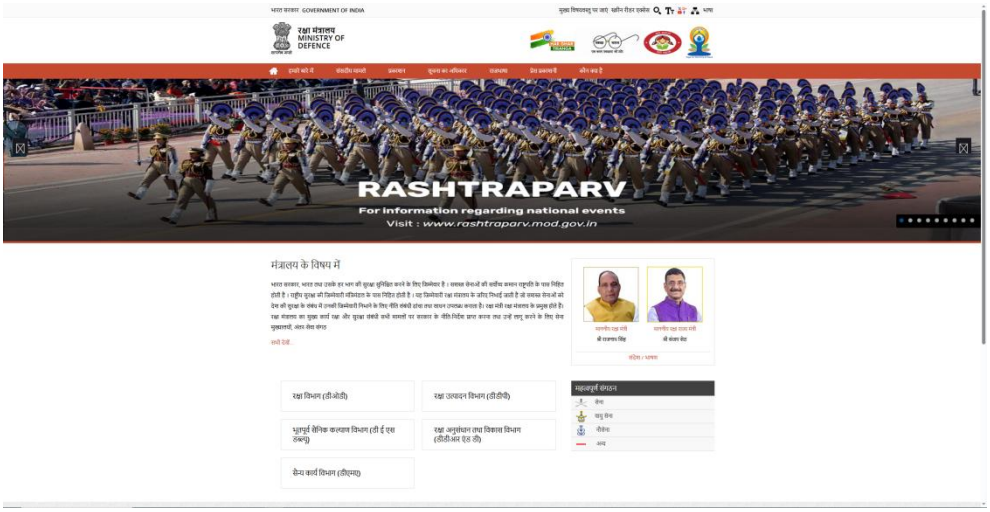


图 5　印度国防部官方网站（印度国内 IP 访问）

2.2 针对印度新闻信息局的网络攻击

2025 年 5 月 10 日 18:59，印度新闻信息局（Press Information Bureau，PIB）官方网站（pib.gov.in）遭到长达 1 小时 2 分 37 秒的 DDoS 攻击，攻击使用 DNS 反射放大手段。

印度新闻信息局是印度政府信息和广播部下属的一个节点机构，管理整个印度的印刷、传媒和网络新闻。其负责人兼任印度政府的官方发言人，该机构是印度的权威媒体机构。印度时间 5 月 10 日早上 10 时，印度新闻

信息局就“巴基斯坦官方称已使用网络攻击手段使印度 70%电力系统瘫痪”这一新闻予以反驳，声称电力系统运行正常。同日晚 18 时 59 分 17 秒，即遭受 DDoS 攻击。

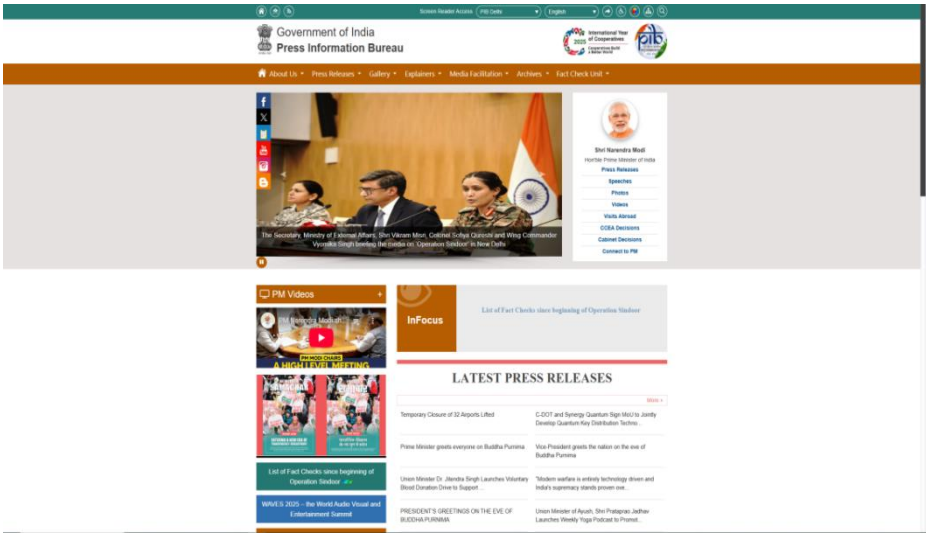


图 6　印度新闻信息局官方网站

2.3 针对印度总理办公室网站的网络攻击

2025 年 5 月 10 日 16:55，印度总理办公室网站（pmindia.gov.in）遭到长达 1 小时 51 分 13 秒的 DDoS 攻击。监测数据显示，攻击使用 DNS 反射放大手段。

印度总理办公室承担着政策传递、政府事务公开及公众互动等核心职能。是印度事实最高权力机构，承担着重要的政治角色和精神领袖角色。总理办公室网站遭受到 DDoS 攻击将影响到印度的社会舆情、国际形象、社会秩序等多个方面。

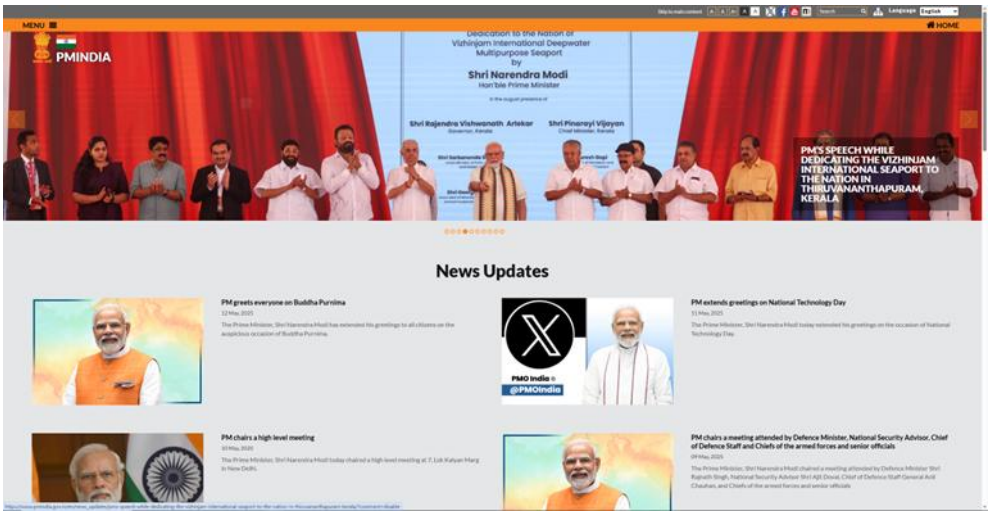


图 7　印度总理办公室官方网站

2.4　针对印度查谟和克什米尔邦政府网站攻击

2025 年 5 月 9 日 14:21，监测到 Mirai 僵尸网络针对印度查谟和克什米尔邦政府网站（www.jkgad.nic.in）攻击，攻击者使用 ACK Flood 攻击手段。

该网站主要发布查谟和克什米尔邦政府的行政通知、政策更新和公共事务声明，提供邦政府及下属机构的职位空缺、考试通知和录用结果，以及获取政府表格、报告、年度计划等文件。针对该网站攻击影响包括政务公告发布、行政文件下载等核心功能。

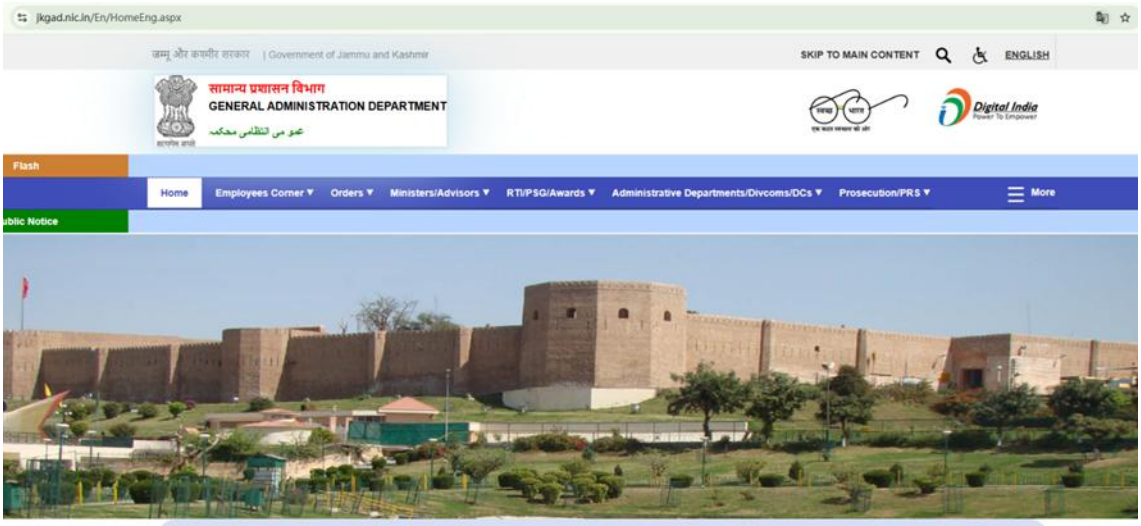


图 8　印度查谟和克什米尔邦政府网站

2.5 针对印度总统办公室网站攻击

2025 年 5 月 7 日至 8 日，印度总统办公室网站（presidentofindia.gov.in）连续遭受两轮 DDoS 攻击。监测数据显示，攻击者使用 DNS 反射放大手段发起攻击。首轮攻击始于 5 月 7 日 17:38，持续 2 小时 16 分钟 11 秒；次轮攻击更甚，从 5 月 8 日 00:47 开始，持续长达 19 小时 46 分钟 29 秒。

作为印度最高元首办公室的官方门户，总统办公室网站承担着政务公开、外事活动公示等重要职能。此次攻击可能会对网站服务造成影响，影响包括外事活动查询、总统府公告发布、公民请愿提交等在内的多项核心政务功能。

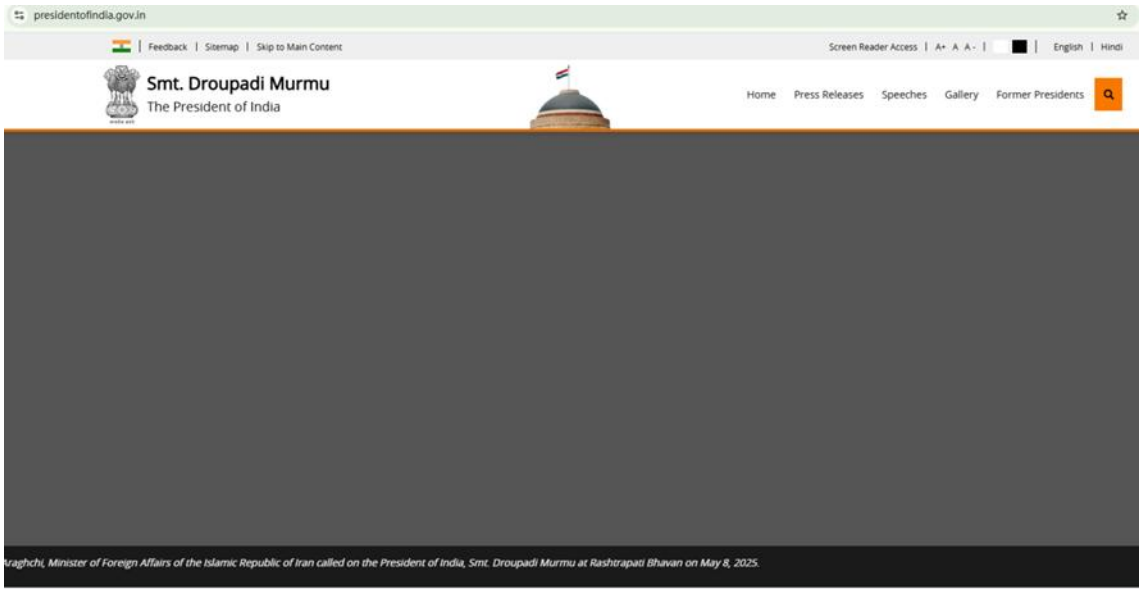


图 9　印度总统办公室网站

2.6 针对印度信息学中心域名解析服务的网络攻击

2025 年 5 月 7 日至 8 日，印度国家信息学中心的域名解析服务（ns2.nic.in）连续遭受两轮 DDoS 攻击。监测数据显示，攻击使用 DNS 反射放大手段发

起攻击。首轮攻击始于 5 月 7 日 22:29:28，持续 19 分 03 秒；次轮攻击更甚，从 5 月 8 日 00:46:44 开始，持续长达 1 小时 05 分钟 11 秒。

国家信息学中心（NIC）是印度电子和信息技术部（MeitY）下属的技术合作伙伴。NIC 成立于 1976 年，旨在为中央和州政府提供技术驱动的解决方案。NIC 作为印度政府核心 IT 基础设施管理机构，其域名解析服务可能因攻击瘫痪，导致全国大面积的互联网服务中断，影响极大。

图 10　印度信息学中心网站

结论：随着印巴局势的持续升温，DDoS 攻击的即时性特征愈发凸显，同时也展现出"规模压制"与"精准打击"的双重效果。一方面，攻击规模增长近两个数量级；另一方面，攻击目标明显向关键基础设施和政府核心部门等高价值目标集中。

此外，随着实体冲突升级至热战阶段，网络攻击行为已完全摒弃了传统的隐匿特性，攻击方开始公然宣称攻击行动，特别是国家力量的直接介入，使得网络打击呈现出前所未有的规模化和精准化特征。

值得警惕的是，即便现实冲突趋于缓和，网络空间的对抗也并没有立即停息。尽管印巴双方已于 2025 年 5 月 10 日达成停火协议，但 DDoS 攻击仍持续存在，只是攻击规模有所缩减。这充分体现了网络空间对抗的长期性和复杂性。

致谢

特别感谢绿盟科技伏影实验室对相关研究工作给予的支持。绿盟科技伏影实验室专注于安全威胁监测与对抗技术的研究，涵盖 APT 高级威胁、Botnet、DDoS 对抗、流行服务漏洞利用、黑灰产业链威胁及数字资产等新兴领域。

研究目标是掌握现有网络威胁，识别并追踪新型威胁，精准溯源与反制威胁，降低风险影响，为威胁对抗提供有力决策支持。

采用前沿技术探索与实战对抗相结合的研究模式，协助国家单位破获 APT 攻击案件数起，全球率先发现 8 个新型 APT 攻击组织，处置 40 多起涉我 APT 攻击事件，为国家重大网络安保做出突出贡献。（作者：北京神州绿盟科技有限公司 郑开发 吴铁军 范敦球 欧帅 兰星 孙炜）

行业前沿观察二:“智御未来-网络空间 AI 应用安全”论坛举行;《政务领域人工智能大模型部署应用指引》印发;“商用密码与数据安全创新应用”高级研修班举办;违法违规涉军自媒体账号典型案例

导读:近日,在国家网络安全宣传周火热开展之际,“岭南科技创新论坛”——“智御未来-网络空间 AI 应用安全”平行论坛在广州隆重举行。

为安全稳妥有序推进政务领域人工智能大模型部署应用,中央网信办、国家发展改革委近日联合印发《政务领域人工智能大模型部署应用指引》,为各级政务部门提供人工智能大模型部署应用的工作导向和基本参照。

9 月 26 日至 29 日,由国家人力资源和社会保障部批准、广东省人力资源和社会保障厅主办、广东省网络空间安全协会承办的“商用密码与数据安全创新应用”高级研修班在广州成功举办。

近期,一些自媒体账号违反《互联网军事信息传播管理办法》,违规发布涉军信息,误导公众认知,损害军队形象,社会影响恶劣。军地职能部门依法依规处置了一批网上违法违规信息及自媒体账号,通报有关典型案例。

关键词:互联网、AI、网络安全、网信办、未成年

1.聚焦人工智能健康发展，共建 AI 安全生态【岭南科技创新论坛】“智御未来-网络空间 AI 应用安全”论坛举行

近日，在国家网络安全宣传周火热开展之际，“岭南科技创新论坛”——“智御未来-网络空间 AI 应用安全”平行论坛在广州隆重举行。本次论坛由广东省科学技术协会主办，广东省网络空间安全协会承办，广东关键信息基础设施保护中心、广州网络空间安全协会、广东科技新闻工作者协会协办，广州华南检验检测中心有限公司、国源天顺科技产业集团有限公司为支持单位，汇聚政产学研用各界精英，共同探讨 AI 时代的安全新路径，分享 AI 应用安全新成果，凝聚共识，为构建安全、可信、负责任的 AI 应用生态贡献智慧。

广东省科学技术协会党组成员华旭初，广东省人力资源和社会保障厅原二级巡视员魏建文，广东省科学技术学会学术部三级调研员冯娟，北京网络空间安全协会理事长、广东省网络空间安全协会创会会长黄丽玲，广东科技新闻工作者协会理事长林亚茗，广州铁路公安局警务支援总队高级工程师林海，广东省网络空间安全协会常务副会长方满意、黄志豪、成珍苑及协会相关部门负责人等领导嘉宾出席论坛。国际先进技术与工程院院士、广州公共交通集团总工程师谢振东出席会议并作主题报告。中国网络空间安全协会副理事长兼人工智能安全治理专业委员会主任卢卫，中山大学电子与信息工程学院教授、博士生导师孙伟等 8 位业界学术领袖、企业高工出席会议并发表主题演讲。来自各大高校、科研院所、相关企业、安

全机构的专家学者和相关人士共200余人参加论坛。论坛由省网络空间安全协会党支部专职副书记、执行秘书长黄汝锡主持。

AI浪潮正重塑世界，赋能千行百业，但随之而来的安全风险也日益凸显。本次论坛就此至关重要的议题，设置了1场论坛和2场专题研讨会，14场学术报告，聚焦网络空间安全中“AI应用安全”，剖析大模型应用中的新型安全威胁，展示AI应用安全前沿科学技术和应用，共建AI安全生态，推动安全测评标准、安全检测工具与人才体系发展，为各单位、企业AI应用安全生态构建提供借鉴和参考。

北京网络空间安全协会理事长、广东省网络空间安全协会创会会长黄丽玲在致欢迎辞中提到，2025年“岭南科技创新论坛”以“科技赋能 向新自强”为主题，聚焦人工智能、量子科技等前沿领域，而广东协会承办的“智御未来-网络空间AI应用安全”平行论坛正是紧扣主论坛核心导向精心设计的，既是主论坛“科技赋能”重要拼图，也是对“向新自强”的有力支撑。为了让本次论坛成为AI安全领域的思想碰撞平台，论坛特别邀请到院士专家、行业大咖们带来主题分享。她表示，广东省网络空间安全协会作为5A级社团、广东省科协信创联合体牵头单位、省科协和省科技厅认定的科普教育基地，始终把“守护网络空间安全、服务数字广东建设”作为核心使命，以本次论坛为起点，在广东省科协的带领下，继续发挥桥梁纽带作用，深化科研机构的合作，加强与企业的联动，助力企业“安全用AI、放心用AI”。

广东省科协党组成员、副主席华旭初在致辞中高度评价协会的工作，他表示本次论坛是2025年“岭南科技创新论坛”七大平行论坛中首场举办的平行论坛，广东省网络空间安全协会进行了非常精心细致的准备，设置了2个分论坛，14场学术报告，内容非常充实。他代表省科协对协会的倾情付出表示感谢，对协会的蓬勃发展感到高兴。他指出，科技创新是推动国家发展和社会进步的核心动力，希望各与会代表、各会员单位坚持创新求变的科学情怀、求真务实的科学精神，深入交流学术思想与最新成果，积极开展跨领域的对话合作，为全面推进广东科技创新强省和粤港澳大湾区国际科技创新中心建设贡献智慧和力量。

作为活动重磅内容，本次论坛通过与会院士专家、行业领袖、企业高工们覆盖具身智能安全、AI治理、风险研判、安全测评、可信算力环境等前沿内容的高质量分享，探索人工智能技术在网络空间应用带来的机遇与挑战，展现AI应用安全前沿科学技术和应用。

国际先进技术与工程院院士、广州公共交通集团总工程师谢振东首先发表了《AI从落地到防护：具身智能应用与安全设计》主题报告，通过背景介绍、具身智能落地与特点、具身智能落地应用场景、具身智能落地安全风险与挑战、具身智能安全设计、总结展望六大点内容，为大家系统性地阐述了具身智能的应用前景与安全设计要点。他指出，具身智能是AI技术落地的重要方向，它能提升效率、解决难题，但“安全”永远是前提——没有安全的应用，再先进的技术也无法真正服务于人。他表示，人机协同是未来的趋势，希望未来具身智能将聚焦“应用与安全并重”，安全技

术上可能出现 AI 自修复系统，机器人能自主检测漏洞并修复。相信只要我们守住安全底线，持续技术创新，具身智能一定能更好地融入生活、赋能产业。

“AI 安全治理，需要通过持续优化技术、完善规则、提升共识，让 AI 发展更符合人类共同利益。”中国互联网协会副理事长、中国网络空间安全协会副理事长卢卫以《人工智能赋能网络空间治理的实践探索》为题，通过各类型示例图文展示剖析人工智能伴随的各类风险问题，分享人工智能技术内生安全风险及技术应对措施，为 AI 产业健康发展提出具体建议和方向。

中山大学电子与信息工程学院教授、博士生导师孙伟在《科学研判人工智能发展的风险与挑战》主旨演讲中，为大家总结梳理了 AI 技术发展的八大基本态势，并从“对社会治理的风险挑战”“国家安全风险”“对伦理和法律的风险挑战”三大方面内容分析了人工智能带来的风险挑战。通过对发展态势和风险挑战的梳理、分析，帮助大家进一步健康使用 AI。

广东省通信产业服务有限公司研究总院副总工程师/正高级工程师肖恒辉以《移动互联网 AI 应用安全能力评价研究》为主题，分享了关于 AI 应用安全的研究、AI 应用落地过程中的安全问题、AI 应用的安全能力、AI 应用安全能力评价体系、AI 应用安全框架—OWASP、AI 应用安全能力评测架构等研究内容，以及 AI 内容安全评价方法、智能体安全评价方法、大模型安全评价方法等。

广东关键信息基础设施保护中心主任张伟作《AI 大模型应用安全风险与防控》主题分享，从大模型安全风险概述、训练阶段安全风险、微调阶段安全风险、应用阶段安全风险、安全风险防控策略、行业最佳实践六大方面内容，助力企事业单位有效应对大模型应用中的各类风险，提升安全使用能力。

华为技术有限公司 AI 安全解决方案架构师王伟以《大模型安全挑战及防护方案》为题做分享计算中心安全建设经验，分析阐述了 AI 发展阶段下当前基于 Transformer 的 AI 模型威胁与挑战，以及为应对 AI 发展过程中安全威胁与挑战，各利益相关方建立 AI 安全的多层护栏等内容。以华为为例，分享了华为 AI 安全治理管理护栏实践、华为 AI 安全治理管理护栏实践。

联通（广东）产业互联网有限公司安全事业部副总经理、高级工程师苏轶作《让智能更安全，让安全更智能》主题演讲，通过展示网络安全典型案例与发展趋势和对人工智能自身安全风险、人工智能赋能安全攻防等方面内容的分析，分享人工智能安全标准体系、人工智能安全风险与能力矩阵、人工智能技术在安全领域应用的演进相关内容，以及相关应用场景和实战应用效果，为企业提供参考。

杭州安恒信息技术股份有限公司副总裁、资深安全专家宋宸宇以《大模型应用全生命周期安全实践》为主题，分享了数据合规风险、数据泄漏风险、数据篡改风险、数据投毒风险等大模型的风险挑战与安全威胁，并为大家梳理 AI 安全防护思路、构建前中后数据围栏、大模型安全应对防护方案、运行和使用防线、风险评估等实际应对内容。

深信服科技股份有限公司安全设计方案总监、安全专家常晓宇以《构建面向未来的 AI+安全架构体系》为题做分享，聚焦“安全大模型应该优先选择哪些场景来赋能？”这一问题分析行业和技术痛点，并就“大模型重构安全的下一阶段——闭环安全工作流”这一内容进行了详细展示，为未来的 AI+安全架构体系打开可落地的新思路。

智御未来筑网络空间 AI 应用安全新堡垒

人工智能的未来浩瀚无垠，AI 安全发展是行稳致远的关键。本次论坛的成功举行，是广东乃至全国人工智能健康安全发展的新起点，各位业界领袖、行业专家的深刻见解，为人工智能领域行业的发展提供了宝贵经验和重要参考。

岭南科技创新论坛是广东省列入保留举办清单的少数高层次学术活动品牌之一，已有 20 年历史，设立以来始终聚焦服务广东省重点产业发展，推动形成跨领域的深度对话合作机制。

“智御未来-网络空间 AI 应用安全”论坛是 2025 年“岭南科技创新论坛”的七大平行论坛之一，同期还在 9 月 20 日举行“AI 应用安全攻防”“AI 应用安全保障”两场研讨会，展示企业级 AI 安全防护框架与实践案例，共建 AI 安全生态，推动安全测评标准、安全检测工具与人才体系发展。

2.中央网信办、国家发展改革委印发《政务领域人工智能大模型部署应用指引》

贯彻党中央、国务院决策部署，落实《关于深入实施“人工智能+”行动的意见》要求，为安全稳妥有序推进政务领域人工智能大模型部署应用，中央网信办、国家发展改革委近日联合印发《政务领域人工智能大模型部署应用指引》（以下简称《指引》），为各级政务部门提供人工智能大模型部署应用的工作导向和基本参照。

《指引》坚持以习近平新时代中国特色社会主义思想为指导，深入贯彻落实党的二十大和二十届二中、三中全会精神，全面贯彻习近平总书记关于网络强国的重要思想，坚持系统谋划、集约发展，以人为本、规范应用，共建共享、高效协同，安全稳妥、务求实效，有序推进人工智能大模型技术、产品和服务在政务领域的部署、应用和持续优化。

《指引》强调场景牵引。政务部门可围绕政务服务、社会治理、机关办公和辅助决策等工作中的共性、高频需求，因地制宜、结合实际，选择典型场景进行人工智能大模型探索应用。

《指引》强调规范部署。政务部门应根据不同政务场景需求与现有技术基础，审慎选择人工智能大模型实施路径。应以统筹集约的方式开展政务领域人工智能大模型部署，地市应在省（自治区、直辖市）统一要求下开展部署应用，县级及以下原则上应复用上级的智能算力和模型资源开展应用和服务。应探索构建“一地建设、多地多部门复用”的集约化部署模

式，统筹推进政务大模型部署应用，防止形成“模型孤岛”。应加强政务数据治理，持续提升数据质量，支撑政务大模型的优化训练。

《指引》强调运行管理。政务部门应统筹减负和赋能，避免盲目追求技术领先、概念创新，切实防范“数字形式主义”。应建立健全全周期管理体系，明确应用方式和边界，落实人工智能大模型“辅助型”定位，防范模型“幻觉”等风险。应将持续迭代优化作为人工智能大模型部署应用的关键环节，建立常态化更新机制。应扎实做好安全管理，建立安全责任制度，明确安全职责和任务，提升人工智能安全风险应对能力。应严格落实保密要求，防止国家秘密、工作秘密和敏感信息等输入非涉密人工智能大模型，防范敏感数据汇聚、关联引发的泄密风险。

《指引》指出，要加强组织实施，加快推进政务领域人工智能大模型国家标准体系建设和重点标准研制，及时总结推广典型场景和创新应用。开展监测评估，构建政务领域人工智能大模型部署应用全流程监测评估体系，持续迭代优化。做好培训宣传，增强工作人员应用能力和水平，提升全民数字素养。

政务领域人工智能大模型部署应用指引

为深入贯彻落实党中央、国务院决策部署，规范和引导人工智能大模型在政务领域的发展与应用，提升政务数字化智能化治理和服务水平，制定本指引。本指引主要为各级政务部门提供人工智能大模型部署应用的工作导向和基本参照，将根据实践进展，结合人工智能大模型发展和应用的新形势、新要求，进行动态调整。

一、总体要求

坚持以习近平新时代中国特色社会主义思想为指导，深入贯彻落实党的二十大和二十届二中、三中全会精神，全面贯彻习近平总书记关于网络强国的重要思想，完整准确全面贯彻新发展理念，统筹高质量发展和高水平安全，坚持系统谋划、集约发展，以人为本、规范应用，共建共享、高效协同，安全稳妥、务求实效，有序推进人工智能大模型技术、产品和服务在政务领域的部署、应用和持续优化，充分发挥人工智能大模型在复杂语义理解与推理、多模态内容生成、知识整合与分析等方面的优势，为工作人员提供高效辅助，为公众和企业提供便捷服务，推动政务创新发展，提升治理效能、优化服务管理、辅助科学决策。

二、应用场景

政务部门可围绕政务服务、社会治理、机关办公和辅助决策等工作中的共性、高频需求，因地制宜、结合实际，选择典型场景进行人工智能大模型探索应用。主要包括以下参考场景：

（一）政务服务类

1.智能问答。整合本地区、本部门、本领域业务资源和知识库等数据，利用自然语言理解、检索增强生成和知识图谱等技术，提供便捷的在线政务咨询服务，加强对公众诉求的准确理解，实时生成参考回答，帮助解决公众疑惑，提升信息获取便捷性。

2.辅助办理。整合政务服务办事指南、常见问题、用户评价和历史办理记录等数据，利用智能匹配和自动化处理等技术，提供智能导办、个性引

导、表单预填、辅助审核、进度查询和提醒等一站式政务辅助办理服务，辅助工作人员高效审核材料，支撑公众和企业便捷办理事项。

3.政策服务直达快享。构建政策服务知识库，细化政策要求、政策标签、推送条件、申兑流程等相关内容，利用“政策找人”“政策找企业”算法模型，加强公众和企业需求分析，实现政策智能匹配，推进惠民利民、惠企利企服务主动精准送达和一站式办理。

（二）社会治理类

4.智能监测巡检。利用无人机、视频监控、智能传感器等设备和计算机视觉等技术，对监控视频、图像、物联感知数据等进行实时分析，辅助工作人员实时监测房屋、道路、燃气、桥梁、供水、排水、供热、综合管廊等基础设施，及时发现异常行为、环境问题或设施故障等，自动识别潜在风险隐患，及时进行提醒，并根据异常情况和严重程度提供处置建议，提高监测巡检效率。

5.辅助执法监管。采用语音识别、视频分析、知识图谱、逻辑推理等技术，辅助执法人员将案件信息实时录入系统、穿透式发现问题线索、生成案件报告、快速检索法律依据和司法解释、查询类似典型案例等，提供针对性案件办理建议，提高执法监管效率和规范性。

6.市场风险预测。运用生成式时间序列分析模型和异常检测算法等，对各类市场数据进行监测和深度分析，捕捉市场动向，包括经济指标波动、异常情况等，预测可能出现的市场风险，研判对经济社会带来的影响和经济走势，并及时发出预警，为政府管理和社会治理提供支撑。

（三）机关办公类

7.辅助文书起草。利用大语言模型的生成能力，通过构建本地知识库和预设模板，为工作人员提供写作建议、辅助起草文书，对格式和内容等进行检查、校对和优化，提高工作效率，减轻基层负担。

8.资料检索。利用知识图谱构建和信息检索等技术，准确理解工作人员资料检索需求，实现政务信息快速检索、精准定位、多维度排序、智能关联和对比分析等，帮助工作人员提升资料检索效率和准确性。

9.智能分办。利用自然语言理解和多模态识别等技术，构建多维度任务分类和分办规则，对来文、来电、工单等任务进行自动识别、准确分类、辅助填写和优先级排序，实现辅助分发和智能派单，提高任务分办效率。

（四）辅助决策类

10.灾害预警。对来自卫星、地面传感器、地质监测站，以及预报预警、灾害风险普查等多源、多维、多模态数据进行大数据关联和综合分析研判，识别异常波动情况，预测可能发生的自然灾害，并提前发出预警，辅助政务部门及时采取有效措施，减轻灾害风险，减少灾害损失。

11.应急处置。利用强化学习等技术，对社会公共安全等突发事件的性质、特点、危害程度、影响范围、发展趋势和公众反应等进行分析研判，及时发现和预警风险隐患，基于突发场景、力量资源分布等快速模拟应急处置方案效果，提供科学合理的应急处置建议，优化救援资源配置，提高应急响应速度和效率。

12.政策评估。利用人工智能大模型推断分析能力与数据挖掘能力，对公众反馈、市场反应、经济指标和社会满意度等进行分析，构建多维度指标，评估政策目标实现程度、政策影响力和潜在问题，支撑政策制定部门进行政策优化。

13.智能辅助评审。利用自学习泛化认识、类人化评审推理、多模态智能解析等能力，对照有关要求开展项目评审，对项目文件内容进行深度扫描、智能解析，提出评审意见建议，辅助提高项目评审效率和科学性。

三、规范部署

政务部门应结合工作实际和场景特点，充分论证人工智能大模型的应用需求、实施路径、功能设计等，选择适宜的部署模式，统筹推进实施，推动共建共享，提升建设管理效能。

（一）合理选择实施路径

政务部门应根据不同政务场景需求与现有技术基础，审慎选择人工智能大模型实施路径。对于智能问答、辅助文书起草等通用性较强、数据资源丰富的场景，需采用市场上成熟，并已完成网信部门备案的模型产品和服务。对于辅助执法监管、市场风险预测等专业性较强、业务逻辑复杂的场景，可利用领域专家知识和专业数据进行针对性训练，打造垂直模型。在保障安全和不泄露国家秘密、工作秘密和敏感信息等的前提下，充分利用互联网算力和模型资源，开展政务领域人工智能大模型部署应用。鼓励探索政务智能体、具身智能等创新应用。

（二）统筹集约开展部署

政务部门应以统筹集约的方式开展政务领域人工智能大模型部署，依托“东数西算”和全国一体化算力网，统筹推进智能算力基础设施布局，并实施集中统一的安全管理和体系化技术防护措施，避免“碎片化”安全风险。有条件的中央和国家机关部门、省（自治区、直辖市）可统一部署智能算力资源、人工智能大模型，面向下属单位或下辖地区提供电子政务外网环境下的人工智能大模型服务。地市应在省（自治区、直辖市）统一要求下开展部署应用，县级及以下原则上应复用上级的智能算力和模型资源开展应用和服务，不再独立进行政务大模型建设和部署。

（三）探索实现统管复用

政务部门应探索构建“一地建设、多地多部门复用”的集约化部署模式，统筹推进政务大模型部署应用，防止形成“模型孤岛”。省（自治区、直辖市）应搭建政务领域人工智能大模型统一服务平台，并与政务云管理平台、政务应用和组件管理平台等融合共建，将区域内电子政务外网智能算力、政务大模型、政务数据集等资源纳入统一管理，形成要素资源“一本账”，支撑政务大模型运行监测，提供资源申请与调度服务，推动高效复用。国家行业主管部门按照业务需求和发展需要探索细分领域政务垂直大模型的统一训练与构建，加强与省（自治区、直辖市）协同部署，深化跨层级、跨地域的行业领域智能化赋能。垂直管理部门应强化模型、算力、数据等资源的统筹部署和管理，避免资源浪费。

（四）持续夯实数据基础

政务部门应加强政务数据治理，持续提升数据质量，加快构建客观反映公共政策、制度规范、业务流程和治理实效的高质量政务数据集和知识库，支撑政务大模型的优化训练。分类分级管理政务大模型涉及数据，加强训练数据、微调数据、知识库等管理，建立台账并详细记录数据来源、类型和规模等信息，确保数据来源可靠可追溯、内容准确有效。依托政务数据共享协调机制，统筹数据治理成果，推进高质量政务数据集的共建共享和生成数据的归集治理。探索基于大模型的政务知识治理路径，打造可信知识库，确保数据源的权威性、准确性和时效性。

四、运行管理

政务部门应强化政务领域人工智能大模型运行管理，健全管理制度、运行模式和安全要求，有序推进人工智能大模型技术、产品和服务在政务领域部署应用。

（一）明确应用管理要求

政务部门应统筹减负和赋能，严格落实《整治形式主义为基层减负若干规定》《关于防治“指尖上的形式主义”的若干意见》等相关要求，避免盲目追求技术领先、概念创新，避免重复建设、无效建设，避免未审先建、建而不管，避免强制使用、无效使用，避免数据多头采集、重复索要，切实防范“数字形式主义”。中央和国家机关政务领域人工智能大模型部署应用应纳入国家政务信息化规划统筹。政务部门应建立健全涵盖政务领域人工智能大模型部署应用全周期管理体系，明确应用方式和边界，落实人工智能大模型“辅助型”定位，及时解决部署与应用过程中出现的新问

题。应在政务大模型应用界面显著位置设置风险提示，明确告知大模型服务的局限性，做好大模型输出内容标识。对于智能问答、辅助办理等代表政务部门面向公众和企业提供服务的人工智能大模型应用场景，应严格执行内容审核制度流程，结合场景特点和技术能力合理采用人工审核、生成内容实时风控、多模型交叉校验等措施，防范模型“幻觉”等风险，确保输出内容不超出业务范围，保障内容准确性，维护政务部门公信力。

（二）持续推动迭代优化

政务部门应将持续迭代优化作为人工智能大模型部署应用的关键环节，建立常态化更新机制，加快功能优化，深化场景应用。密切关注技术发展动态，持续更新优化政务领域人工智能大模型的基础模型和安全能力。建立高效数据收集处理机制，及时更新支撑人工智能大模型运行的输入数据和知识库，并适时进行清洗、标注，补充优化训练数据集，持续提升模型能力。建立政务领域人工智能大模型用户评价反馈机制，及时收集、处理用户需求，以用户反馈驱动迭代优化。

（三）扎实做好安全管理

政务部门应建立安全责任制度，明确数据处理、大模型训练和场景应用各阶段参与主体的安全职责和任务，做好用户身份识别和权限管理。政务部门提供人工智能大模型服务时，应遵守《生成式人工智能服务管理暂行办法》等相关规定，使用具有合法来源的数据和基础模型，依法履行算法备案和安全评估等义务，与使用者签订服务协议，明确双方权利义务。构建政务领域人工智能大模型分类分级治理制度，完善安全管理流程，针

对可能出现的安全风险，制定应急处置预案。做好政务大模型对抗攻击的检测与处置，识别并拦截提示词注入、资源消耗攻击等。加强政务大模型内容安全管理，综合运用语义识别、规则库、模型算法等，做好多模态输入输出内容的识别、分析与管控，建立合理的代答、拒答机制，及时发现并处置违法和不良信息、敏感内容等。发挥新闻媒体内容审核优势，做好政务大模型训练数据的内容审核把关，加强政务大模型内容监测管理。做好政务大模型应用运行日志管理，定期对日志记录进行审计。推动形成安全风险威胁信息共享和应急处置机制，按照规定及时处置并报告安全事件，提升人工智能安全风险应对能力。

（四）严格落实保密要求

政务部门在模型训练、部署应用等过程中应加强数据安全保密和个人信息保护，坚持底线思维，严格落实“涉密不上网、上网不涉密”等保密纪律要求，采取加装保密“护栏”等措施，防止国家秘密、工作秘密和敏感信息等输入非涉密人工智能大模型，防范敏感数据汇聚、关联引发的泄密风险。制定完善人工智能大模型在政务领域应用相关保密管理制度，规范人工智能大模型选型、部署、训练、使用、废止等全流程保密管理。涉密信息系统应用人工智能大模型按照国家保密行政管理部门要求稳妥推进。

五、保障措施

（一）加强组织实施

加强统筹协调，稳妥有序推动人工智能大模型在政务服务、社会治理、机关办公、辅助决策等领域规范应用。加快推进政务领域人工智能大模型

国家标准体系建设和重点标准研制，明确应用效果评估、系统技术要求、智能技术应用等工作规范，支撑部署应用取得实效。及时总结推广政务领域部署应用人工智能大模型的典型场景和创新应用，推动复用增效。加强政务领域人工智能大模型部署应用经费保障，引入市场化的产品和服务竞争机制，探索企业建设运营、政府购买服务、按使用情况结算费用的运作模式，营造高效、可持续的政务大模型生态。

（二）开展监测评估

构建政务领域人工智能大模型部署应用全流程监测评估体系，适时开展监测评估工作。建立政务大模型安全测评机制，上线前对模型算法、生成内容、应用功能、配置环境、挂接数据、漏洞风险等进行充分测试验证，对发现的问题隐患进行整改加固。加强政务领域人工智能大模型系统运行状态、响应时间、准确性、安全性和潜在风险的实时监测分析，及时发现问题，并采取有效措施解决。做好人工智能大模型应用效能评价，及时总结经验，持续迭代优化，推动部署应用取得实效。

（三）做好培训宣传

开发涵盖人工智能大模型理论、技术、应用、安全、伦理、产业等内容的培训课程体系，开展人工智能素养和技能培训，提升领导干部对人工智能的认知水平，增强工作人员应用能力和水平。面向公众做好宣传教育，提升全民数字素养，积极回应用户关切，正确引导社会对政务领域人工智能大模型适用人群、场景、用途的认识和预期，客观反映人工智能大模型在优化政务服务、满足公众和企业需求、提升社会治理水平等方面的作用。

3.赋能数字时代“守密人”！“商用密码与数据安全创新应用”高级研修班圆满举办

9 月 26 日至 29 日，由国家人力资源和社会保障部批准、广东省人力资源和社会保障厅主办、广东省网络空间安全协会承办的“商用密码与数据安全创新应用”高级研修班在广州成功举办。此次研修班紧扣《商用密码管理条例》实施要求与国家网络安全战略部署，旨在培育兼具理论深度与实战能力的复合型安全人才，吸引了来自广东、广西、河北、江苏、山东、北京等多地的94 名中高级专业技术人员及管理人员通过线上线下结合方式参训，共同完成了一场聚焦数字安全核心领域的知识进阶之旅。

9 月 26 日至 29 日，由国家人力资源和社会保障部批准、广东省人力资源和社会保障厅主办、广东省网络空间安全协会承办的“商用密码与数据安全创新应用”高级研修班在广州成功举办。此次研修班紧扣《商用密码管理条例》实施要求与国家网络安全战略部署，旨在培育兼具理论深度与实战能力的复合型安全人才，吸引了来自广东、广西、河北、江苏、山东、北京等多地的94 名中高级专业技术人员及管理人员通过线上线下结合方式参训，共同完成了一场聚焦数字安全核心领域的知识进阶之旅。

魏建文在讲话中明确指出，数字经济已成为高质量发展的核心引擎，而商用密码与数据安全是守护这一引擎的“核心盾牌”。“此次高研班既是落实国家专业技术人才知识更新工程的具体行动，更是响应《广东省加快数字人才培育 支撑数字经济发展的若干措施》的务实举措。”他强调，随着《关键信息基础设施商用密码使用管理规定》等法规深入实施，密码

应用已从“合规要求”升级为“战略刚需”，希望学员们以此次学习为契机，筑牢理论根基、强化实战思维、深化省际协作、坚持学以致用，为各地数字安全防线建设注入新动能。同时，他对广东省网络空间安全协会的精心筹备与组织付出给予高度肯定，称其为研修班的高质量开展提供了坚实保障。

广东省网络空间安全协会常务副会长方满意代表承办单位致辞时表示，商用密码作为保障网络与信息安全的核心技术，直接关系国家主权、安全和发展利益。为确保培训质量，协会组建了“政产学研”融合的顶尖师资团队——既有广州市密码管理局的政策专家，也有工信部五所、西安电子科技大学、中山大学等单位的技术权威，更有广州华南检验检测中心的实战派测评专家；13 场专题课程覆盖法规政策、前沿技术、行业应用、风险防控全链条，实现从理论到实践的无死角覆盖，为学员搭建起系统的知识学习平台。

精品课程+顶尖师资：构建“政策-技术-应用-评估”完整知识体系 此次研修班的师资阵容与课程设计堪称行业标杆。授课专家中，广州市密码管理局商用密码处副处长刘昌劲深度解读商用密码产业发展法规政策，帮助学员精准把握合规边界；工业和信息化部电子第五研究所教授级高级工程师刘杰剖析国内外商用密码标准体系，厘清技术应用的规范框架；西安电子科技大学广州研究院副教授赵搏文聚焦商用密码前沿技术趋势，带学员洞察行业发展方向；中山大学网络空间安全学院教授付印金则深入讲解人工智能对密码的挑战与应对策略，破解新兴技术带来的安全难题。 此外，

量子通信与量子密钥分发（QKD）、后量子（PQC）密码安全、轻量级密码算法应用、数据要素安全技术、多方计算在隐私计算中的应用等热点专题，均由华南师范大学、广东工业大学等高校教授及广州华南检验检测中心资深测评师主讲。课程体系严格遵循“政策-技术-应用-评估”逻辑：政策层面夯实法规认知，技术层面聚焦量子、后量子等前沿方向，应用层面覆盖金融、交通、医疗等关键领域，评估层面则通过密评流程、风险应急演练等内容强化实操能力——全方位满足不同领域学员的学习需求，为跨界交流搭建起优质平台。

学员心声：多维度收获，从“知识更新”到“思维重塑” 三天的研修课程不仅传递了专业知识，更引发了学员们的深度思考与热烈共鸣。不同背景、不同领域的学员纷纷分享学习心得，展现出研修班的显著成效。

高校代表：政策引领技术，搭建教学科研新框架

“商用密码技术作为保障数据安全的核心手段，是信息技术工作者迫切需要更新的知识领域。”珠海城市职业技术学院人工智能学院副教授杨裕表示，此次研修让她对商用密码的认知实现了从“碎片化”到“体系化”的跨越。她特别提到，政策法规课程让自己深刻认识到标准规范的引领作用，“国家制定的法律与标准体系，不仅为产业发展提供方向，更为我们今后申报、开发信息系统明确了密码安全要求”；而量子密码、后量子密码等前沿技术课程，则让她既有“危机感”——意识到技术迭代需持续学习，又有“自豪感”——我国在国产商用密码与量子技术领域的领先地位

令人振奋，并表示在未来将把所学融入教学与科研，为密码学科普教育和人才培养贡献力量。

科研院所代表：合规为基，打通“理论-实践”转化通道

“这次研修是连接理论与实践、打通科研与应用的宝贵经历。”广州市农业农村科学院高级工程师徐鸿卓的感受颇多。作为来自科研院所的学员，他此前更关注技术探索，而此次课程让他对“合规”有了全新认知，“三级等保系统必须通过密评，这不是技术选项，而是刚性制度约束。”这一认知将直接影响他未来的课题研究与项目申报——“让科研更好地与国家法规、行业标准对齐”。同时，技术“落地”的必要性也让他深受触动：“实验室里的算法再精妙，最终要能解决数据传输、存储、认证的实际问题。” 徐鸿卓表示，将把研修收获带回到科研岗位与三尺讲台，推动学术成果转化为保障数据安全的生产力。

企业代表：从“问号”到“感叹号”，解锁产业实践新路径

“3 天前，我们带着‘后量子时代加密投资会不会归零’‘数据要素安全边界在哪’的问号来；现在，13 个专题像十三束聚光灯，把问号都拉直成了感叹号！”深圳市品格营销服务有限公司市场咨询部总经理刘帅表示，作为企业学员，他最关注课程与产业实践的结合，而刘昌劲处长、刘杰高工对《密码法》《数据安全法》的解读，让他颠覆了“合规是成本”的认知，“合规是打开政府、金融、医疗大市场的钥匙！”，程晓峰老师讲解的国产密码算法进展更让他倍感振奋，“ZVC、SM9 等算法纳入国际标准，从‘跟跑’到‘领跑’的转变，让民族自豪感爆棚！”刘帅用“螺旋上升”

总结学习收获：“技术是螺旋桨，法规是尾翼，场景是气流——只有把密码嵌入AI、物联网的缝隙，才能产生真正的产业价值。”

跨区域学员：搭建协作桥梁，助力人才培育体系建设

“这次学习不仅构建了知识框架，更为广西与广东的密码人才协作搭建了桥梁。”广西桂测信息技术有限公司总经理刘燕作为对口帮扶省份学员，对研修班的“省际协作”价值感受深刻。她表示，课程让自己实现了三大思维转变，认识到密码安全是“基于计算复杂性的安全观”，明白“系统安全性取决于最弱一环”，更坚定了“密码学是支撑多领域的实用技术”的认知。同时，刘燕还分享了广西在密码人才培训方面的探索——申请《密码工程技术人员》《机器人工程技术人员》省级培训资质、申报职业技能等级评价机构等。她认为，研修班的结束是合作的开始，未来将推动桂粤两地在密码人才培育与技术应用上的深度协作。

“零基础”学员：从“陌生”到“系统”，开启密码安全新认知

“此前我对‘商用密码’的理解只停留在‘银行U盾’，甚至分不清‘商用密码’与‘核心密码’的区别。”揭西县人民医院信息技术员杨树勋坦言，自己是商用密码领域的“小白”，而此次研修实现了“从零到一”的启蒙。通过法规课程，她建立起系统认知：“商用密码不是可选的安全附加项，而是数字业务合法合规运行的必选项”；行业案例则让抽象技术变得具体，她直观感受到密码技术的落地价值。密评流程课程更让她警醒：“某政务云平台因未用国密算法被评为‘部分符合’，需投入百万元整改——密评是倒逼安全提升的硬约束。”黄湘云表示，未来将向团队分享所

学，推动“商用密码合规”理念普及，并计划考取专业认证，持续深化学习。

技术团队代表：未雨绸缪，聚焦前沿安全挑战

中国电子科技集团公司第五十四研究所检验试验中心部门主任王桂娟重点聚焦商用密码标准体系、密评流程与后量子密码三大专题。“商用密码早已不是抽象概念，而是守护数字世界的核心基石。”她分享道，通过对比国内外标准体系，看到了我国商用密码在与国际接轨的同时展现的特色优势；密评课程则让小组摸清了“安全落地”的路径——“2025 年 8 月实施的新规要求关基设施‘规划、运行前必过密评，运行后每年再评’，这是从源头防控风险”；而后量子密码课程更让大家感受到“未雨绸缪”的战略意义：“传统 RSA 算法可能被量子计算破解，‘现存后解’攻击风险提醒我们，必须提前布局 PQC 迁移。”王桂娟小组的体会颇具高度，“密码安全是合规必修课，密评是安全试金石，后量子密码是未来防火墙——这三点将指导我们未来的技术研究。”

结业展望：以知促行，为数字安全贡献力量

研修班结业后，考核合格的学员将获得《广东省专业技术人才知识更新工程培训证书》，培训学时可记入《专业技术人员继续教育证书》，为职业发展提供有力支撑。广东省网络空间安全协会副会长、此次高研班班主任成珍苑表示，后续将持续跟踪学员学习成效，希望各位学员能够学以致用，将所学到的理论知识应用到实际工作中去，不断提升自己的业务能

力和综合素质，广东省网络空间安全协会将继续为广大专业技术人员搭建成长与提升的平台，推动研修成果转化为数字安全治理的实际效能。

此次“商用密码与数据安全创新应用”高级研修班的举办，不仅为全国培养了一批数字时代的“守密人”，更搭建了跨区域、跨领域的交流协作桥梁。正如学员们所言，“聚是一团火，散是满天星”——带着三天的知识沉淀与思维重塑，他们将奔赴五湖四海，把商用密码与数据安全的理念、技术与实践经验融入工作，为我国数字经济安全发展、网络强国建设注入源源不断的力量。

4.违法违规涉军自媒体账号典型案例

近期，一些自媒体账号违反《互联网军事信息传播管理办法》，违规发布涉军信息，误导公众认知，损害军队形象，社会影响恶劣。军地职能部门依法依规处置了一批网上违法违规信息及自媒体账号，通报有关典型案例。

一、消费退役军人身份。网络账号“你的赖班长”、“泔肃青年”等，以退役人员身份，发布服役期间拍摄的日常训练、演训任务影像。网络账号“久久（已退役）”、“小文子退伍女兵”等，借退役军人身份吸粉引流，违规着军服拍摄短视频、进行网络直播，诱导网民充值打赏。

二、兜售涉密敏感资料。网络账号“小川素材店”、“强荷好物”等，售卖军事行动相关视频素材和限军队内部发行书籍，借涉密敏感军事资料违规牟利。

三、歪曲解读政策规定。网络账号“未来领导者”、“红岸与帝方”、“红盾主任”等，长期发帖炒作涉军校招生、转业安置、待遇保障、文职招考等有关政策，唱衰军事职业前景，并有偿提供相关咨询指导服务。

四、抹黑军队军人形象。网络账号“与军偕老”、“辣手写字”等，编撰大量抹黑军队军人形象文章，污名化军婚军恋，掺杂披露训练任务细节。网络账号“我喜欢在公园撸猫”、“军中绿花争芳斗艳”等，长期利用 AI 工具，制作发布丑化军队形象的图像视频。

5.“2025 首都工会公益伙伴项目-生产企业数字化人才培训与培养项目”线下培训活动打造数字化人才队伍

“北京市总工会 2025 首都工会公益伙伴项目——生产企业数字化人才培训与培养系列活动”以“安全为本-智造未来：数字化人员人工智能安全保障能力提升”为主题，由北京市总工会主办，北京网络空间安全协会承办，中国冶金地质总局矿产资源信息中心作为系列活动顺义区联合承办。活动以“送课上门”方式，在全市生产企业聚集的六个产业园区内举办六场免费课程。这些课程分别面向各产业园内及附近的生产企业、有关单位以及工会职工，由人工智能安全专家进行授课。此外，活动还组织部分学员分别实践走访四家网络安全行业的头部企业，探寻网络安全先进技术，聆听实战专家的讲解。

当前，人工智能技术加速迭代、深度融入经济社会各领域，成为驱动高质量发展的核心引擎，但技术跃进的背后，数据安全、算法公平、伦理

规范、防范滥用等安全挑战也随之凸显，筑牢人工智能安全防线、提升专业保障能力，既是时代赋予的使命，更是推动人工智能健康有序发展的关键支撑。随着人工智能技术的广泛运用，制作业作为传统产业的典型代表，相当一部分企业已经远远地落后于新技术发展的步伐，出现了发展瓶颈。生产企业做为制造业的关键组成部分，加强职工对人工智能和 AI 技术安全的认识和应对能力，是企业发展甚至关系存亡的重要举办。

此次系列活动旨在宣传生产企业数字化人才培训与培养项目，提升生产企业从管理层到基层员工的数字化意识，培养既懂技术又懂安全的生产企业数字化复合型人才，帮助企业职工更深入理解和应对由人工智能技术引发的安全挑战，确保生产企业在数字化转型过程中的安全性和可控性。当然，人才培养是一项系统工程，非一朝一夕可以达成。故本活动设计名称为系列活动，旨在有步骤、有针对性、稳妥地逐步推进、渗透扩散，营造氛围、版块提升，努力为生产企业数字化人才队伍建设做出应有的贡献。

举办生产企业数字化人才培训活动，核心目的是打通“技术-业务-人”的协同壁垒，具体有三点核心价值：破解数字化落地瓶颈，解决一线员工“不会用”、技术与生产“两张皮”问题，让 MES、IoT 等工具真正融入生产流程，提升设备利用率、产能及质量稳定性；构建复合型人才梯队，培养既懂生产工艺又掌握数字化技能的核心团队，填补工业数据分析师、智能制造工程师等关键岗位缺口，支撑企业长期数字化转型；激活数据驱动能力，帮助员工建立“用数据说话、用数据决策”的思维，从生产数据

中挖掘优化空间（如预测性维护、排产优化），降低成本、提升企业核心竞争力。

此次活动为社会培养大量适配产业升级需求的数字化人才，缓解就业市场专业技能人才供需矛盾，助力劳动力结构优化。活动已经在产业园区、单位举办 6 场线下集中培训，并组织 4 场走访行业头部企业，参加培训学员超 700 人，目前已完成 4 场培训，正在全面推进中。众多生产企业成功数字化转型后，将提升整个制造业的生产效率与产品质量，增强产业国际竞争力，推动上下游产业链协同发展，进而带动区域经济增长，为社会繁荣注入活力。

未来，在北京市总工会领导下，北京网络空间安全协会将继续以企业需求为导向，为北京地区的新型生产企业数字化人才提供网络空间安全专业性的培训，为首都打造一支掌握网络安全专技能力的数字化人才队伍。

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，开展信创大赛，举行安全论坛，举办教育培训活动等。广东省网络空间安全协会将举办2025年“第四届广东信创大赛”；湖南省网络空间安全协会走访数字湖南有限公司深化网安合作，共筑数字湖南屏障；甘肃省商用密码行业协会“密码法治陇原行”活动获评全省网络法治宣传优秀案例；中关村可信计算产业联盟成功举办自主可信计算与数据流通基础设施安全论坛；上海市信息安全行业协会成功举办“安全智造2025——AI赋能智能制造安全新生态”主题论坛；沈阳市网络安全协会开展2025年国家网络安全宣传周培训教育活动；海南省网络安全和信息化协会与海口市信息中心党支部联合开展网络安全主题党日活动；苏州市互联网协会举办苏州市网络安全进园区医疗卫生专场活动等。

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将举办2025年“第四届广东信创大赛”

为贯彻落实习近平总书记对技能人才工作的重要指示精神，打造职业技能竞赛中的广东信创职业技能竞赛品牌，弘扬精益求精的工匠精神。进一步发挥竞赛在高技能人才培养选拔和技能人才队伍建设方面的推动作用，加快培养和选拔一批信息通信信息化系统管理和数据库管理高技能人才，促进广东信息通信信息化系统管理员和数据库管理员高技能人才队伍提质增量，根据广东省人力资源和社会保障厅《关于做好2025年广东省行业企业职业技能竞赛工作的通知》（粤人社函（2025）112号）要求，广东省网络空间安全协会将于9-12月面向全省信息化系统管理员、数据库管理从业人员和在校学生举办“2025年第四届广东信创大赛—信息通信信息化系统管理员职业技能竞赛、数据库管理员技能竞赛”、2025年“第四届广东信创大赛—信创知识竞赛”。

2.湖南省网络空间安全协会走访数字湖南有限公司深化网安合作，共筑数字湖南屏障

为进一步深化网络安全领域政企协同，强化行业资源整合与技术交流，9月3日，湖南省网络空间安全协会在理事长苏金树教授的带领下，前往数字湖南有限公司开展专项走访交流活动。

在数字湖南公司总经理石凌凡、相关部门负责人陪同下，协会一行参观了公司安全体系大屏。安全和科技部总经理燕玮现场讲解，汇报了公司在网络安全态势感知、风险预警及应急响应等方面的技术架构与实战能力。

协会主管单位省公安厅网络安全支队杨军副支队长、协会理事长苏金树教授向数字湖南公司颁发“副理事长单位”牌匾，标志着双方正式建立更深层次的协作关系。

3.甘肃省商用密码行业协会“密码法治陇原行”活动获评全省网络法治宣传优秀案例

日前，在庆阳市举办的2025年“全国网络普法行·甘肃站”活动上，全省网络法治宣传十大优秀案例发布。由甘肃省国家密码管理局指导、甘肃省商用密码行业协会创新实施的“密码法治陇原行”活动成功入选。

“密码法治陇原行”活动自2020年启动以来，已先后在兰州、武威、庆阳等8个市州成功举办。活动坚持总体国家安全观，深入贯彻落实《密码法》和《商用密码管理条例》，创新实施“省局政策指导+协会会员参与+市（州）局属地执行”的协同普法模式，着力解决基层单位“不知、不懂、不会用密码”的难题。

4.中关村可信计算产业联盟成功举办自主可信计算与数据流通基础设施安全论坛

9 月 25 日，由中关村可信计算产业联盟主办的 2025 地理信息技术创新大会平行论坛——自主可信计算与数据流通基础设施安全论坛成功举办。

中国工程院沈昌祥院士出席会议并做《用自主可信计算确保数据基础设施安全可信》主题演讲。地理信息系统与自主可信计算的交叉融合形成该论坛的亮点，与会代表期待以此次论坛为契机，在推动地理信息系统智能化、生态化、产业化发展的同时，运用自主可信计算筑牢网络安全的防护基础，为可信数据空间及地理信息系统保驾护航。

5.上海市信息安全行业协会成功举办“安全智造 2025——AI 赋能智能制造安全新生态”主题论坛

9 月 24 日下午，由上海市信息安全行业协会承办的“安全智造 2025——AI 赋能智能制造安全新生态”主题论坛在国家会展中心（上海）5.2 馆圆满落幕。上海市经济和信息化委员会总工程师裘薇、东浩兰生会展集团副总裁张荣健出席并致辞，来自制造业、安全企业、科研院校的专家、企业代表和专业技术人才等近百人出席了活动。

论坛聚焦人工智能技术在智能制造安全领域的应用与治理，共同探讨 AI 驱动下智能制造面临的安全挑战与应对策略，并举行了多项备受行业瞩目的颁奖与聘书颁发仪式。

6.沈阳市网络安全协会开展2025年国家网络安全宣传周培训教育活动

为进一步增强人民群众的网络安全意识和自我防范能力，营造安全、健康、文明、和谐的网络环境，近日沈阳市网络安全协会开展了2025年国家网络安全宣传周培训教育活动。

活动中，协会专家组先后前往辽沈银行、中铁建大桥工程局集团第三工程有限公司、中国航发燃气轮机有限公司、中国石化辽宁分公司开展网络安全专题培训。此次培训不仅是协会践行“网络安全靠人民”理念的具体行动，更以专业赋能为公众筑牢网络安全“防护网”，为区域网络安全建设注入关键力量。

7.海南省网络安全和信息化协会与海口市信息中心党支部联合开展网络安全主题党日活动

9月18日，海口市信息中心党支部联合海南省网络安全和信息化协会党支部成功开展“增强网络安全意识，共筑网络安全防线”主题党日活动，将网络安全理念从理论推向实践，为筑牢区域网络安全屏障注入红色动能，以党建引领护航数字时代安全发展。

在网络安全意识专题培训环节，网络安全专家麦培围绕“日常办公中的高风险场景”“AI钓鱼邮件识别”“政务数据分类分级”等热点，通过真实攻防案例、网络安全架构设计，为参会人员敲响警钟。座谈交流环节气氛热烈，党员代表们结合岗位实际，就“网络安全人才缺口”“跨境数

据流动监管”“重保时期应急值守”等话题畅所欲言。宣传环节，“网络安全宣传小分队”分赴市政府办公区，粘贴宣传标语、发放网络安全知识手册、防范指南等宣传资料。

8.苏州市互联网协会举办苏州市网络安全进园区医疗卫生专场活动

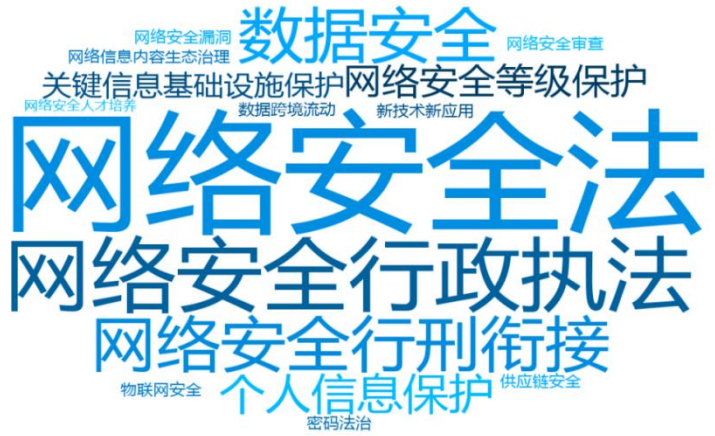
9 月 17 日，恰逢 2025 年国家网络安全宣传周期间，由苏州市互联网协会、苏州市卫生信息与健康医疗大数据学会卫生健康网络安全专委会联合主办的苏州市网络安全进园区医疗卫生专场活动在苏州大学附属第一医院顺利举行，50 余名医疗卫生机构及网络安全企业代表参会。

活动中，苏州市卫生健康信息中心介绍了苏州市 2025 年卫生健康系统网安行动总体情况，并针对行动中发现的问题宣贯相关标准。现场，网络安全领域的指导老师带领三支队伍分别围绕“数据安全”“账号权限”“API 安全”核心主题开展集中培训、讨论与桌面推演，每组代表通过主题陈述的方式展示团队研讨成果，并接受现场提问与点评。

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

……