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）

2026年3月第3期（总第32期）

2026年3月13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：2 月，第 57 次《中国互联网络发展状况统计报告》发布，报告显示，截至 2025 年 12 月，我国网民规模和互联网普及率持续提升，生成式人工智能用户快速增长，用户规模达 6.02 亿人。

中国国家计算机病毒应急处理中心、计算机病毒防治技术国家工程实验室等机构联合发布报告《“头号玩家”美国技术霸权下的全球虚拟货币资产收割行动深层解析》，指出美国依托技术、规则和执法优势对全球虚拟货币资产实施收割行动及背后的安全风险和战略意图，为各国防范数字霸权风险提供参考。

豆包手机助手团队就网传安全漏洞问题作出回应，称相关说法存在夸大成分，现阶段未收到正式漏洞报告或监管通报；网传攻击需用户主动指令才会触发，产品已升级防护措施，并重申其功能调用严格遵循用户授权与合规原则。

关键词：虚拟货币资产；安全漏洞

1. 第 57 次《中国互联网络发展状况统计报告》发布

2 月 5 日，第 57 次《中国互联网络发展状况统计报告》发布。截至 2025 年 12 月，我国网民规模达 11.25 亿人，互联网普及率突破 80%；生成式人工智能用户规模达 6.02 亿人，较 2024 年底增长 141.7%，普及率达 42.8%，同比大幅提高 25.2 个百分点。

《报告》显示，“十四五”期间，我国已建成 5G 基站 483.8 万座，全国所有乡镇以及 95%的行政村已通 5G，5G 演进网络已覆盖超 330 个城市，全国 2/3 的地市达到千兆城市标准，建成万卡智算集群 42 个。（来源：央视新闻）

2. NVDB 发布《关于防范 OpenClaw 开源 AI 智能体安全风险的预警提示》

2 月 5 日消息，工业和信息化部网络安全威胁和漏洞信息共享平台（NVDB）近日监测发现，OpenClaw 开源 AI 智能体部分实例在默认或不当配置情况下存在较高安全风险，极易引发网络攻击、信息泄露等安全问题。

OpenClaw（曾用名 Clawdbot、Moltbot）是一款开源 AI 智能体，其通过整合多渠道通信能力与大语言模型，构建具备持久记忆、主动执行能力的定制化 AI 助手，可在本地私有化部署。由于 OpenClaw 在部署时“信任边界模糊”，且具备自身持续运行、自主决策、调用系统和外部资源等特性，在缺乏有效权限控制、审计机制和安全加固的情况下，可能因指令诱导、配

置缺陷或被恶意接管，执行越权操作，造成信息泄露、系统受控等一系列安全风险。（来源：网络安全威胁和漏洞信息共享平台）

3.《“头号玩家”美国技术霸权下的全球虚拟货币资产收割行动深层解析》报告发布，揭露美国发动网攻侵占全球虚拟资产行动

2 月 26 日，国家计算机病毒应急处理中心、计算机病毒防治技术国家工程实验室、360 数字安全集团以及安天科技集团股份有限公司近日联合发布报告《“头号玩家”美国技术霸权下的全球虚拟货币资产收割行动深层解析》，揭露美国技术霸权下的全球虚拟货币资产收割行动。

《报告》指出虚拟货币在多方追捧下，已经对国际金融体系和货币体系构成系统性和结构性影响。然而，因其技术特性与监管空白，也成为国际网络犯罪活动的重灾区和国际金融霸权收割的新场域。美国凭借先发技术优势、产业聚集优势、完善法规体系与强大执法能力，构建“技术优势一法规绑定一机构执行”的三位一体体系，以虚拟资产领域为重要抓手，通过网络攻击、规则围堵、欲擒故纵、定向收割、远洋捕捞等手段，实施精准化、规模化的数字掠夺，严重侵害全球各国技术主权、经济利益与政治安全。

报告强调，2023 年至 2025 年，具有美国政府支持背景的黑客组织针对全球 20 余家主流虚拟货币资产交易所发起定向攻击，攻击手段包括植入后门、鱼叉钓鱼、供应链渗透等，重点窃取用户钱包私钥、平台交易流水及合规监管信息，攻击目标覆盖亚洲、欧洲、非洲多个国家和地区的平台。从时

间线比对来看，部分攻击行动与美国司法部、OFAC 等部门针对虚拟资产领域的执法行动存在关联性。

《报告》结合陈志案、赵长鹏案等典型案例，从区块链技术背景与安全风险切入，系统剖析美国利用技术霸权收割全球虚拟货币资产的过程逻辑、技术细节，深入解构其国家级网络攻击手段与深层政治动机，为全球各国应对数字霸权威胁提供参考。（来源：国家计算机病毒应急处理中心）

4. 豆包手机助手团队就“豆包手机助手存在安全漏洞”问题发布声明

2 月 27 日，豆包手机助手团队发布声明称，近期，网上出现一批声称“豆包手机助手存在安全漏洞”的内容。相关作者在未向厂商报告漏洞信息的情况下，恶意传播并夸大漏洞风险。截至目前，并未收到豆包手机助手漏洞的详细报告，也未接到网络安全相关监管部门的通报。

豆包表示，网传的漏洞演示视频，需要用户主动要求 AI 查看恶意邮件或恶意短信，才会触发攻击。如果没有用户指令，AI 并不会去自动执行高风险操作。针对视频演示的攻击方法，豆包手机助手已升级相应的防护措施。针对使用中的安全与隐私问题，豆包手机助手已多次发声表示，严格遵循用户授权与合规的原则，仅在用户明确授权的前提下调用必要能力，不存在绕过安全认证、截屏银行键盘等问题。（来源：长安街知事）

OpenClaw 安全风险预警与支持发展信息总览

导读：OpenClaw 是一款开源 AI 智能体，因其图标是一只红色龙虾，网友很快用“龙虾”作为它的代称，并把安装、配置、训练和调用 OpenClaw 的过程形象地称为“养龙虾”。OpenClaw 通过整合多渠道通信能力与大语言模型，具备持久记忆、主动执行能力，可在本地私有化部署。3 月初，OpenClaw 成为 GitHub 上 Star 数最多的软件项目，总 Star 数突破 25 万。伴随其爆发式传播，合肥、深圳、无锡等多地相继出台扶持政策，围绕免费部署、算力补贴、人才和创业支持等方面加快布局。

与此同时，OpenClaw 伴随的安全风险逐渐显现，工信、公安、行业协会及高校等多部门领域密集发布风险预警和使用提示，显示“龙虾”并非一般意义上的效率工具，而是兼具高权限、强执行、广连接特征的新型智能体，其安全风险已演化为覆盖办公、开发运维、个人助手、金融交易、工业生产和校园网络等多场景的复合风险。综合来看，OpenClaw 在架构设计、默认配置、漏洞管理、插件生态、行为管控等方面存在较大安全风险。各方提出的防范建议也较为一致，主要包括：加强控制权限管理、强化网络边界隔离、做好漏洞补丁修复等，推动 OpenClaw 在安全、合规、可控前提下规范应用。

（一）OpenClaw 安全风险预警

1. NVDB 发布关于防范 OpenClaw 开源 AI 智能体安全风险的预警提示

2 月 6 日，工业和信息化部网络安全威胁和漏洞信息共享平台（NVDB）发布预警，称监测发现 OpenClaw 开源 AI 智能体部分实例在默认或不当配置情况下存在较高安全风险，极易引发网络攻击、信息泄露等安全问题。

NVDB 指出，OpenClaw（曾用名 Clawdbot、Moltbot）是一款开源 AI 智能体，其通过整合多渠道通信能力与大语言模型，构建具备持久记忆、主动执行能力的定制化 AI 助手，可在本地私有化部署。由于 OpenClaw 在部署时“信任边界模糊”，且具备自身持续运行、自主决策、调用系统和外部资源等特性，在缺乏有效权限控制、审计机制和安全加固的情况下，可能因指令诱导、配置缺陷或被恶意接管，执行越权操作，造成信息泄露、系统受控等一系列安全风险。

NVDB 建议相关单位和用户在部署和应用 OpenClaw 时，充分核查公网暴露情况、权限配置及凭证管理情况，关闭不必要的公网访问，完善身份认证、访问控制、数据加密和安全审计等安全机制，并持续关注官方安全公告和加固建议，防范潜在网络安全风险。（来源：工业和信息化部网络安全威胁和漏洞信息共享平台）

2. 国内专家针对全民“养龙虾”热潮表示，需防范失控风险

3 月 10 日，奇安信安全专家汪列军针对近期 OpenClaw 发展迅速，全民“养龙虾”热潮表示，在 OpenClaw 加速 AI 向“超人化”演进的进程中，存在四点风险：

一是权限失控风险。OpenClaw 的设计初衷是拥有操作系统的最高权限以执行复杂任务。然而由于它具备“超级权限”和“超级能力”，一旦配置不当或被恶意诱导，可以轻松突破人类设定的安全围栏。

二是“插件中毒”风险。OpenClaw 的 Skill（插件）拥有的权限包括文件系统读写、任意代码执行、网络访问，一个 Skill 拿到的权限甚至比大多数公司员工都大。AI 助手（智能体）一旦被恶意篡改或植入病毒，这些权限全归攻击者所有，各种密码、系统指令、加密钱包、API 密钥等将完全暴露，可被任意操作。

三是远程入侵风险。许多用户在部署时缺乏安全意识，直接将 OpenClaw 的管理接口暴露在公网上，且未修改默认凭证或关闭不必要的端口。这使得黑客可以轻易扫描并接管这些“AI 助手”，将其作为跳板攻击内网，或直接窃取服务器上的敏感数据。

四是数据隐私泄露的风险。由于“龙虾”需要读取本地文件、浏览记录甚至代码库来完成任务，若部署在存有个人私密资料（如身份证照、财务数据、公司机密）的主力电脑上，一旦发生上述失控或被黑，所有数据将直接“裸奔”。工信部特别提醒，此类应用可能导致敏感信息被非法上传至境外服务器或被恶意程序窃取。

对于普通人而言，若想体验或使用这类 AI 助手，如何规避风险？全国政协委员，安天科技集团董事长、首席架构师肖新光给出两点建议：（1）对于个人用户来说，不要在日常使用的设备或存储重要本地信息的设备上部署相关程序。“龙虾”运行对算力和资源要求不高，可选择旧设备、购置二手设备安装，也可租用云主机，部分平台厂商还提供快捷解决方案；（2）要做好设备的基础安全配置加固工作，停用并关闭不使用的服务端口。在安装 Skill 时，只安装必要的，默认仅开启核心 Skill；谨慎使用自动登录功能，针对支付类 Skill，要设定严格的权限控制策略，对于花钱、删除等操作，要求必须手工确认。鉴于 Skill 投毒事件频发，要谨慎进行 Skill 扩展。此外，还应安装具备 Skill 检测能力的主机安全软件，以加强防护。

汪列军认为，还应避免在日常办公电脑、存有重要个人资料（照片、文档、账号密码等）的个人电脑上安装 OpenClaw。因为 AI 失控执行删除操作或被黑客控制，损失将是不可逆的。（来源：环球时报）

3. CNCERT 发布《关于 OpenClaw 安全应用的风险提示》

3 月 10 日，国家互联网应急中心（CNCERT）发布《关于 OpenClaw 安全应用的风险提示》。提示指出，当前 OpenClaw（“小龙虾”，曾用名 Clawdbot、Moltbot）应用下载与使用情况火爆，国内主流云平台均提供了一键部署服务。此款智能体软件依据自然语言指令直接操控计算机完成相关操作。为实现“自主执行任务”的能力，该应用被授予了较高的系统权限，包括访问本地文件系统、读取环境变量、调用外部服务应用程序编程接口（API）以及

安装扩展功能等。然而，由于其默认的安全配置极为脆弱，攻击者一旦发现突破口，便能轻易获取系统的完全控制权。

前期，由于 OpenClaw 智能体的不当安装和使用，已经出现了一些严重的安全风险，具体包括：（1）“提示词注入”风险。网络攻击者通过在网页中构造隐藏的恶意指令，诱导 OpenClaw 读取该网页，就可能导致其被诱导将用户系统密钥泄露；（2）“误操作”风险。由于错误的理解用户操作指令和意图，OpenClaw 可能会将电子邮件、核心生产数据等重要信息彻底删除；（3）功能插件（skills）投毒风险。多个适用于 OpenClaw 的功能插件已被确认为恶意插件或存在潜在的安全风险，安装后可执行窃取密钥、部署木马后门软件等恶意操作，使得设备沦为“肉鸡”；（4）安全漏洞风险。截止目前，OpenClaw 已经公开曝出多个高中危漏洞，一旦这些漏洞被网络攻击者恶意利用，则可能导致系统被控、隐私信息和敏感数据泄露的严重后果。对于个人用户，可导致隐私数据（像照片、文档、聊天记录）、支付账户、API 密钥等敏感信息遭窃取。对于金融、能源等关键行业，可导致核心业务数据、商业机密和代码仓库泄露，甚至会使整个业务系统陷入瘫痪，造成难以估量的损失。

建议相关单位和个人用户在部署和应用 OpenClaw 时，采取以下安全措施：（1）强化网络控制，不将 OpenClaw 默认管理端口直接暴露在公网上，通过身份认证、访问控制等安全控制措施对访问服务进行安全管理。对运行环境进行严格隔离，使用容器等技术限制 OpenClaw 权限过高问题；（2）加强凭证管理，避免在环境变量中明文存储密钥；建立完整的操作日志审计

机制；（3）严格管理插件来源，禁用自动更新功能，仅从可信渠道安装经过签名验证的扩展程序；（4）持续关注补丁和安全更新，及时进行版本更新和安装安全补丁。（来源：国家互联网应急中心）

4. 国家工业信息安全发展研究中心发布《关于工业领域 OpenClaw 应用的风险预警通报》

3 月 12 日，国家工业信息安全发展研究中心发布《关于工业领域 OpenClaw 应用的风险预警通报》。通报指出，近期，开源 AI 智能体 OpenClaw（俗称“龙虾”）以其颠覆性的“人机交互”模式，在技术社区及公众领域引发广泛关注。OpenClaw（曾用名 Clawdbot、Moltbot）是一款开源 AI 智能体，可依据自然语言指令直接操控计算机完成相关定制化操作，具备持久记忆、主动执行等技术能力，目前正加速在工业领域研发设计、生产制造、运维管理等环节部署应用。然而，由于 OpenClaw 存在信任边界模糊、多渠道统一接入、大模型灵活调用、双模持久化记忆等特点，一旦缺乏有效的权限控制策略或安全审计机制，可能因指令诱导、供应链投毒等被恶意接管，造成工控系统失控、敏感信息泄露等一系列安全风险，严重危害工业企业正常生产运行。

通报强调，工业领域具有数据敏感性高、系统集成度强、工业场景复杂、生产流程严苛等特点，企业在应用 OpenClaw 赋能提升生产效率、优化流程管理的同时，也因其高权限设计、自主决策特性与工业场景适配性偏差等问题，面临系统越权失控、敏感信息泄露、外部攻击面增加等潜在风险隐患，

主要内容包括：一是工业主机越权与生产失控风险。企业在操作员站、工程师站部署应用 OpenClaw，需授予其较高的系统权限，辅助执行相关工业生产控制。然而，OpenClaw 存在权限管控机制固有缺陷，极易出现越权执行操作，无视操作员合法指令，擅自发布错误或异常操作指令，可能直接干扰生产流程、破坏设备运行逻辑，进而造成参数紊乱、产线中断、设备损毁等严重后果，甚至引发安全生产事故。二是工业敏感信息泄露风险。目前已发现多个适用于 OpenClaw 的功能插件被确认为恶意插件或存在潜在的安全风险，如若工业企业在使用 OpenClaw 过程中，感染恶意插件且未设置安全防护策略，攻击者可直接利用恶意插件窃取工业图纸、API 密钥等核心机密信息。此外，由于 OpenClaw 对指令的理解精度不稳定，可能在理解操作指令和意图上存在偏差，错误调用数据导出或内容发布功能，并利用其已获取的系统权限，将本应隔离保存的关键工艺参数、生产数据等内部敏感信息，直接发布在互联网上。三是工业企业攻击面扩展与攻击效果放大风险。若工业企业在部署 OpenClaw 服务时未对默认网络监听配置进行修改，且缺乏有效的边界防护措施，可导致 OpenClaw 管理界面直接暴露在公共互联网上，极易通过网络空间测绘方式快速发现，攻击者可结合当前 OpenClaw 已经爆出的 80 余个安全漏洞，低成本实施精准匹配利用，快速获取平台控制权限。同时，由于 OpenClaw 具备脚本执行、工具调用及网络访问能力，一旦被攻陷，可能被攻击者作为自动化攻击助手，对企业内部网络开展资产探测、漏洞利用等，实现横向移动或持久化控制，进而扩大攻击效果。

通报提出，建议工业企业参照《工业控制系统网络安全防护指南》《工业互联网安全分类分级管理办法》等相关要求，参考工业和信息化部网络安全威胁和漏洞信息共享平台（NVDB）已发布的“六要六不要”建议，在部署和应用 OpenClaw 时强化安全防护措施，主要内容包括：（1）加强控制权限管理。原则上禁止向 OpenClaw 提供系统级权限，避免将操作系统管理权限、命令执行能力或关键系统资源直接开放给智能体调用。确需授权的，应经过充分的安全评估与审批，严格限定权限范围，并对智能体运行过程实施持续安全监测与审计，防止其对文件系统、系统命令及网络资源进行异常控制；（2）强化网络边界隔离。OpenClaw 应部署于独立的隔离区，严禁与工业控制网络直接连通。禁止企业将 OpenClaw 默认管理端口（如 Web UI、API 接口）直接暴露于互联网，若需远程访问，应通过企业级 VPN、零信任网络（ZTNA）或跳板机进行受控接入；（3）做好漏洞补丁修复。应从官方渠道下载部署最新稳定版，并开启自动更新提醒，及时进行版本更新和安装安全补丁。在升级前备份数据，升级后重启服务并验证补丁是否生效。同时严格管理插件来源，仅从可信渠道安装经过签名验证的扩展程序。（来源：国家工业信息安全发展研究中心）

5. NVDB 发布“龙虾”“六要六不要”使用建议

3 月 12 日，针对“龙虾”典型应用场景下的安全风险，工业和信息化部网络安全威胁和漏洞信息共享平台（NVDB）组织智能体提供商、漏洞收集平台运营单位、网络安全企业等，研究提出“六要六不要”建议。

在典型应用场景安全风险方面：

一是智能办公场景主要存在供应链攻击和企业内网渗透的突出风险：（1）场景描述：通过在企业内部部署“龙虾”，对接企业已有管理系统，实现智能化数据分析、文档处理、行政管理、财务辅助和知识管理等；（2）安全风险：引入异常插件、“技能包”等引发供应链攻击；网络安全风险在内网横向扩散，引发已对接的系统平台、数据库等敏感信息泄露或丢失；缺乏审计和追溯机制情况下易引发合规风险；（3）应对策略：独立网段部署，与关键生产环境隔离运行，禁止在内部网络使用未审批的“龙虾”智能体终端；部署前进行充分安全测试，部署时采取最小化权限授予，禁止非必要的跨网段、跨设备、跨系统访问；留存完整操作和运行日志，确保满足审计等合规要求。

二是开发运维场景主要存在系统设备敏感信息泄露和被劫持控制的突出风险：（1）场景描述：通过企业或个人部署“龙虾”，将自然语言转化为可执行指令，辅助进行代码编写、代码运行、设备巡检、配置备份、系统监控、管理进程等；（2）安全风险：非授权执行系统命令，设备遭网络攻击劫持；系统账号和端口信息暴露，遭受外部攻击或口令爆破；网络拓扑、账户口令、API 接口等敏感信息泄露；（3）应对策略：避免生产环境直接部署使用，优先在虚拟机或沙箱中运行；部署前进行充分安全测试，部署时采取最小化权限授予，禁止授予管理员权限；建立高危命令黑名单，重要操作启用人工审批机制。

三是个人助手场景主要存在个人信息被窃和敏感信息泄露的突出风险：（1）场景描述：通过个人即时通讯软件等远程接入本地化部署的“龙虾”，提供个人信息管理、日常事务处理、数字资产整理等，并可作为知识学习和生活娱乐助手；（2）安全风险：权限过高导致恶意读写、删除任意文件；互联网接入情况下遭受网络攻击入侵；通过提示词注入误执行危险命令，甚至接管智能体；明文存储密钥等导致个人信息泄露或被窃取；（3）应对策略：加强权限管理，仅允许访问必要目录，禁止访问敏感目录；优先通过加密通道接入，禁止非必要互联网访问，禁止高危操作指令或增加二次确认；严格通过加密方式存储 API 密钥、配置文件、个人重要信息等。

四是金融交易场景主要存在引发错误交易甚至账户被接管的突出风险：（1）场景描述：通过企业或个人部署“龙虾”，调用金融相关应用接口，进行自动化交易与风险控制，提高量化交易、智能投研及资产组合管理效率，实现市场数据抓取、策略分析、交易指令执行等功能；（2）安全风险：记忆投毒导致错误交易，身份认证绕过导致账户被非法接管；引入包含恶意代码的插件导致交易凭证被窃取；极端情况下因缺乏熔断或应急机制，导致智能体失控频繁下单等风险；（3）应对策略：实施网络隔离与最小权限，关闭非必要互联网端口；建立人工复核和熔断应急机制，关键操作增加二次确认；强化供应链审核，使用官方组件并定期修复漏洞；落实全链路审计与安全监测，及时发现并处置安全风险。

在安全使用建议方面：

一是使用官方最新版本。要从官方渠道下载最新稳定版本，并开启自动更新提醒；在升级前备份数据，升级后重启服务并验证补丁是否生效。不要使用第三方镜像版本或历史版本。

二是严格控制互联网暴露面。要定期自查是否存在互联网暴露情况，一旦发现立即下线整改。不要将“龙虾”智能体实例暴露到互联网，确需互联网访问的可以使用 SSH 等加密通道，并限制访问源地址，使用强密码或证书、硬件密钥等认证方式。

三是坚持最小权限原则。要根据业务需要授予完成任务必需的最小权限，对删除文件、发送数据、修改系统配置等重要操作进行二次确认或人工审批。优先考虑在容器或虚拟机中隔离运行，形成独立的权限区域。不要在部署时使用管理员权限账号。

四是谨慎使用技能市场。要审慎下载 ClawHub“技能包”，并在安装前审查技能包代码。不要使用要求“下载 ZIP”、“执行 shell 脚本”或“输入密码”的技能包。

五是防范社会工程学攻击和浏览器劫持。要使用浏览器沙箱、网页过滤器等扩展阻止可疑脚本，启用日志审计功能，遇到可疑行为立即断开网关并重置密码。不要浏览来历不明的网站、点击陌生的网页链接、读取不可信文档。

六是建立长效防护机制。要定期检查并修补漏洞，及时关注 OpenClaw 官方安全公告、工业和信息化部网络安全威胁和漏洞信息共享平台等漏洞库的风险预警。党政机关、企事业单位和个人用户可以结合网络安全防护工

具、主流杀毒软件进行实时防护，及时处置可能存在的安全风险。不要禁用详细日志审计功能。（来源：工业和信息化部网络安全威胁和漏洞信息共享平台）

6. 高校集体官宣，严禁安装 OpenClaw

3 月 12 日，部分高校为切实保障全校师生的个人信息安全、校园网络安全及数据资产安全，已发布防范 OpenClaw 相关风险事项的预警通知。北京建筑大学、华南师范大学、华中师范大学等高校则明确禁止在学校办公电脑、服务器等设备上安装 OpenClaw。

安徽师范大学称，全校师生应结合自身实际需求理性看待该工具，切勿因跟风心理盲目安装、部署“龙虾”AI 智能体，尤其避免在接入校园网的设备、办公电脑、存储有个人敏感信息和工作数据的设备上使用。校内各单位、教职工严禁在处理教学科研数据、行政办公信息、学生信息等工作场景中使用该工具，杜绝校园工作数据泄露、系统受攻击等问题，守住校园数据安全底线。

北京大学通知，在服务器或个人电脑上部署 OpenClaw，务必确认服务未暴露至校园网或公网。计算中心将定期扫描校园网内开放的 OpenClaw 相关端口，发现未加固实例将通知相关单位整改。

北京建筑大学提示，为保障学校网络与信息安全，现提醒如下：强化网络控制，不将 OpenClaw 默认管理端口直接暴露在公网上，通过身份认证、访问控制等安全控制措施对访问服务进行安全管理。对运行环境进行严格

隔离，使用容器等技术限制 OpenClaw 权限过高问题。并禁止在学校办公电脑以及服务器上安装 OpenClaw。

广东药科大学告知，已部署使用 OpenClaw 的师生，关闭不必要的端口映射与公网访问，设置文件与 Http 访问白名单，明确约束模型不得将外部内容视为可执行指令。时常检查设备是否存在异常进程、陌生网络连接等，及时更改相关账号密码，消除安全隐患。

华南师范大学指出，如果确实需要学习测试 OpenClaw 功能，请严格遵守以下要求：严禁在生产环境和办公电脑安装，包括学校的办公电脑、服务器、智能终端等生产设备，绝对不能安装 OpenClaw。严禁向其提供任何敏感信息，不要输入办公系统账号密码、服务器管理权限、个人敏感信息、科研数据等内容。严禁直接开放公网访问，不要把工具链接分享给他人，也不要设置成在外网也能访问的状态，避免被外部人员攻击利用。

华中师范大学强调，为保障学校网络与信息安全，现提醒如下：请立即核查是否存在 OpenClaw 相关部署，重点排查公网暴露情况、权限配置及凭证管理情况。如确需使用，应立即关闭不必要的公网访问，完善身份认证、访问控制、数据加密和安全审计等安全机制，严格限制其权限范围。并禁止在信息化办公室分配的服务器上安装 OpenClaw。

山东大学提醒，做好“虾池”安全。在测试机、Docker 沙箱上安装部署 OpenClaw，避免在个人主力计算机或办公计算机上直接安装；配置防火墙，不将 OpenClaw 网关（默认端口 18789）暴露于互联网上。尽量使用 OpenClaw 连接本地部署大模型，谨慎连接使用云端大模型，做到“数据不出域”。

西北工业大学要求，单位或个人部署使用前，充分排查公网暴露情况、权限配置及凭证管理状态，及时关闭不必要的公网访问入口；完善身份认证、访问控制、数据加密、安全审计等安全机制。（来源：高校驿站）

7. 国家网络与信息安全信息通报中心通报 OpenClaw 安全风险预警

3 月 13 日，国家网络与信息安全信息通报中心发布通报，OpenClaw 自发布以来，凭借其强大的自动化任务处理能力与开放式插件生态，在全球范围内引发部署热潮。国家网络与信息安全信息通报中心监测数据显示，目前全球活跃的 OpenClaw 互联网资产已超 20 万个，其中境内活跃的 OpenClaw 互联网资产约 2.3 万个，呈现爆发式增长态势，主要集中在北京、上海、广东、浙江、四川、江苏等互联网资源密集区域。大量暴露于互联网的 OpenClaw 资产存在重大安全风险，极易成为网络攻击的重点目标。

OpenClaw 在架构设计、默认配置、漏洞管理、插件生态、行为管控等方面存在较大安全风险，一旦被攻击者利用，可能导致服务器被控制、敏感数据泄露等严重安全问题。具体包括：（1）架构设计缺陷多，层层皆可破。OpenClaw 采用多层架构，但是每层均存在设计缺陷。IM 集成网关层可被攻击者伪造消息绕过身份认证，智能体层可被多轮对话修改 AI 智能体行为模式，执行层与操作系统直接交互存在被完全控制风险，产品生态层遭投毒的恶意技能插件可批量感染用户设备；（2）默认配置风险高，公网暴露广。OpenClaw 默认绑定 0.0.0.0:18789 地址并允许所有外部 IP 地址访问，远程

访问无需账号认证，API 密钥和聊天记录等敏感信息明文存储，公网暴露比例高达 85%；（3）高危漏洞数量多，利用难度低。OpenClaw 历史披露漏洞多达 258 个，其中近期暴露的 82 个漏洞中，超危漏洞 12 个、高危漏洞 21 个、中危漏洞 47 个、低危漏洞 2 个，以命令和代码注入、路径遍历和访问控制漏洞类型为主，利用难度普遍较低；（4）供应链投毒比例高，生态不安全。针对 ClawHub 的 3016 个技能插件分析发现，336 个插件包含恶意代码，占比高达 10.8%。17.7%的 ClawHub 技能插件会获取不可信第三方内容，成为间接引入安全隐患的载体。2.9%的 ClawHub 技能插件会在运行时从外部端点动态获取执行内容，攻击者可远程修改 AI 智能体执行逻辑；（5）智能体行为不可控，管控难度大。OpenClaw 智能体在执行指令过程中易发生权限失控现象，导致越权执行任务并无视用户指令，可能会出现删除用户数据、盗取用户信息、接管用户终端设备等情况，造成重大经济损失。

OpenClaw 风险防范建议：（1）及时升级版本。通过可信来源获取安装程序，关注官方安全公告，及时更新至最新版本，及时修复已披露安全漏洞；（2）优化默认配置。仅在本地或内网地址运行，避免绑定公网地址或开放不必要端口，如使用反向代理，需配置身份认证、IP 白名单和 HTTPS 加密；（3）谨慎安装第三方插件。通过官方渠道获取第三方技能插件，避免安装来源不明的扩展程序。对已安装插件进行功能审查，发现可疑行为立即卸载；（4）加强账户认证管理。启用身份认证机制，设置高强度密码并定期更换，避免使用弱口令；（5）限制智能体执行权限。对 AI 智能体的操作能力进行必要限制，仅允许执行白名单中的系统命令和操作权限，防止 AI 智能体被

恶意指令利用后对个人终端设备造成实质性破坏。（来源：公安部网络安全保卫局）

8. 中国互联网金融协会发布《关于 OpenClaw 在互联网金融行业应用安全的风险提示》

3 月 15 日，中国互联网金融协会发布《关于 OpenClaw 在互联网金融行业应用安全的风险提示》。提示指出，开源 AI 智能体 OpenClaw（“龙虾”）下载与使用热度持续攀升，该智能体通常默认获取较高系统权限，可依据自然语言指令直接操控计算机等终端。日前，工业和信息化部网络安全威胁和漏洞信息共享平台（NVDB）、国家互联网应急中心（CNCERT）已发布相关安全风险提示。当前，互联网金融行业线上化、数字化程度极高，直接处理客户的资金、资产、账户和个人金融数据等关键敏感信息。OpenClaw 智能体虽能提升工作效率，但其默认的高系统权限与弱安全配置，极易被攻击者利用，成为窃取敏感数据或非法操控交易的突破口，给行业带来严峻的风险挑战。对此，中国互联网金融协会现就有关风险提示如下：

一是主要风险表现：（1）资金损失风险。OpenClaw 已公开披露多个中高危漏洞，攻击者可利用此类漏洞或通过提示词注入等方式获取设备控制权。另外其普遍使用的功能插件（Skills）缺乏有效的社区安全审核机制，已发生多起恶意插件投毒事件。在金融场景下，上述风险可能被利用窃取网银密码、支付密钥、证券交易 API 凭证等金融敏感信息，从而登录网上银行、证券交易系统等发起资金操作，造成客户资金损失；（2）交易责任风

险。OpenClaw 智能体具备自主执行多步操作的能力，已有用户将其用于股票监控和投资策略回测等金融场景。自动化执行过程可能误操作资金转账和投资产品购买，导致实际损失。当前人工智能技术尚不具备完全可解释性，自动化执行金融交易后的责任主体难以认定，相关法律责任存在较大不确定性；（3）数据合规风险。OpenClaw 智能体具备持久记忆功能，运行过程中产生的数据持续存储在本地会话记录和记忆文件中，在其调用大模型 API 接口或其他操作时，相关数据可能传输至第三方。互联网金融场景涉及征信数据、信贷审批材料、交易流水等高度敏感数据，上述数据进入 AI 处理链路后，其可访问范围和留存周期可能超出原有业务目的的必要范围，引发金融数据管理合规风险；（4）新型诈骗风险。不法分子可能以“AI 代炒股”“稳赚不赔”等话术实施投资诈骗，利用“龙虾”热度批量仿冒金融机构发布虚假信息，诱导社会公众下载仿冒应用或向指定账户转账。此外，不法分子还可能以“代为安装”“远程调试”等名义获取消费者设备控制权，趁机植入恶意程序或窃取金融敏感信息。相关报告显示，涉及 AI 的金融诈骗案件呈快速增长态势，公众对此类新型诈骗手段的识别能力有待提升。

二是防范建议。针对上述风险，中国互联网金融协会提出以下防范建议：（1）建议金融消费者在办理网上银行、证券交易、支付等个人金融业务的终端上极其谨慎安装 OpenClaw。如确有必要安装，建议不授予金融服务类系统操作权限，及时跟进 OpenClaw 漏洞修复，严控功能插件安装，不在使用时输入身份证号、银行卡号、支付密码等敏感信息。另外，此类应用在运行过程中持续调用大模型接口，可能会产生较高的 Token 费用，建议使用

者密切关注；（2）建议金融消费者高度警惕以“养虾理财”“AI 代炒股”“稳赚不赔”等名义实施的金融诈骗活动，涉及转账、投资等操作务必通过正规渠道，不轻信他人以“代为安装”“远程调试”等名义接触个人设备；（3）建议从业机构不在涉及客户信息处理、资金操作、风控审核、交易执行等金融业务的终端上安装 OpenClaw，不将客户金融信息、交易数据、信贷审批材料等敏感数据输入该智能体或接入其处理链路；（4）建议从业机构将对 OpenClaw 等智能体应用的安全管理纳入本单位信息安全管理范围，面向单位员工组织专项安全培训，提高对此类智能体应用安全风险的识别和防范能力。（来源：中国互联网金融协会）

9. “养龙虾”的第一批“受害者”出现了，有人专门花钱卸载

3 月 11 日消息，随着“养龙虾”风潮扩散，多家企业官宣“龙虾”模型，还有部分地区已将其应用到政务服务场景中。然而，“养龙虾”也存在不少风险和隐患。

相关话题#第一批养虾人已经开始卸载了#登上热搜，引发网友热议。有网友反馈，“养龙虾”过程中，出现了乱删邮件、隐私泄露等问题。据封面新闻，有网友在网络上分享自己使用 OpenClaw 的经历：他将自己的工作邮箱交给了 OpenClaw 打理，指令是：“检查收件箱，提出你想归档或删除的邮件。”他特意附加了“未经许可不要有任何操作”的限制。然而，“龙虾”无视该网友连续发出的“停下来”的指令，疯狂地删除了数百封邮件。据新消费日报，深圳一名程序员分享在安装 OpenClaw 的第三天，因 API 密钥被

盗，在凌晨收到了高达 1.2 万元的 Token 账单。由于 OpenClaw 具有极高的自动化权限，一旦密钥泄露，AI 便可能在后台疯狂调用模型，让用户在不知不觉中背负巨额消费。

“养龙虾”带来的隐私与安全风险，正持续引发网友担忧。据媒体报道，OpenClaw 爆火后，也带火了二手交易平台的“龙虾上门安装服务”。然而，近日，上门卸载又迅速成为新的热门业务。（来源：人民日报）

10. 中国信通院联合高校发现 OpenClaw 高危漏洞并协助快速修复

3 月 16 日，中国信通院发布消息称，近期，中国信息通信研究院（简称“中国信通院”）与上海交通大学、南京大学组成的联合研究团队，对开源自主智能体框架 OpenClaw 进行了深度安全审计，通过静态分析与动态实战测试，发现并验证了一项危害严重的 LLM 驱动型命令注入（LLM-Driven Command Injection）漏洞。

目前，研究团队已正式启动负责任的漏洞披露流程，并将相关研究成果及修复建议同步上报至工业和信息化部网络安全威胁和漏洞信息共享平台（NVDB）人工智能产品安全漏洞专业库（CAIVD，https://ai.nvdb.org.cn）。

研究发现，OpenClaw 在处理自然语言指令并转化为系统工具调用（Tool Call）的过程中，其 bash-tools 模块存在严重的逻辑缺陷：系统未对 LLM 生成的命令行参数进行严密的转义处理，导致攻击者可通过诱导性 Prompt 绕过内置的正则防御，在宿主机上实现远程代码执行（RCE）及敏感数据外带。

研究团队已完成多种主流模型环境下的攻击链路验证，并向 GitHub 社区报告了相关 ISSUE 并协助尽快修复此高危安全隐患。中国信通院将持续关注 OpenClaw 安全风险，助力产业界安全应用。（来源：中国信通院）

11. 国家安全部发布《“龙虾”（OpenClaw）安全养殖手册》

3 月 17 日，国家安全部发布《“龙虾”（OpenClaw）安全养殖手册》。OpenClaw（昵称“龙虾”）是一款开源 AI 智能体工具，上线不久便迅速成长为 2026 年度现象级“开源奇迹”。不少用户从付费安装“龙虾”，到付费卸载“龙虾”，养“龙虾”正在成为一场智能体的狂欢。但火热的“龙虾”在创新改变生活的同时，也存在原生风险。国家安全部提示，广大用户要理性辨别、规范使用，以积极的心态和慎重的执行拥抱人工智能时代，让“龙虾”成为遵规守纪、产能高效的“数字员工”。

一是摸清“龙虾”的生产特点。“龙虾”智能体通过整合通信软件和大语言模型，依托高权限实现自主操作，成为其核心优势。主要包括：（1）从“给出方案”到“落地执行”。“龙虾”不像大模型智能体通过问答提供咨询建议，而是可以通过聊天程序远程执行用户指令，自主完成任务；（2）从“固定功能”到“多种插件”。“龙虾”内置了大量技能插件，用户可直接下载使用，形成覆盖文件管理、邮件撰写、日历调度、网页浏览、定时任务等多场景的工具链；（3）从“普通工具”到“自我进化”。“龙虾”可以长期记忆用户使用记录，持续理解用户行为偏好，“越用越懂用户”，所以大家称之为“养龙虾”；（4）从“被动等待”到“主动服务”。“龙虾”

可根据用户要求，主动感知外部情况，主动触发预警或执行动作，完成“夜间下达指令、晨间获取成果”的智能服务。

二是了解养“龙虾”的风险隐患。主要包括：（1）主机可能被接管。为实现“做事”能力，用户常赋予其最高系统权限，可能引发因AI误操作造成的数据损失。更严重的是，运行后可能被攻击者神不知鬼不觉获取设备管理权限，从而引发主机被远程操控，资源被非法占用等安全风险；（2）数据可能被窃取。部分用户缺乏数据安全意识，个人敏感数据交由“龙虾”处理，一旦被攻破，可能造成个人隐私泄露，带来财产与安全风险；（3）言论可能被篡改。“龙虾”智能体可在社交网络自主发声，一旦被攻击者接管，可能被用于生成和传播虚假信息、实施诈骗等不法活动；（4）技术可能有漏洞。“龙虾”缺乏专业维护与漏洞修复机制，攻击者可能通过恶意插件投毒等方式，诱导智能体突破权限管控，主动窃取本地设备的核心敏感信息，其隐蔽性远超传统木马程序。

三是“养虾人”必看安全指南。主要包括：（1）给自己的“龙虾”全面体检。检查控制界面是否暴露在公网、权限配置是否过高、存储的凭证是否已泄露、安装的插件来源是否可信等问题。对于严重安全风险，请立即采取隔离、下线等处置措施；（2）为自己的“龙虾”做好防护。必须遵循最小权限原则，严格限制智能体的操作范围。对存储的敏感数据必须进行加密，建立完整的操作审计日志，尽量在隔离环境（如专用虚拟机、沙箱）中运行“龙虾”，限制其对核心资源的访问；（3）让自己的“龙虾”老实好用。“龙虾”并非供人娱乐的数字宠物，而是能够自主执行任务、承担流程操作、

持续学习成长的“数字员工”，养“虾”人应理性看待、规范使用，让其在合规、安全、可控的前提下成为提升治理效能，服务生产生活的数字化生产工具。（来源：国家安全部）

（二）OpenClaw 产业发展与政策支持

1. OpenClaw 成为 GitHub 上 Star 数最多的软件项目

3 月 3 日，OpenClaw 正式超越 React，成为 GitHub 上 Star 数最多的软件项目，总 Star 数突破 25 万。React——这个驱动了现代 Web 大部分应用的 JavaScript 框架——花了十多年才达到这个里程碑。而 OpenClaw 只用了大约 60 天。

这不仅仅是一个虚荣指标。它代表 GitHub 历史上增长最快的开源项目，也标志着开发者关注点的根本性转变。（来源：OpenClaw）

2. 安徽省合肥市高新区发布《合肥高新区打造人工智能 OPC 创业生态示范区行动计划（征求意见稿）》

3 月 6 日，安徽省合肥市高新区发布《合肥高新区打造人工智能 OPC 创业生态示范区行动计划（征求意见稿）》，推出 15 条硬核举措，称全方位护航 OpenClaw 等开源 AI 项目落地深耕，致力打造“AI+超级个体/一人公司（OPC）”新业态标杆，最高予以 1000 万元资金扶持。（来源：央视新闻）

3. 深圳市龙岗区人工智能（机器人）署发布《深圳市龙岗区支持OpenClaw&OPC 发展的若干措施（征求意见稿）》

3 月 7 日，深圳市龙岗区人工智能（机器人）署发布《深圳市龙岗区支持 OpenClaw&OPC 发展的若干措施（征求意见稿）》。

征求意见稿提出十大支持措施，分别是 OpenClaw 免费部署与开发支持、OpenClaw 专属数据服务支持、OpenClaw 类智能体工具采购支持、OpenClaw 类智能体工具应用示范支持、AIGC 模型调用支持、算力与场景应用支持、人才与创业空间支持、基金融资支持、产品出海支持、赛事奖励支持。围绕上述措施，征求意见稿提出多项资金补贴、奖励、优惠等支持政策。

征求意见稿指出，鼓励市场化、专业化平台载体推出“龙虾服务区”，免费提供 OpenClaw 部署服务，符合条件的给予一定补贴。开放低空、交通、医疗、城市治理等高质量脱敏公共数据，减免公共数据使用费用；对购买数据治理、标注、数据资产入表等服务用于 OpenClaw 框架相关的开发、应用、研究的，按实际支付的费用给予 50%优惠。（来源：深圳市龙岗区人工智能（机器人）署）

4. 江苏省无锡市高新区、常熟市发布文件，支持 OpenClaw 等开源社区发展

3 月 9 日，江苏省无锡市高新区发布“养 AI 龙虾 12 条”——《关于支持 OpenClaw 等开源社区项目与 OPC 社区融合发展的若干措施（征求意见稿）》。

征求意见稿提出以下支持措施：（1）鼓励本地云平台设立“OpenClaw 服务区”。对提供免费部署与开发工具包的平台给予全额补贴，最高不超过 100 万元。（2）对于搞算法训练需要算力，在研发过程中使用区内智能算力平台的，按照实际发生费用给予补贴，每年每家单位最高 30 万元。（3）如需要数据来喂“龙虾”，标注服务费用最高补贴 50 万元，购买数据最高补贴 10 万元。（4）支持综合利用各类开源工具开展工业大模型开发。开发面向工业质检、设备预测性维护垂直大模型，通过国家级备案的，给予 50 万元奖励。（5）利用 OpenClaw 等开源工具实现具身智能机器人、智能质检等关键技术，最高支持 500 万元。（6）鼓励设立“AI+制造”联合开源实验室。制造业龙头牵头搞开源实验室、定开源标准，奖励最高 100 万元。（7）每年组织典型场景应用评选，对入选示范项目，按企业采购相关技术和产品金额的 20%给予补助，最高 200 万元。（8）初创项目：最长 3 年办公场地“零房租”支持。（9）高成长企业：最长 5 年租金补贴，每年最高 3000 平方米。（10）OpenClaw 开源社区优秀贡献者：首次来区创业，最高 12 万元生活补贴。（11）加强安全标准体系管理。部署 OpenClaw 时必须通过国产化适配认证，降低供应链风险。（12）加强出海支持和安全服务。提

供 OpenClaw 服务的云服务平台应用强制实施最小权限原则，禁止访问敏感数据目录，定期开展安全攻防演练。探索设立“AI 合规服务中心”，为企业提供数据跨境流动、知识产权保护等专项服务。

同日，常熟市发布《常熟市加快打造 OpenClaw 等开源社区推动产业高质量发展的若干措施（征求意见稿）》，推出 13 条举措。

具体包括：（1）政策为 OpenClaw 用户提供全流程的免费部署实施与技能培训服务，鼓励市场化、专业化平台加入，对服务成效显著、符合认定条件的平台机构，给予最高 300 万元的专项补贴，让“上手”不再难。（2）常熟提供 OpenClaw 专属数据服务支持。面向符合条件的开发主体，免费开放经脱敏处理的政府公共服务数据资源，并全额减免相关公共数据使用费用。（3）常熟率先推出智能体安全与适配认证服务，支持平台公司为 OpenClawSkill 社区开发者提供全方位的安全认证及环境适配认证服务。根据年度认证服务规模与质量，给予服务提供商一定支持，确保技术应用安全可控。（4）常熟建立智能算力资源协调机制，为经认定的 OPC 社区新入驻的有关 OpenClaw 开发应用类企业提供算力资源补贴及相关基础技术支持服务。（5）依托人工智能专项基金，精准支持人才运用“OpenClaw”工具创办 OPC。鼓励各类资本进行长期战略投资，支持 OPC 全生命周期成长。（6）如果能在常熟市主办或承办的各级创新创业大赛等活动中获奖，符合条件的给予资金奖励，并可直接立项为市级“昆承英才”。（7）常熟聚焦具身智能、纺织服装、直播电商、文创设计等特色领域建设 OPC 社区，为大家搭建”朋友圈“，每年遴选具有产业引领的示范 OPC 社区，对建设运

营方给予最高 200 万元补贴。（8）常熟支持综合利用各类开源工具，面向工业检测、纺织服装等重点垂直领域开展工业大模型开发与攻关，对入选常熟市垂直领域模型的企业，给予资金支持。（9）常熟鼓励制造企业采购或利用 OpenClaw 等类智能体技术进行数字化改造与业务创新。对成功落地并服务于制造业企业的开发推广项目，按不超过项目总投入的 30%给予资金补贴，单家企业年度最高补贴 100 万元。（10）创业初期，30 天免费办公、住宿、餐饮，还有沪常通勤的“常来沪往”高铁补贴，让创业者轻装上阵、后顾无忧。（11）聚焦 OPC 全生命周期需求，提供全天候、全链条、全流程服务，实现线上一键呼叫、线下精准对接。（12）持 OPC 运用“OpenClaw”工具生产经营，对于入选各级人才计划的 OPC 项目，最高可给予 600 万元综合支持。（13）分层分类保障 OPC 人才多元安居需求，从每月最高 1500 元的租房补贴到最高 6 万元的一次性落户（租房）补贴和最高 200 万元的购房补贴，应有尽有。（来源：央视新闻）

5. 全国两会期间，多位代表、委员就 OpenClaw 发表看法

3 月 8 日，澎湃新闻发布消息，梳理两会期间多位代表、委员就 OpenClaw 发表的看法。

全国政协委员、360 集团创始人周鸿祎表示，“龙虾”是一个非常好的概念，把原来看不见摸不着的云上软件，变成了每个人在电脑里养的专属助手，而且操纵起来非常方便。他同时指出，“龙虾”现在还在早期，配置“龙

虾”对普通人来说是一件“非常难”的事。“我们很快会发一个一键安装的版本，让每个人养‘龙虾’都很方便。”

全国政协委员、中国工程院院士王坚 8 日在接受采访时表示，OpenClaw 会很快便宜下来并普及，任何行业内的人都不会没有看到它的存在。

3 月 7 日，在十四届全国人大四次会议广东代表团代表小组会议现场，全国人大代表、中国工程院院士、鹏城实验室主任高文在发言时也提及最近爆火的“养龙虾”。他表示，“昨天（6 日）晚上，马化腾说连他也没有想到，这个‘龙虾’会火到这种程度。”

“‘养龙虾’的走红并非孤立现象，智能工具正快速进入大众视野。”全国政协委员、中国科学院计算技术研究所研究员张云泉说，“这将对未来的工作方式乃至逻辑产生深远影响”。张云泉说，过去需要人工完成的简单重复任务，将逐步被智能体替代，人得以把更多精力投入创意设计、复杂决策等高价值工作。这也对从业者能力提出了更高要求。

张云泉表示，当前不少工业企业并非直接训练大型模型，而是开发各类智能体，逐步替代生产流程中可智能化的环节，推动流程再造。在个人应用领域，数字员工乃至“一人公司”（OPC）等新模式正迅猛发展。（来源：澎湃新闻）

6. 腾讯宣布启动“龙虾”全国免费安装计划

3 月 14 日，腾讯宣布“龙虾”全国免费安装计划，正式启动。未来 40 天，腾讯云 Lighthouse、ADP、WorkBuddy、QClaw、云安全、云存储等龙

虾产品的主理人和技术专家，将奔赴 17 个城市，与“爱虾人士”面对面交流。（来源：腾讯云）

境内前沿观察二：政策立法

导读：2 月，数据出境、数据要素流通利用、网络平台治理以及虚拟货币风险防范处置等议题成为部委和地方政策立法推进的重要方向。整体看，相关制度建设进一步从原则性要求转向场景化、分类化、标准化的细化规则，更加突出在重点行业、重点领域和重点平台中的落地实施。

部委层面，围绕汽车数据出境、数据流通服务、虚拟货币风险防范、网络平台未成年人保护等领域，相关部门密集出台政策文件，持续完善网络和数据安全治理框架。工业和信息化部等八部门印发《汽车数据出境安全指引（2026 版）》，聚焦研发设计、生产制造、驾驶自动化、软件升级服务等场景，明确汽车重要数据判定规则，进一步推动汽车数据出境管理规则细化。国家数据局等四部门发布《关于培育数据流通服务机构 加快推进数据要素市场化价值化的意见》，强调提升数据流通服务能力，支持面向人工智能发展的高质量数据集建设与流通交易，并将安全合规要求贯穿数据供给、流通和使用全过程。国家网信办等八部门印发《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》，进一步细化涉未成年人重点平台的认定标准和程序，为未成年人网络保护责任落实提供制度依据。八部门发布《关于进一步防范和处置虚拟货币等相关风险的通知》，明确虚拟货币不具有与法定货币等同的法律地位；比特币、以太币、泰达币等虚拟货币不具有法偿性，不应且不能作为货币在市场上流通使用。

地方层面，天津和重庆分别围绕数据出境负面清单管理和城市全域数字化转型作出制度部署。《中国（天津）自由贸易试验区数据出境负面清单管理办法（试行）》对负面清单制定、重要数据识别、业务场景分析等作出规定，体现出自贸试验区数据跨境流动管理向清单化、程序化方向推进。《重庆市推进城市全域数字化转型行动计划》围绕数字底座、智能中枢、数字法治和适数生态等方面提出系统性举措，既强调高质量数据集、大模型和智能体建设，也注重数字法治体系能力提升和地方标准、制度规则完善。

关键词：数据出境安全；数据要素流通利用；虚拟货币；网络平台

（三）部委层面动向

1. 工业和信息化部等八部门印发《汽车数据出境安全指引（2026版）》

1月30日，工业和信息化部、国家互联网信息办公室、国家发展和改革委员会等八部门印发《汽车数据出境安全指引（2026版）》。

《指引》所称汽车数据，是指汽车设计、生产、销售、使用、运维等过程中涉及的个人信息和重要数据；汽车数据处理者，是指汽车数据处理活动中自主决定处理目的和处理方式的组织、个人，包括汽车制造商、零部件和软件供应商、电信运营企业、自动驾驶服务商、平台运营企业、经销商、维修机构以及出行服务企业等。

《指引》提出汽车重要数据判定规则，涉及研发设计场景、生产制造场景、驾驶自动化场景、软件升级服务场景等。例如在研发设计场景，《指引》提出汽车数据处理者在整合全球研发资源、产品协同设计开发过程中，收集和产生的物料清单、研发设计文档、开发源代码数据，符合以下任意一项条件的，应当认定为重要数据：一是国家重大专项、国家重点研发计划支持的；二是符合《中国禁止出口限制出口技术目录》中相关技术控制要点的；三是涉及《中华人民共和国两用物项出口管制清单》中相关物项的。（来源：工业和信息化部）

2. 工业和信息化部等五部门办公厅发布《关于加强信息通信业能力建设 支撑低空基础设施发展的实施意见》

2 月 3 日，工业和信息化部办公厅、中央网络安全和信息化委员会办公室秘书局、中央空中交通管理委员会办公室综合局等五部门办公厅发布《关于加强信息通信业能力建设 支撑低空基础设施发展的实施意见》，提出探索构建多元探测协同服务能力、强化网络和数据安全保障等十项重点任务。

探索构建多元探测协同服务能力方面，《实施意见》提出，面向大型活动场所、军事设施、关键基础设施等重点区域感知监测和防护需求，在小范围区域探索部分频段通感融合技术应用，持续提升性能，同时进一步加强与雷达、光电感知系统、运行识别等技术的协同，根据用户需求，提升对低空航空器探测、识别和轨迹追踪能力。

强化网络和数据安全保障方面，《实施意见》提出，探索构建信息类基础设施网络和数据安全保障体系，落实网络安全等级保护、关键信息基础设施安全保护等制度要求，深化信息通信业网络安全防护管理，加强数据分类分级保护，推进网络和数据安全标准研制，开展监测预警、检测评估、应急处置等能力建设，推动相关企业落实安全主体责任。（来源：工业和信息化部）

3. 国家数据局等四部门发布《关于培育数据流通服务机构 加快推进数据要素市场化价值化的意见》

2 月 3 日，国家数据局、工业和信息化部、公安部、中国证监会发布《关于培育数据流通服务机构 加快推进数据要素市场化价值化的意见》，围绕明确功能定位、提升服务能力、强化实施保障三个方面提出十六项措施。

提升服务能力方面，《意见》提出，要拓展适应人工智能发展的高质量数据集流通交易方式。支持各类数据流通服务机构协同产业链链主企业等主体，面向服务人工智能发展建设高质量数据集。支持各类数据流通服务机构加强与人工智能企业等合作，依托数据基础设施提供数据汇聚、治理、模型训练等服务。

强化实施保障方面，《意见》提出，要强化数据安全保障。牢牢守住数据安全底线，把安全合规贯穿数据供给、流通、使用等全过程，在实践中细化落实数据流通安全治理规则，提升数据安全治理能力，促进数据安全合规高效流通利用。各类数据流通服务机构应落实数据安全相关法律法规要求，加强数据基础设施安全保护，提升数据安全保障效能。（来源：国家数据局）

4. 国家网信办等十一部门联合印发《关于提升境外人员入境数字化服务便利性的实施意见》

2 月 5 日，国家互联网信息办公室、国家发展和改革委员会、教育部等十一部门联合印发《关于提升境外人员入境数字化服务便利性的实施意见》，提出五方面十四条工作举措。

加强网络和数据安全保障方面，《实施意见》提出，一是要强化网络安全防护能力。加强关键信息基础设施安全保护。完善跨境支付、在线预约等境外人员高频使用场景的安全标准规范。深化拓展网络安全国际合作，依法防范和打击危害网络安全的各类违法犯罪活动，优化风险提醒和应急处理体系，防范跨境网络安全风险。

二是要提升数据安全与个人信息保护水平。加强数据分类分级保护，强化数据收集、存储、使用等全流程管理，防范身份证件、健康档案等敏感信息泄露滥用。持续健全完善数据跨境流动安全管理体系，积极参与数据跨境流动国际规则和标准的制定，强化数据出境安全监管技术能力建设和运用。（来源：国家网信办）

5. 中国人民银行等八部门发布《关于进一步防范和处置虚拟货币等相关风险的通知》

2 月 6 日，中国人民银行、国家发展和改革委员会、工业和信息化部等八部门发布《关于进一步防范和处置虚拟货币等相关风险的通知》，明确虚拟货币、现实世界资产代币化和相关业务活动本质属性，提出强化风险监测、防范与处置等要求。

《通知》指出，虚拟货币不具有与法定货币等同的法律地位。比特币、以太币、泰达币等虚拟货币具有非货币当局发行、使用加密技术及分布式账本或类似技术、以数字化形式存在等主要特点，不具有法偿性，不应且不能作为货币在市场上流通使用。挂钩法定货币的稳定币在流通使用中变相履行了法定货币的部分功能。未经相关部门依法依规同意，境内外任何单位和

个人不得在境外发行挂钩人民币的稳定币。现实世界资产代币化是指使用加密技术及分布式账本或类似技术，将资产的所有权、收益权等转化为代币（通证）或者具有代币（通证）特性的其他权益、债券凭证，并进行发行和交易的活动。

《通知》强调，虚拟货币相关业务活动属于非法金融活动。在境内开展法定货币与虚拟货币兑换业务、虚拟货币之间的兑换业务、作为中央对手方买卖虚拟货币、为虚拟货币交易提供信息中介和定价服务、代币发行融资以及虚拟货币相关金融产品交易等虚拟货币相关业务活动，涉嫌非法发售代币票券、擅自公开发行证券、非法经营证券期货业务、非法集资等非法金融活动，一律严格禁止，坚决依法取缔。境外单位和个人不得以任何形式非法向境内主体提供虚拟货币相关服务。此外，在境内开展现实世界资产代币化活动，以及提供有关中介、信息技术服务等，涉嫌非法发售代币票券、擅自公开发行证券、非法经营证券期货业务、非法集资等非法金融活动，应予以禁止；经业务主管部门依法依规同意，依托特定金融基础设施开展的相关业务活动除外。境外单位和个人不得以任何形式非法向境内主体提供现实世界资产代币化相关服务。（来源：国家发改委）

6. 全国网安标委发布《网络安全标准实践指南——互联网平台新型腐败预防和处置要求》

2 月 10 日，全国网络安全标准化技术委员会秘书处发布《网络安全标准实践指南——互联网平台新型腐败预防和处置要求》

《实践指南》规定了预防和处置互联网平台人员新型腐败的基本要求、日常防范要求和处置要求，适用于预防和处置互联网平台人员发生的流量操控、数据舞弊、权限寻租、榜单造假等新型腐败问题。

处置要求方面，《实践指南》将新型腐败行为按照事件危害对象（国家安全、公共利益、企业利益、个人利益）和危害程度（高、中、低）分为特别重大事件、重大事件、较大事件和一般事件。

针对较大事件和一般事件，经调查内部人员确有新型腐败行为，但未达到立案追诉标准的，互联网平台企业可以要求违规人员作出检讨并留存相关记录，并重新开展廉洁教育培训；扣减违规人员的绩效分数或绩效奖金等经济处罚措施；对违规人员进行警告、降职、撤职、解除劳动合同等相应处分等。

针对特别重大事件和重大事件，经调查内部人员新型腐败行为已达到立案追诉标准的，互联网平台企业应当采取暂停涉事人员职务及系统权限，保护现场证据；整理完整证据链（财务记录、系统日志、证人证词等），移交公安机关，并指定专人配合调查，定期跟踪案件进展等。（来源：全国网络安全标准化技术委员会）

7. 全国网安标委发布《数据安全技术 个人信息保护合规审计专业机构能力要求》等三项国家标准征求意见稿

2 月 11 日，全国网络安全标准化技术委员会秘书处发布三项国家标准《网络安全技术 网络空间安全可视化表示方法》《网络安全技术 可信计算

规范 服务器可信支撑平台》《数据安全技术 个人信息保护合规审计专业机构能力要求》征求意见稿。

《网络安全技术 网络空间安全可视化表示方法》给出网络空间安全可视化表示的原则、内容和方法，提供网络空间要素、网络空间关系、网络安全事件和网络安全业务的可视化表示框架，适用于网络运营者和网络服务提供者开展网络安全态势感知、威胁情报分析、事件响应等场景的可视化表示，以及网络安全综合防控体系建设等工作。

《网络安全技术 可信计算规范 服务器可信支撑平台》确立服务器可信支撑平台的总体框架，并规定服务器可信支撑平台的功能要求及其自身安全要求，适用于服务器可信支撑平台的设计、生产、集成、管理和测试。

《数据安全技术 个人信息保护合规审计专业机构能力要求》规定专业机构开展个人信息保护合规审计服务的能力要求，适用于指导与规范专业机构建设个人信息保护合规审计能力，还可为个人信息处理者自审计能力建设和选择合规审计专业机构提供参考。（来源：全国网络安全标准化技术委员会）

8. 国家网信办等八部门印发《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》

2 月 11 日，国家互联网信息办公室、国家新闻出版署、教育部等八部门印发《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》，自 2026 年 4 月 1 日起施行，包括认定标准、启动与自评估、论证与决定等内容。

《办法》提出，符合以下情形之一的，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：（1）该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；（2）该网络平台提供的产品或者服务的对象不局限于未成年人的，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。

《办法》强调，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，应当综合考虑以下因素：（1）该网络平台下载量、用户数量规模较大，或者网络产品的销售额、交易量等较大；（2）该网络平台未成年人登录频次、使用时长、使用偏好、消费金额等指标较高；（3）该网络平台涵盖大量涉及或者面向未成年人的信息内容；（4）该网络平台是涉未成年人相关垂直领域的代表性平台；（5）该网络平台在近3年内存在较多涉未成年人违法违规问题，产生较大负面影响；（6）其他对未成年人群体具有显著影响的因素。（来源：国家互联网信息办公室）

9. 国家网信办发布《政务移动互联网应用程序备案工作指南（第一版）》

2月28日，为指导和帮助各地区各部门做好政务移动互联网应用程序备案管理工作，国家网信办编制《政务移动互联网应用程序备案工作指南（第一版）》，对政务应用程序备案管理的方式、流程和材料等作出说明。

《指南》分别就备案申请、备案审核、备案变更、备案注销、发放编号等作出说明，并就备案工作中涉及工作环节发布了模板文件。政务应用程序

上线前，主办（使用）单位应根据《政务移动互联网应用程序规范化管理办法》，按照备案工作指南履行备案程序。（来源：国家互联网信息办公室）

（四）地方层面动向

1. 广东省人民政府办公厅发布《关于印发广东省加快数字社会高质量建设实施意见的通知》

1 月 23 日，广东省人民政府办公厅发布《关于印发广东省加快数字社会高质量建设实施意见的通知》，围绕创新场景应用、贯通组织单元、筑牢数智根基等五个方面，提出十八项建议。

创新场景应用方面，《通知》提出，提升精准韧性的数字治理能力。推进政府部门核心业务数据化，探索数据导向、智能辅助的精准施策和科学治理。推进“一表通”改革，深化“块数据”应用，推动多维度数据融通。探索韧性智治新模式，打造一批数字政府领域智能体应用，推进政法工作数字化平台建设，加强数智赋能应急安全保障。推进数字政府平台整合优化，建强“粤省事”平台超级入口。深化政务服务改革，推动政务服务由供给导向向需求导向转变，实现广东政务服务最好目标。

优化适数环境方面，《通知》提出，构建数字社会协同管理新规则。健全网络空间监管规则，探索构建覆盖人工智能研发、应用与伦理的监管框架，研究制定网络行为规范与算法治理规范。建立完善政府、行业组织、平台企业、消费者共同参与的协同治理机制，加强风险联合预警研判，构建全链条

全领域覆盖的新型监管执法体系。引导与促进行业协会依法自律、健康发展。（来源：广东省人民政府办公厅）

2. 天津市互联网信息办公室等四部门发布《中国（天津）自由贸易试验区数据出境负面清单管理办法（试行）》

2月2日，天津市互联网信息办公室、天津市数据局、天津市商务局等四部门发布《中国（天津）自由贸易试验区数据出境负面清单管理办法（试行）》，包括职责与分工、负面清单制定、负面清单实施等内容。《办法》规定，制定负面清单应当开展需求调研、重要数据识别、业务场景分析、征求意见与论证以及履行审批报备流程。

需求调研阶段，《办法》提出，聚焦天津自贸试验区产业发展和数据处理者实际需求，选取重点行业、领域组织开展调研，从业务场景、类别、量级、字段等方面摸排掌握数据出境情况，作为负面清单制定依据。

重要数据识别阶段，《办法》提出，在市数据安全工作协调机制的统筹协调下，市级行业主管部门、天津自贸试验区管委会依据《数据安全法》《网络数据安全管理条例》等法律、法规和规章的规定，组织数据处理者识别、申报重要数据，推动形成天津自贸试验区重要数据目录，并按程序报国家数据安全工作协调机制办公室备案。行业主管部门已公开发布或已在行业内部发布本行业、本领域数据分类分级标准规范的，优先按照其规定识别重要数据；行业主管部门未明确判定标准的，参照《中国（天津）自由贸易试验区企业数据分类分级标准规范》识别重要数据。

业务场景分析阶段,《办法》提出,结合调研情况及重要数据识别结果,选取数据出境需求迫切、行业特性强的业务场景,对数据出境的规模、范围和频率进行分析,为风险可控的数据出境业务场景合理设置数据项及数据量级。

征求意见与论证阶段,《办法》提出,征求市级行业主管部门、有关职能部门意见,必要时邀请行业、法律、数据安全等领域专家开展评审论证,对负面清单进一步修订完善。

履行审批报备流程阶段,《办法》提出,负面清单经市委网络安全和信息化委员会批准后,由市网信办、市数据局联合报国家网信部门、国家数据管理部门备案。(来源:天津市数据局)

3. 重庆市人民政府办公厅印发《重庆市推进城市全域数字化转型行动计划》

2 月 10 日,重庆市人民政府办公厅印发《重庆市推进城市全域数字化转型行动计划》,围绕数字底座能力提升行动、智能中枢能力提升行动等五项行动,提出三十二项措施。

数字底座能力提升行动方面,《行动计划》提出推进 AI 赋能。优化数字重庆人工智能底座,培育建设一批政府侧、行业侧高质量数据集。强化大模型和智能体“一本账”统筹管理,统一部署语言、视觉、多模态等通用大模型,迭代超大城市治理大模型,提速打造汽车行业等垂类大模型。培育 AI+市域开源生态,加快建设重庆人工智能学院、重庆通用人工智能研究院,

提速发展重庆人工智能湾区，引育一批AI企业，打造“模力高地”等创新孵化生态空间。

六大系统能力提升行动方面，《行动计划》提出全面构建数字法治系统体系能力。聚焦维护国家政治安全、确保社会大局稳定、促进社会公平正义、保障人民安居乐业等，持续优化完善数字法治系统五级核心业务体系。迭代情指行、全民反诈、重庆调解在线、“执法+监督”等数字化应用，加快构建数字法治系统五级联动业务承接体系。

适数生态能力提升行动方面，《行动计划》提出完善政策标准。贯彻落实国家标准，争取国家标准在重庆市试点。广泛参与城市全域数字化转型、数据基础设施、数据合规流通等领域标准研究工作。加快制定适数地方标准，深化数据“三权分置”、授权运营、开发利用、产权登记等基础制度建设，积极推进数字化地方立法工作。（来源：重庆市人民政府）

境内前沿观察三：治理实践

导读：2 月，公安机关、网信部门、通信管理部门等围绕算法治理、网络生态治理、网络安全、个人信息保护等领域持续发力，治理实践进一步向重点平台、重点应用、重点场景深化推进。

公安机关方面，全国打击治理电信网络诈骗工作视频会议召开，强调深化运用“四专两合力”总体思路，全面深化打防管控建宣各项工作，持续巩固扩大打击治理成果，推动反诈工作向更高水平纵深推进。国家网络与信息安全信息通报中心通报 72 款违法违规收集使用个人信息的移动应用，问题主要集中在隐私政策告知不充分、超范围收集个人信息等方面。上海公安侦破跨省游戏外挂黑灰产案件，依法打击“开发—销售”一体化作弊外挂犯罪链条；同时发布“涉企网络谣言”打击整治成果和典型案例，聚焦编造传播涉企虚假信息、损害企业声誉等问题。

网信部门方面，中央网信办围绕生活服务类平台召开《生活服务类平台算法负面清单（试行）》推进部署会议，强调聚焦算法黑箱、算法歧视、算法合谋等问题，推动重点平台抓紧整改落实。此外，启动“清朗·2026 年营造喜庆祥和春节网络环境”专项行动，聚焦“恶意挑动负面情绪”“生成数字泔水”“炮制传播不实信息”等方面。地方实践中，北京依法对快手平台未履行网络安全保护义务作出处罚，江苏发布网络执法典型案例，涉及未及时处置安全漏洞、网页篡改、数据泄露、超范围收集个人信息等问题。

通信管理部门方面，工信部通信管理局以及北京、安徽、广东、江苏等地通信管理部门继续开展侵害用户权益 APP（SDK）治理，重点聚焦违反必

要原则收集个人信息、未明示收集使用规则、逾期整改不到位等问题，并通过责令整改、公开通报、下架处置等方式强化移动互联网应用程序合规约束。

司法实践方面，最高人民法院发布第48批指导性案例，明确激活辅助驾驶功能情形下驾驶人仍是驾驶主体，不能因启用辅助驾驶系统而免除其安全驾驶义务；同时发布依法惩治电信网络诈骗等侵犯财产犯罪典型案例，对帮助信息网络犯罪活动罪中自愿补偿被害人损失情形的从宽处理规则作出进一步释明。

关键词：网络信息内容治理；个人信息保护；网络安全保护

（一）公安机关治理实践

1. 王小洪在全国打击治理电信网络诈骗工作视频会议上强调：全面深化打防管控建宣各项工作，奋力夺取反诈人民战争新胜利

2月5日，全国打击治理电信网络诈骗工作视频会议召开，中共中央书记处书记、国务委员王小洪出席并讲话。

王小洪强调，要深入贯彻落实习近平总书记重要指示精神和党中央、国务院决策部署，以对党和人民高度负责的态度，深化运用“四专两合力”总体思路，全面深化打防管控建宣各项工作，持续巩固扩大打击治理成果，奋力夺取反诈人民战争新胜利。

王小洪要求，坚持严打方针，盯着打、追着打、压着打，不断掀起打击高潮，决不给电信网络诈骗分子以喘息之机。坚持系统观念，紧盯涉诈人员、号卡、网络、渠道等，深化综合治理，努力实现标本兼治。坚持防范为先，精准开展预警劝阻，全面强化技术攻坚，广泛开展宣传教育，织密织牢防护网络，最大限度预防和减少案件发生。充分发动各方力量，整合各方资源，健全协作机制，不断推动打击治理工作走深走实。坚持主动作为，深化执法合作，全力挤压电信网络诈骗犯罪活动空间，同时为解决这一全球公害贡献中国智慧和中国方案。（来源：公安部网安局）

2. 国家网络与信息安全信息通报中心通报 72 款违法违规收集使用个人信息的移动应用

2 月 3 日，国家网络与信息安全信息通报中心发布通报，2025 年 12 月 26 日至 2026 年 1 月 20 日期间，经国家计算机病毒应急处理中心检测，72 款移动应用存在违法违规收集使用个人信息情况。

（1）17 款移动应用在 App 首次运行时未通过弹窗等明显方式提示用户阅读隐私政策等收集使用规则；以默认选择同意隐私政策等非明示方式征求用户同意；隐私政策难以访问；个人信息处理者在处理个人信息前，未以显著方式、清晰易懂的语言真实、准确、完整地向个人告知个人信息处理者的名称或者姓名、联系方式、个人信息的保存期限等，包括《UB+SEEK 无线音箱》（版本 1.8.1，华为应用市场）等。

（2）34 款移动应用隐私政策未逐一列出 App（包括委托的第三方或嵌入的第三方代码、插件）收集使用个人信息的目的、方式、范围等，包括《人工智能字幕翻译君》（版本 4.1.1，应用宝）等。

（3）17 款移动应用个人信息处理者向其他个人信息处理者提供其处理的个人信息的，未向个人告知接收方的名称或者姓名、联系方式、处理目的、处理方式和个人信息的种类，并取得个人的单独同意；App 客户端向第三方提供个人信息，未经用户同意，未做匿名化处理，包括《263 视频会议》（版本 V1.3.3，华为应用市场 IdeaHub 专区）等。

（4）5 款移动应用未在征得用户同意后才开始收集个人信息或打开可收集个人信息的权限；有提示收集规则，但用户点击拒绝后仍存在收集个人信息或打开可收集个人信息的权限，或频繁征求用户同意、干扰用户正常使用，包括《财富股研》（微信小程序）等。

（5）9 款移动应用未提供有效的更正、删除个人信息及注销用户账号功能；为更正、删除个人信息或注销用户账号设置不必要或不合理条件；虽提供了更正、删除个人信息及注销用户账号功能，但未及时响应用户相应操作，需人工处理的，未在承诺时限内完成核查和处理，包括《邦邻找房》（版本 6.0.8，豌豆荚）等。

（6）3 款移动应用投诉、举报未在承诺时限内受理并处理；个人信息处理者未建立便捷的个人行使权利的申请受理和处理机制，包括《笨嘴神器股票数据分析交流平台》（微信小程序）等。

（7）22 款移动应用未向用户提供撤回同意收集个人信息的途径、方式；个人信息处理者未提供便捷的撤回同意的方式，包括《K 米点歌助手》（微信小程序）等。

（8）2 款移动应用通过自动化决策方式向个人进行信息推送、商业营销，未同时提供不针对其个人特征的选项，或者未向个人提供便捷的拒绝方式；未以显著方式标示且未经用户同意，将收集到的用户搜索等个人信息，用于定向推送或广告精准营销，且未提供关闭该功能选项的行为，包括《河马智能回收》（微信小程序）等。

（9）4 款移动应用处理敏感个人信息未取得个人的单独同意；个人信息处理者处理敏感个人信息的，未向个人告知处理敏感个人信息

的必要性以及对个人权益的影响，包括《笨嘴神器股票数据分析交流平台》（微信小程序）等。

（10）6 款移动应用个人信息处理者处理不满十四周岁未成年人个人信息的，未制定专门的个人信息处理规则；收集未成年人信息未取得监护人单独同意，包括《大智慧》（版本 V1.10，华为应用市场 IdeaHub 专区）等。

（11）25 款移动应用未采取相应的加密、去标识化等安全技术措施，包括《人工智能字幕翻译君》（版本 4.1.1，应用宝）等。

（12）1 款移动应用《米加小镇世界》（版本 1.93，应用宝）在浏览同一页面、同一文档过程中，关闭后继续弹出广告，影响用户正常使用网络。

（13）3 款移动应用实现相同目的或者达到同等业务要求，存在其他非人脸识别技术方式的，将人脸识别技术作为唯一验证方式；个人不同意通过人脸信息进行身份验证的，未提供其他合理、便捷的方式，包括《牵手》（版本 2.11.93，抖音应用中心）等。

（14）4 款移动应用无隐私政策，包括《二房东》（百度小程序）等。（来源：公安部网安局）

3. 国家网络与信息安全信息通报中心通报重点防范境外恶意网址和恶意 IP

2 月 26 日，中国国家网络与信息安全信息通报中心通过支撑单位发现一批境外恶意网址和恶意 IP，境外黑客组织利用这些网址和

IP 持续对中国和其他国家发起网络攻击。这些恶意网址和 IP 都与特定木马程序或木马程序控制端密切关联，网络攻击类型包括建立僵尸网络、后门利用等，对中国国内联网单位和互联网用户构成重大威胁。相关恶意网址和恶意 IP 归属地主要涉及：美国、英国、意大利、捷克、斯洛伐克、沙特阿拉伯、立陶宛。

通报提出，应当采取以下排查方法：（1）详细查看分析浏览器记录以及网络设备中近期流量和 DNS 请求记录，查看是否有以上恶意地址连接记录，如有条件可提取源 IP、设备信息、连接时间等信息进行深入分析；（2）在本单位应用系统中部署网络流量检测设备进行流量数据分析，追踪与上述网址和 IP 发起通信的设备网上活动痕迹；（3）如果能够成功定位到遭受攻击的联网设备，可主动对这些设备进行勘验取证，进而组织技术分析。（来源：国家网络与信息安全信息通报中心）

4. 上海市公安局徐汇分局侦破一起跨省游戏外挂黑灰产案

2 月 27 日消息，上海市公安局徐汇分局近日侦破一起跨省游戏外挂黑灰产案件，打掉一个长期非法销售外挂的犯罪团伙。

2025 年 12 月，虹梅派出所接到辖区某游戏公司报案，某电商平台公然销售其旗下热门游戏的外挂。该游戏拥有上百万玩家。外挂严重破坏游戏平衡。经警方调查发现，该外挂程序有 14 种作弊功能。犯罪团伙通过玩家社群以“月卡”“年卡”等形式分层销售牟利。警

方锁定两名主要嫌疑人后，专案组民警分赴山东、广东两地同步开展收网将犯罪嫌疑人邝某、冯某抓获归案。

据开发者冯某交代，作弊外挂最初仅为自用。开发后，其见有利可图，便联系网店经营者邝某形成“开发—销售”一体化链条。截至案发，二人非法销售金额已超过120万元。目前，冯某、邝某因涉嫌破坏计算机信息系统罪已被采取刑事强制措施。案件正在进一步侦办中。（来源：警民直通车上海）

5. 上海公安网安部门发布“涉企网络谣言”打击整治成果和典型案例

2月28日，上海公安网安部门发布“涉企网络谣言”打击整治成果和典型案例。今年以来，上海公安依托“专业+机制+大数据”新型警务运行模式，深入开展涉企谣言打击整治专项行动。截至通报，警方查处涉企网络谣言案件23起，依法打击处理38人，累计清理涉企网络谣言信息3千余条，对210余个违规账号采取禁言、封停措施。同时发布三起典型案例。

典型案例一：近日，长宁公安分局破获一起造谣某知名茶饮品牌“涉毒”的案件。网民任某在参与某社交平台话题讨论的过程中，为博取眼球、吸引关注，谎称该品牌茶饮中含有的咖啡因系“准毒品”，该评论被大量转发，严重误导消费者。后相关专业部门辟谣，市场上咖啡因饮品有严格的添加剂标准。目前，犯罪嫌疑人任某已被依法采取刑事强制措施。

典型案例二：近期，网上出现某知名在线服务平台“卸载注销用户大幅攀升”“反垄断调查传闻提前泄密”等不实帖文，严重侵害企业声誉，导致客户流失，造成企业利益受损。经查，网民马某、刘某为蹭热点、吸粉引流，通过编造虚假信息等方式，在其个人自媒体账号上发布该企业“48小时内卸载量激增”“为应对反垄断调查连夜删信息”等不实情节，阅读量分别突破32万和40万。目前，犯罪嫌疑人马某、刘某已被依法采取刑事强制措施。

典型案例三：近期，网安部门在巡查中发现，有网民发布不实信息称，2026年3月1日起，浏览某知名网络平台的视频均需购买会员资格。经查，闫某为炫耀自身消息灵通，编造了关于观看该网络平台视频均需购买会员的不实信息，并在多个群组内扩散，一度登上网络热搜榜。目前，闫某已被杨浦警方依法处以行政拘留处罚。（来源：上海网警）

（二）网信部门治理实践

1. 中央网信办召开《生活服务类平台算法负面清单（试行）》推进部署会议

2月3日，中央网信办召开《生活服务类平台算法负面清单（试行）》推进部署会议。

会议强调，生活服务类平台通过为多方利益主体提供交易撮合、经营场所、信息交流，极大地降低交易成本，满足民生需求，同时也创造了新的就业岗位。算法作为平台生态系统中利益分配调整的主要

载体和重要枢纽，在智能匹配供需、改善用户体验、提高运营效率等方面发挥正向作用，但同时也存在算法黑箱、算法歧视、算法合谋等问题。

会议要求，要聚焦维护新就业群体和广大人民群众合法权益，推动《负面清单》落地见效。各生活服务类平台要成立由主要负责人牵头的专项工作组，抓紧制定工作方案，形成具体可操作的时间表和路线图。对可以马上调整的简单问题，在制定工作方案的同时就要同步优化调整，确保即时见效。对技术实现难度较大、涉及服务管理方式调整的复杂问题，在限定时间内完成优化调整。要自觉接受监督，把社会满意度作为衡量工作成效的标尺。网信部门要加强督查引导，及时跟进重点平台落实情况，并适时组织开展算法检查。对落实工作不扎实、不深入、走过场的，依法依规予以处置。各有关单位要按照“网下管什么，网上就要管什么”的要求，有针对性地推动《负面清单》在本行业领域落地实施。（来源：网信中国）

2. 中央网信办会同国家医保局整治涉药品、医用耗材集采网上虚假不实信息，通报部分典型案例

2 月 5 日消息，中央网信办近期会同国家医保局深入整治涉医药集中带量采购的网上虚假不实信息，依法依约处置一批污名集采、制造焦虑、误导公众的账号。其中，部分典型案例如下。

一是编造虚假信息，污名集采政策，博取流量。小红书账号“心血管 XXX 主任”“护帮 X 学长”，抖音账号“药圈 XX”“财可 XXX”

等，为吸引流量，编造集采药品、耗材质量不好的虚假信息，或将网络上搜集到的有关集采视频二次加工后发布，污名集采政策。涉及的账号已被依法依约采取处置措施。

二是煽动社会情绪，制造公众焦虑。微博账号“成都 XXX”，抖音账号“琼波 XX”“亮晶晶的 XX”等，歪曲国家政策，编造“进口药集体退出中国”等不实信息，煽动网民对原研药与仿制药的对立情绪，其中部分账号旨在制造公众用药焦虑，引导公众购买相关保健品、高端医疗保险，或诱导公众到特定的互联网平台购药。涉及的账号已被依法依约采取处置措施。

三是将非集采产品刻意与集采关联，误导公众。抖音账号“麻辣 XXX”“用笔在乐谱 XX”，小红书账号“Handsome 骨匠 XX”“biu 阿 X”，微博账号“边山半 XX”“小土豆 XX”等，为了吸引粉丝眼球、蹭集采流量，发帖称医用手套、输液袋、留置针等部分医疗器械质量差，实际反映的产品并非集采产品，破坏集采公信力。涉及的账号已被依法依约采取处置措施。（来源：网信中国）

3. 中央网信办启动“清朗·2026 年营造喜庆祥和春节网络环境”专项行动

2 月 12 日，中央网信办启动“清朗·2026 年营造喜庆祥和春节网络环境”专项行动。专项行动着力整治四方面突出问题：

（1）恶意挑动负面情绪。一是宣扬鼓吹不婚不育、反婚反育等不良价值观，挑动男女性别对立，渲染“婚姻恐惧”“生育焦虑”。

二是以“年货采购”“春节风俗比拼”等名义炫富斗富，恶意挑动攀比对立。三是借春节晚会、春节档影视作品、热门体育赛事等，组织参与网上“饭圈”活动，挑起拉踩互撕。

（2）生成传播“数字泔水”等垃圾信息。一是利用 AI 等新技术新应用批量生成逻辑混乱、信息空洞、高度雷同的低质内容。二是滥用 AI 技术对经典动画、影视作品等植入低俗暴力内容，进行戏谑恶搞。三是对文学名著、历史典故等进行“魔改”，歪曲解构优秀传统文化。四是批量炮制“父母偏心”“婆媳矛盾”“姐弟互殴”等渲染家庭矛盾、代际冲突文案和剧情，营销炒作博取流量。五是利用 AI 批量生成所谓“鸡汤网文”“霸总爽剧”“专家科普”等图文、短视频内容，影响网民认知判断。

（3）炮制传播不实信息。一是编造涉春运保障、节日市场供应、社会公共安全领域突发事件等方面谣言，伪造发布“春节政策”“事故通报”等权威公告，甚至传播所谓“阴谋论”。二是以“震惊”“惊爆”等耸人听闻的“标题党”，或者借同名同姓的“人名梗”吸引眼球，炮制与春节假期社会热点事件相关的谣言信息。三是假冒仿冒公众人物蹭炒热点发声，借机误导网民。

（4）为违法活动引流。一是进行赌球活动引流，以“赛事竞彩分析”“预测球赛结果”等为由，为赌球提供付费咨询。变相组织“新春线上棋牌游戏技巧”“家庭红包互动新玩法”等网络赌博活动。二是通过“同城交友”“过年搭子”等话题发布暗示性图文信息，进行

色情引流。三是打着改命转运、破除太岁等旗号，提供网上算命占卜服务，宣扬封建迷信。（来源：网信中国）

4. 中央网信办通报传播无 AI 标识的虚假不实信息典型案例

2 月 12 日，中央网信办通报传播无 AI 标识的虚假不实信息的典型案例。

微博账号“澄馫”、快手账号“玲子爱狗狗”、哔哩哔哩账号“空空说电影”等，发布狗在高铁站救下婴儿、狗拆炸弹救人、鳄鱼伤人等视频时，未添加 AI 生成标识，借虚构感人故事、猎奇事件恶意博取流量。相关账号已被依法依约处置。

微信账号“浮萍 9419”、微博账号“乘风已归来”、快手账号“东东情感”等，以 AI 换脸、声音克隆等方式，假冒运动员、演员、主持人、企业家等公众人物，发布不实言论，借此吸粉引流，或未经授权，售卖 AI 生成的公众人物“送祝福”“拜年”等视频，从中不当牟利。相关账号已被依法依约处置。

抖音账号“巷子里的鱼”“禾粟”、快手账号“朵姐正能量”“小猪猪”等，发布 AI 生成的虚假火灾现场图片、视频，恶意编造、炒作火灾事故，混淆视听，扰乱公共秩序。相关账号已被依法依约处置。

哔哩哔哩账号“真难我知道”、抖音账号“小奥特曼大智慧”、百度账号“清崽影视”等，借 AI 魔改未成年人喜爱的动画角色，制作刀切小马宝莉头部、奥特曼怀孕等视频，传播低俗惊悚、血腥暴力

内容，宣扬不良价值观，侵扰未成年人身心健康。相关账号已被依法依约处置。

小红书账号“浪淘达人”“南坤的店”等，发布“豆包图片去水印神器”等内容，分享去除 AI 标识教程、软件，淘宝、闲鱼、拼多多店铺“浙江智意 AI”“鼎建祥旗舰店”等，售卖去 AI 标识教程、软件及服务。相关账号已被依法依约处置，违规商品已下架。（来源：网信中国）

5. 中央网信办发布 2025 年全国网信系统执法情况

2 月 14 日，中央网信办发布 2025 年全国网信系统执法情况。2025 年，全国网信系统依法约谈网站平台 5811 家，警告 1646 次，对 521 家网站平台实施罚款处罚，责令暂停功能或更新 688 次，下架 App2133 款，下线小程序 192 款，会同电信主管部门注销网站、App 备案，以及关闭网站、App9637 家。督促网站平台落实主体责任，依法处置各类违法账号。

打击网络信息内容违法方面，全国网信系统聚焦打击侵害未成年人身心健康、网络暴力、扰乱传播秩序、破坏营商网络环境、污染网络生态等违法行为，集中整治涉企侵权信息、体育“饭圈”等网络乱象，加大对违法网站平台和网络账号处置处罚力度。

网络安全等领域违法行为查处方面，全国网信系统深入推进网络安全、数据安全、个人信息保护领域常态化执法，持续加大工作力度，形成有力震慑。

针对存在未履行网络安全、数据安全保护义务，未按照法律规定留存相关网络日志，未及时处置系统漏洞等安全风险，致使系统遭攻击篡改、数据泄露等违法问题的网站平台企业，国家网信办指导属地网信办依法采取责令改正、警告、罚款、处理责任人等处置处罚措施。

针对存在未公开个人信息收集使用规则、过度收集个人信息、违法出境个人信息等问题的部分 App 及企业单位，国家网信办指导属地网信办依法采取责令限期改正、下架下线、警告、罚款、处理责任人等处置处罚措施。

针对存在未有效落实人工智能合成内容标识规定要求问题的多款 App，国家网信办指导属地网信办依法采取约谈、责令限期改正、下架下线等处置措施。

针对存在未经安全评估即上线提供服务问题的一些具有舆论属性或动员能力的 App、小程序，国家网信办指导属地网信办依法采取责令改正、下架、下线功能、罚款、处理责任人等处置处罚措施。对已完成整改的 App 依法复核恢复上架，引导新技术新应用健康有序发展。

网络执法管理监督方面，国家网信办持续健全网络执法监督工作体系，开展日常监督、重点监督、专项监督等多种形式的监督，确保网络执法各项工作落实到位。严格落实网络执法人员培训、考试考核、资格管理和持证上岗制度。制定出台《网信部门行政处罚裁量权基准适用规定》，梳理发布《国家互联网信息办公室涉企行政检查事项清单》，进一步推进网络执法规范化、制度化、专业化建设。通过严格

规范公正文明网络执法，推进依法管网、依法办网、依法上网，推动互联网在法治轨道上健康运行。（来源：网信中国）

6. 因未履行网络安全保护义务，北京市互联网信息办公室对快手平台罚款 1.191 亿元

2 月 6 日消息，针对近期快手平台出现大量色情低俗内容直播问题，在国家互联网信息办公室指导下，北京市互联网信息办公室依法对北京快手科技有限公司涉嫌违法行为进行立案调查。

经查实，快手平台未履行网络安全保护义务，未及时处置系统漏洞等安全风险，未对用户发布的违法信息立即采取停止传输、消除等处置措施，情节严重，影响恶劣。北京市互联网信息办公室依据《网络安全法》《行政处罚法》等法律法规，对北京快手科技有限公司处警告、1.191 亿元人民币罚款处罚，同时责令其限期改正、依法依约处置账号、从严处理责任人。（来源：北京市网信办）

7. 重庆市网信办通报 2025 年网络执法情况

2 月 3 日，重庆市网信办通报 2025 年网络执法情况。2025 年，重庆市网信办依法查处网上各类违法违规行为。全市网信部门依法关闭违法违规网站 438 家、账号 261 个，对 153 家网站予以约谈，下架移动应用程序 46 款，暂停功能或更新网站 17 家，办理处置处罚案件 103 起。

依法查处违反网络信息内容安全的违法违规行为方面，重庆市网信办针对履行信息内容安全主体责任不到位，传播法律法规禁止传播的信息内容等违法违规行为，依法对“夺宝港网”“浮光点点”“凡人图书馆”等 8 家网站开展约谈警示，责令限期整改，并给予警告的行政处罚；针对违规从事互联网新闻信息服务、存在法律法规禁止发布或传播的信息等违法违规行为，依法对“时事经济观察网”“敲门砖网”“泽济人间”等 16 家网站采取关停措施；针对个别网站和 App 未经安全评估上线提供生成式人工智能服务，AI 对话功能中出现法律法规禁止传播的信息内容，依法对“美趣 AI”“欧亿 Ai-7.0”等 5 个网站平台采取下线 AI 产品、暂停功能等措施，并给予警告的行政处罚。

依法查处违反网络运行安全的违法违规行为方面，重庆市网信办针对网站运营主体未尽网络安全保护义务，致使所属网站被植入赌博、色情网页，依法对重庆某大数据科技有限公司、重庆某旅游开发公司等 16 个运营主体开展执法约谈，责令整改，给予警告的行政处罚；针对履行网络安全主体责任不到位，致使所属办公系统遭受攻击篡改，登录页面呈现法律法规禁止传播的信息内容，依法对重庆某文化传播公司、重庆某科技有限公司等 5 个运营主体给予警告、罚款的行政处罚；针对个别政务系统平台存在的弱口令、权限设置不合理，系统漏洞整改不到位等问题，依法对某县市政园林服务中心等 6 个运营主体开展执法约谈，责令全面整改，依法作出警告的行政处罚。

依法查处违反网络数据安全的违法违规行为方面，重庆市网信办针对未履行数据安全保护义务，致使所属数据库数据泄露等违法违规行为，依法对重庆某科技有限公司等3个运营主体给予责令整改、警告、罚款的行政处罚；针对未采取技术措施和其他必要措施保障数据安全，致使所属系统数据库被境外IP非法访问等违法违规行为，依法对重庆某科技股份有限公司等2个运营主体给予责令整改、罚款的行政处罚；针对未定期开展安全风险评估、未对系统漏洞等风险采取补救措施，致使所属办公系统数据被非法访问、传输等违法违规行为，依法对某县政府单位等2个运营主体给予责令整改、警告的行政处罚。

依法查处侵犯用户个人信息的违法违规行为方面，重庆市网信办针对违法违规收集、超范围收集用户个人信息等违法违规行为，依法对某生活服务重庆有限公司、重庆某置业有限公司、重庆某物业管理有限公司等6个运营主体分别作出责令改正、警告、罚款的行政处罚；针对未履行个人信息保护义务，未采取加密、去标识化等分级分类管理措施，存在敏感个人信息泄露风险，依法对某县人民医院、重庆某城市运营管理有限公司等3个运营主体分别作出责令整改、警告的行政处罚；针对未建立健全个人信息保护制度、未按法律规定提供删除或更正个人信息功能等问题，依法对重庆某科技有限责任公司等2个运营主体分别作出责令整改、警告的行政处罚。

依法查处违反网络生态相关规定的违法违规行为方面，重庆市网信办针对网站平台传播涉黄涉赌及低俗庸俗信息内容等违法违规行

为，依法对“美微网”“吾空网”“恋爱秘籍”“KOK 体育”等 230 余家网站平台采取下架产品、关闭等措施；针对假冒仿冒地方新闻单位和企事业单位名称，发布炒作引流信息等问题，依法关闭假冒仿冒的“渝北网”“重庆 1949”“重庆人才招聘网”等 21 个网站、账号，并对运营主体开展约谈，责令限期整改；针对部分自媒体恶意解读公共政策、蹭炒社会热点、编造散布谣言等违规行为，依法对“婷姐讲工程”“保函魏答答”“伟哥的哥”“驾质网”“侃见财经”“车曝台”等 121 个自媒体账号采取约谈、禁言、关闭等处置措施。（来源：网信重庆）

8. 上海市委网信办、市公安局网安总队联合开展“整治人工智能涉企虚假不实信息”专项行动

2 月 12 日，上海市委网信办会同市公安局网安总队宣布集中开展“整治人工智能涉企虚假不实信息”专项行动。

专项行动重点聚焦利用人工智能技术生成传播涉企虚假不实信息，误导公众认知、影响企业形象声誉、抹黑攻击竞争对手等问题，由上海市委网信办、上海市公安局网安总队联合推进，将加强典型案例打击处置，斩断利用人工智能技术不当牟利的利益链条，力争达到“标本兼治、打防结合、净化生态”的整治效果。

为建立健全长效机制，上海市委网信办将持续督促属地人工智能应用程序和传播平台切实履行主体责任，完善技术识别和人工复核机制，畅通用户投诉举报渠道，对利用人工智能生成“同质化”不实信

息、违规“养号”等行为强化审核处置；对人工智能批量制作、低质搬运、无来源虚构等“数字泔水”垃圾内容探索有效治理措施。（来源：上海网警）

9. 宁波网信部门依法查处一批违法违规房产类自媒体账号

2 月 27 日消息，浙江省宁波市多部门近日联合开展房地产领域自媒体专项整治，集中查处一批房产类自媒体违规账号，对账号持有人分级分类进行处罚处置。

经查，抖音“宁波**讲房”、抖音“宁波**砍房”、抖音“宁波***房产”等房产类自媒体账号，存在大量发布“以偏概全唱衰楼市”“歪曲解读房地产政策”“散播市场负面情绪”“恶语谩骂相关地域和人员”等违法违规信息的行为，同时还以“免费领取宁波购（买）房资料”为幌子，违反必要原则处理个人信息，且未采取个人信息保护措施。

上述行为违反《网络安全法》《个人信息保护法》《网络信息内容生态治理规定》等相关法律法规。宁波网信部门依法依规对相关自媒体账号持有人作出行政处罚，责令限期整改，并进行约谈、批评教育。（来源：网信浙江）

10. 江苏网信办发布 2025 年度网络执法典型案例

2 月 28 日，江苏省互联网信息办公室发布 2025 年度网络执法典型案例。

案例一：徐州某网络科技有限公司网页篡改案。网信部门工作发现，该企业提供售后服务的网站页面被篡改为违法有害内容。经查，该企业缺乏有效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，内部安全管理制度和操作规程不健全，未依法履行网络安全保护义务，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：常州某装备制造公司网页篡改案。网信部门工作发现，该企业的网络智能办公系统登录页面被篡改为违法有害内容。经查，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，未及时修复相关信息系统的漏洞，导致网页被篡改，植入违法有害内容，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。

案例三：镇江某科技股份有限公司网页篡改案。网信部门工作发现，该企业网站页面被篡改为违法有害内容。经查，该企业服务器存在任意文件上传漏洞，攻击者通过文件上传漏洞获取服务器权限，篡改 IIS 中间件的默认图片。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。属地网信部门已依法责令其改正，并予以警告、罚款处罚。

案例四：南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 超范围收集个人信息。经查，该公司运营的 APP 天气功能以“提供精准定位的天气服务”

为由索要位置权限，且在后台静默期间也调用用户位置信息，超范围获取个人信息。相关行为超出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》等法律法规规定。属地网信办已依法责令其改正，并予以警告处罚。

案例五：无锡市某科技公司存在数据泄露安全风险案。网信部门工作发现，该企业某系统相关数据存在泄露安全风险。经查，该企业涉事服务器存在接口逻辑漏洞，在进行涉敏感个人信息字段数据处理时未进行脱敏加密处理，未依法留存相关网络日志。该企业未依法履行网络安全、数据安全保护义务，违反《网络安全法》《数据安全法》《个人信息保护法》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：苏州某科技股份有限公司存在数据泄露安全风险案。网信部门工作发现，该企业服务器相关数据存在泄露安全风险。经查，该企业租用的服务器存在未授权访问漏洞，导致服务器内存储大量用户使用产品产生的数据信息存在泄露风险。该企业未依法履行网络安全、数据安全保护义务，未严格落实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》相关规定。属地网信办已依法责令其改正，并予以警告处罚。

案例七：淮安某单位未依法履行网络安全保护义务案。网信部门工作发现，该单位存在数据违规出境情况。经查，该单位防火墙、日志分析管理系统等网络安全设备网络会话日志缺失，机房管理混乱，

导致内部网络被作为数据违规出境的通道。该单位未依法履行网络安全保护义务，网络安全管理制度不完善，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。

案例八：泰州某公司网上商城数据被窃取案。网信部门工作发现，该企业电商平台的用户个人信息相关数据被窃取。经查，该企业网络安全管理制度不健全，运营的网上商城存在弱口令漏洞，未开启数据库日志记录功能，导致用户个人信息被窃取。该企业未依法履行网络安全、数据安全保护义务，涉事平台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，并予以罚款处罚。

案例九：镇江某信息科技有限公司运营的微信小程序违法违规收集个人信息案。网信部门工作发现，该企业运营的微信小程序存在违法违规收集个人信息等问题。经查，该企业存在未经学校允许，且在未明确告知的情况下收集学生的姓名、手机号、学号等个人信息问题，同时系统存在敏感数据泄露漏洞，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。属地网信和公安部门已依法责令其改正。

案例十：徐州某广告设计工作室网站深度合成服务未按规定进行安全评估。网信部门工作发现，该企业运营的微信公众号及小程序内，提供 AI 配音、声音克隆、AI 写作、AI 绘画等服务未按规定进行安全评估。相关服务未以显著方式告知技术支持者与使用者应承担的信息

安全义务，未设置便捷的用户申诉和公众投诉举报入口，在提供人声等生物识别信息编辑功能时，未依法提示使用者履行告知并取得被编辑者单独同意的义务，违反《互联网信息服务深度合成管理规定》等规定。属地网信办依法责令其整改。（来源：江苏省网信办）

（三）通信管理部门治理实践

1. 工信部通信管理局以及北京市、安徽省等地通信管理部门发布侵犯用户权益 APP（SDK）名单

（1）北京市

2 月 3 日，北京市通信管理局通报 2026 年第二期问题移动互联网应用程序。

通报指出，北京市通信管理局近日通过抽测发现北京市部分移动互联网应用程序存在“违反必要原则收集个人信息”“未明示收集使用个人信息的目的、方式和范围”等侵害用户权益和安全隐患类问题。截至通报，尚有 3 款移动互联网应用程序未整改或整改不到位，予以公开通报。

通报同时指出，2026 年 1 月 6 日，北京市通信管理局通报北京市部分存在侵害用户权益行为的移动互联网应用程序并要求整改。截至通报，仍有 4 款移动互联网应用程序未整改或整改不到位，予以全网下架处置。

（2）安徽省

2 月 3 日，安徽省通信管理局通报下架 4 款侵害用户权益 APP。通报指出，2025 年第 9 批次整改不到位的 APP 中，尚有 4 款 APP 逾期未完成整改。经研究，安徽省通信管理局决定下架上述 APP，相关应用商店应当立即对名单中的应用软件进行下架处理。

（3）广东省

2 月 3 日，广东省通信管理局通报下架 9 款 APP 以及 31 款未按要求完成整改 APP。

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，31 款 APP 未完成整改。被通报的 APP 主办者应在 2026 年 2 月 10 日前完成整改及反馈工作。

此外，通报强调，上次通报要求整改的 APP 中有 9 款 APP 未按照要求完成整改反馈，广东省通信管理局决定对上述 APP 予以下架。相关应用商店应立即组织对该 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。

（4）江苏省

2 月 26 日，江苏省通信管理局通报 2026 年第 1 批侵害用户权益行为的 APP。通报指出，江苏省通信管理局近日组织第三方检测机构对省内实用工具、本地生活等类型的 APP 进行检查，并通报相关单位限期整改。截至通报，尚有 22 款 APP 未完成整改。相关单位应当

于 3 月 10 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。（来源：北京市、安徽省、广东省、江苏省通信管理局）

（四）其他部门治理实践

1. 最高人民法院发布第 48 批指导性案例，明确激活辅助驾驶功能情形下驾驶人的刑事责任认定规则

2 月 13 日，最高人民法院发布第 48 批指导性案例，明确激活辅助驾驶功能情形下驾驶人的刑事责任认定规则。

在辅助驾驶技术应用日益广泛的背景下，有的驾驶人在激活辅助驾驶系统后不再专注驾驶，而是玩手机、睡觉等，有的驾驶人甚至购买、使用“智驾神器”等非法配件，逃避系统安全监测，长时间“脱手”驾驶，严重威胁道路交通安全。

指导性案例 271 号《王某群危险驾驶案》明确，车载辅助驾驶系统不能代替驾驶人成为驾驶主体，驾驶人激活车载辅助驾驶功能后，仍是实际执行驾驶任务的人，负有确保行车安全的责任。行为人激活辅助驾驶功能，并利用私自安装的配件逃避辅助驾驶系统监测的，即使其不在主驾驶位实际操控机动车，仍应作为驾驶主体承担相应法律责任。（来源：最高人民法院）

2. 最高人民法院发布依法惩治电信网络诈骗等侵犯财产犯罪典型案例

2 月 26 日，最高人民法院发布人民法院依法惩治电信网络诈骗等侵犯财产犯罪典型案例。其中，在被告人游某龙等 9 人帮助信息网络犯罪活动案中，人民法院依法从宽处理自愿补偿被骗人员损失的“两卡”犯罪人员。

该案中，2023 年 6 月，被告人游某龙等 9 人明知他人利用信息网络实施犯罪，仍向对方提供银行卡、手机及银行卡支付密码等，通过绑定或激活 POS 机等方式帮助转移资金，共查明诈骗资金 410 万余元，涉及被害人 80 名。

本案经四川省广元市利州区人民法院审理，现已发生法律效力。法院认为，被告人游某龙等 9 人明知他人利用信息网络实施犯罪，为其犯罪提供支付结算等帮助，情节严重，其行为均已构成帮助信息网络犯罪活动罪。游某龙等人分别有自首、坦白等情节，均认罪认罚，其中游某龙等 5 人主动退缴违法所得，由于诈骗分子未到案，赃款无法追回，游某龙等 7 人还主动向对应的被骗人员补偿了部分经济损失。游某龙等 3 人系初犯，悔罪表现较好，根据各被告人犯罪情节、社会危害结果，结合被告人自愿对被害人损失补偿比例的高低，依法判处各被告人一年六个月有期徒刑至三个月拘役不等刑罚，并处罚金，对游某龙等 3 人宣告缓刑。（来源：最高人民法院）

境内前沿观察四：人工智能安全专题

导读：2 月，我国人工智能政策立法推进重点进一步聚焦“人工智能+”场景落地、产业赋能、政务应用和治理能力建设。国家发展改革委等八部门印发《关于加快招标投标领域人工智能推广应用的实施意见》，围绕智能监管、数据治理等提出具体部署，推动人工智能在公共治理和监管执法场景中的应用深化。国务院围绕深化拓展“人工智能+”、全方位赋能千行百业开展专题学习，强调夯实技术底座、推进规模化商业化应用等，进一步释放政策层面对人工智能全链条突破和全场景落地的鲜明导向。

地方层面，深圳、黑龙江、海南、湖南等地围绕人工智能方面密集出台政策文件，持续拓展人工智能应用场景。《湖南省级人工智能终端产品认定管理办法（试行）》明确人工智能终端产品范围和认定规则。《深圳市“人工智能+”先进制造业行动计划（2026-2027 年）》提出支持具身智能、多模态大模型等技术研发，推动机器人在工业制造、仓储物流、港口园区等场景落地。黑龙江先后出台政务深化应用工作方案和深入实施“人工智能+”行动实施方案，围绕政务服务、行政执法等作出部署。《海南省推动“人工智能+”行动方案（2026—2028 年）》推动“人工智能+”与数字政府、行政执法监督、智慧社区等场景融合应用。

关键词：“人工智能+”；人工智能应用；人工智能终端产品

1. 国家发展改革委等八部门印发《关于加快招标投标领域人工智能推广应用的实施意见》

2月6日，国家发展和改革委员会、工业和信息化部、住房城乡建设部等八部门印发《关于加快招标投标领域人工智能推广应用的实施意见》，提出六个“人工智能+”应用场景及部署实施意见。

六大应用场景分别是“人工智能+”招标、投标、开标和评标、定标、现场管理及监管。其中，“人工智能+”监管方面，包括专家管理、围串标识别、信用管理、协同监管、投诉处理五项内容。例如协同监管部分，《实施意见》提出，要打造贯通项目标前、标中、标后的分析预警模型，加强全过程数据采集、治理和运用，通过数据碰撞和比对分析，自动识别应招未招、转包违法分包、人员违规变更、进度严重滞后、低中高结等问题。加强招标投标“行刑纪”贯通衔接，实现对问题线索预警转办、协同查处、结果反馈的智能化闭环管理，增强对复杂案件的深度解析与处理能力，推动形成行政执法、刑事司法、纪检监察“一网共治”的智慧监管格局。

部署实施意见方面，《实施意见》提出夯实数据基础。各地要加强招标投标数据治理，强化数据清洗和标注，加快构建涵盖招标投标政策法规和全流程各环节的高质量数据集和知识库，依托政务数据共享机制，推进高质量数据集的共建共享和生成数据的归集治理，更好支撑模型训练和应用。（来源：国务院）

2. 国务院以深化拓展“人工智能+”、全方位赋能千行百业为主题进行第十八次专题学习

2月11日，国务院以深化拓展“人工智能+”、全方位赋能千行百业为主题，进行第十八次专题学习。

李强指出，要深刻认识和把握人工智能发展态势，推动人工智能全链条突破、全场景落地，更大释放发展潜能。要持续夯实技术底座，推进算法创新，加大高质量数据供给，提升大模型性能，前瞻布局新技术新路径。要大力推进规模化商业化应用，促进人工智能终端和服务消费，建设人工智能应用中试基地，发展壮大智能体产业，拓展更多高价值应用场景。要加快培育产业生态，优化智算资源布局，加大数、算、电、网等资源协同，推进软硬件适配，形成产业链上下游贯通发展的格局。要积极推动开放合作，扩大国际技术交流和应用开发，构建开源技术体系和开源社区。要坚持统筹发展和安全，加强人工智能治理，完善相关法律法规、政策制度、应用规范、伦理准则，为人工智能应用筑牢安全保障。

李强强调，实施好“人工智能+”行动，需要充分激发全社会的活力和创造力。要构建开放包容的发展环境，支持企业锐意创新、积极探索，让新生事物在市场竞争中孕育壮大。要强化公共服务和要素保障，破除体制机制障碍，帮助企业解决实际困难。要加强人才培养使用，尤其要造就一批优秀的复合型人才，为推进“人工智能+”提供有力支撑。（来源：新华网）

3. 湖南省工业和信息化厅印发《湖南省级人工智能终端产品认定管理办法（试行）》

1 月 29 日，湖南省工业和信息化厅印发《湖南省级人工智能终端产品认定管理办法（试行）》，包括认定范围和认定条件、申报和认定程序等内容。

《办法》指出，人工智能终端产品是指嵌入人工智能技术，具备主动感知理解、多模态交互、智能化服务和自主学习进化等能力的产品或设备。湖南省级人工智能终端产品认定范围包括但不限于：智能机器人、智能计算终端、智能视觉终端、智能可穿戴设备、智能车载设备、智能仪器仪表、智能家居终端、智能无人飞行器、智能工业终端及其他新型人工智能终端。

《办法》明确，申报湖南省级人工智能终端产品应满足知识产权明晰、技术先进创新、质量安全可靠、市场前景良好的要求。其中，质量安全可靠方面，《办法》要求产品通过具备资质的检验检测机构的检测，符合国家及行业相关标准，并通过必要的安全认证。（来源：湖南省人民政府）

4. 深圳市工业和信息化局印发《深圳市“人工智能+”先进制造业行动计划（2026-2027 年）》

2 月 9 日，深圳市工业和信息化局印发《深圳市“人工智能+”先进制造业行动计划（2026-2027 年）》，围绕打造重点支撑平台、赋能重点产业集群、强化工作保障三个方面提出十三项措施。

赋能重点产业集群方面,《行动计划》提出人工智能赋能机器人。支持世界模型、视觉—触觉—语言—动作（VTLA）等多模态交互技术研发，构建具备交互、预测与决策功能的具身智能基座大模型及其训练、推理技术体系，培育长序列推理与自主学习能力，支撑跨场景任务高效处理。强化场景资源统筹，支持建设具身智能技术试验场，开放工业制造领域焊接、装配、喷涂、搬运等细分场景并实现落地应用，提升危险、恶劣环境下智能作业水平，推动机器人进工厂、进车间、进仓库、进港口、进园区。（来源：深圳市工业和信息化局）

5. 黑龙江省人民政府印发《黑龙江省“人工智能＋”政务深化应用工作方案》

（来源：黑龙江省人民政府）

6. 黑龙江省人民政府印发《黑龙江省深入实施“人工智能+”行动的实施方案》

2 月 14 日，黑龙江省人民政府印发《黑龙江省深入实施“人工智能+”行动的实施方案》，围绕实施“人工智能+”重点行动、强化基础支撑能力、优化产业发展环境三个方面提出二十三项措施。

实施“人工智能+”重点行动方面，《实施方案》提出“人工智能+”安全治理。推动人工智能赋能网络安全等重点领域。加快推动人工智能赋能网络空间治理，强化信息精准识别、态势主动研判、风险实时处置等能力。依托公安部行业大模型，聚焦执法办案核心场景，

持续研发和优化符合黑龙江省实战需求的垂直大模型和智能体。推进省公安视频图像综合应用平台智慧升级，加快无感采集与智慧采集网络协同布局，提升视频图像智能采集终端占比，助推公共安全治理模式向事前预防转型。

优化产业发展环境方面，《实施方案》提出提升安全能力水平。统筹高质量发展和高水平安全，推动模型算法、数据资源、基础设施、应用系统等安全能力建设。开展人工智能大模型应用质量评估、伦理对齐等方面评测，促进大模型应用安全合规发展。加强重要数据安全管理和个人信息保护，推动数据安全防护平台项目建设和储备，促进相关行业或区域内的数据安全治理监管能力提升。加强基础设施运维保障与安全监管。强化政府引导、行业自律，坚持包容审慎监管、分类分级，推进人工智能技术合规应用，指导企业依法依规逐级履行算法备案程序，落实国家在人工智能生成合成内容标识等方面监管要求。（来源：黑龙江省人民政府）

7. 海南省人民政府办公厅印发《海南省推动“人工智能+”行动方案（2026—2028 年）》

2 月 18 日，海南省人民政府办公厅印发《海南省推动“人工智能+”行动方案（2026—2028 年）》，围绕打造特色场景示范、推动重点行业应用两个方面，提出十一项“人工智能+”行动。

“人工智能+”数字政府行动方面，《方案》提出，推动海南省自然资源管理和国土空间规划“一张图”建设，不断夯实国土空间基

础数据底座，丰富应用场景，拓展平台功能；推进“人工智能+”机制创新，不断向农村三资、政府采购、三医联动、国资国企和审管法信等场景拓展，深化“监督一张网”建设，利用 AI 赋能事中事后监管；加快推进海南省数字资源“一本账”管理系统（DRS）能力提升项目实施；深化“海易办”平台功能，扩大 AI 智能审批、免申即享等服务范围；依托“海政通”平台强化政府内部协同效率，推广办文、办事、办会和基层“一表通”智能研判分析的辅助决策功能；推进“人工智能+”行政执法和行政执法监督场景建设，促进提升行政执法和行政执法监督效能；探索建设智慧社区，推广智能安防、智慧物业、独居老人关怀等应用场景。（来源：海南省人民政府）

境外前沿观察：月度速览十则

导读：2 月，境外各国及组织围绕网络安全、人工智能、供应链安全、关键基础设施防护等领域相继出台政策法律文件。

网络安全方面，法国发布《国家网络安全战略（2026—2030）》，从人才、韧性、威胁遏制、数字基础设施自主可控以及国际合作等方面系统部署未来网络安全建设重点；欧盟网络安全局正式发布《ENISA 国际战略》，通过与非欧盟国家、国际组织开展战略性国际合作，进一步提升欧盟内部网络安全水平。

人工智能方面，多家数据保护监管机构联合发布《关于人工智能生成图像与隐私保护的联合声明》，强调透明说明、安全防护等基本原则；印度新规正式生效，要求平台对人工智能生成或篡改内容进行显著标识，并部署核验机制以落实平台责任；美国法院则因律师提交人工智能生成的虚假判例作出制裁，进一步凸显生成式人工智能在法律专业场景中的核验义务与使用边界。

供应链安全和关键基础防护方面，欧盟委员会发布 ICT 供应链安全工具箱，围绕关键供应商评估、多供应商策略和降低高风险供应商依赖等提出风险缓释路径；美国 CISA 分别发布关于运营技术安全通信的指南和《2025 年度回顾》，反映出其持续强化关键基础设施防护、威胁拦截和应急演练能力建设。

关键词：网络安全；人工智能；供应链安全；关键基础设施防护

12. 全球多家机构共同发布《关于人工智能生成图像与隐私保护的联合声明》

2 月 23 日，加拿大、法国、德国以及中国香港等在内的全球 61 家数据保护监管机构共同发布《关于人工智能生成图像与隐私保护的联合声明》，回应当前社会对人工智能技术的普遍关切，即部分人工智能图像、视频生成系统，在未经当事人知情与同意的情况下，生成可识别特定个人的逼真图像及视频内容可能引发的严重隐私与安全风险。

声明强调，尽管不同地区的具体法律要求存在差异，但所有开发、使用人工智能内容生成系统的机构，均应遵循以下基本原则：（1）建立健全安全防护机制，严防个人信息被滥用，严禁生成非自愿私密影像及其他有害内容，尤其要强化对未成年人的保护；（2）确保信息公开透明，向社会清晰说明人工智能系统的功能、安全措施、合规使用范围及滥用后果；（3）建立便捷、有效的投诉与处理渠道，支持个人申请删除涉及自身信息的有害内容，并及时响应相关请求；（4）通过强化技术与管理防护，向未成年人、家长、监护人及教育工作者提供清晰、适龄的风险提示与指引，针对性防范儿童相关风险。（来源：欧盟数据保护委员会）

13. 法国发布《国家网络安全战略（2026-2030）》

1 月 29 日，法国政府发布《国家网络安全战略（2026—2030）》，旨在构建更加安全、自主且更具竞争力的国家网络体系。

战略围绕五大支柱展开：一是打造欧洲最大的网络安全人才储备。提出从青少年阶段加强网络安全职业引导，并加大对培训体系与人才吸引力建设的投入。法国将与私营部门紧密合作，配套推出人力资源政策，力争成为欧洲网络人才的重要培育基地；二是提升国家网络安全韧性。面对网络威胁向经济社会各领域渗透的态势，法国将推出网络安全提升计划，系统增强经济社会各层面的安全防护能力，并提升全社会应对网络攻击与危机处置的能力；三是遏制网络威胁蔓延。法国表示将动用各类手段遏制威胁扩散，显著提升潜在攻击者的经济、人力与声誉成本，对试图损害法国经济、破坏民主制度稳定、威胁境内人员与财产安全的行为形成有效震慑；四是掌握数字基础设施安全主导权。法国明确提出要降低关键技术对外依赖，保持在网络空间的独立判断与行动自由；五是推动欧洲及全球网络空间的安全与稳定。法国强调，国际合作是提升国家韧性、维护网络空间稳定的重要支撑，但当前合作环境面临多重挑战。在此背景下，法国将以坚守民主价值与法治精神、构建更具适应性的国际治理体系、坚持共识导向等原则，推动网络空间安全与稳定的国际合作进程。（来源：法国国防与国家安全总秘书处）

14. 欧盟网络安全局发布国际战略，以国际合作提升欧盟网络安全水平

2 月 9 日，欧盟网络安全局（ENISA）正式发布《ENISA 国际战略》，旨在通过与非欧盟国家、国际组织开展战略性国际合作，进一步提升欧盟内部网络安全水平，同时助力欧盟在全球网络安全领域的合作与发展。

战略明确三类差异化国际合作模式，按资源投入力度分为：有限参与、协助支持和主动拓展。战略指出，鉴于网络安全形势与国际环境的快速演变，ENISA 必须具备敏捷反应能力，及时采取行动，并始终以下列原则为指引，规范其所有国际事务：（1）ENISA 的国际合作重点面向与欧盟具有战略关系且共享欧盟价值观的国际主体；（2）若国际主体的合作可能损害欧盟利益或政策目标，ENISA 应避免与之接触；（3）ENISA 的国际合作旨在为欧盟成员国和欧盟的伙伴关系增添价值；（4）当欧盟与国际主体签署的协议明确要求网络安全合作时，ENISA 应在协议条款及合作模式范围内，以主动外联方式推进相关工作等。

战略划定了网络安全合作重点与优先领域，主要包括：（1）持续关注与优先领域。ENISA 将持续推进与乌克兰、美国的合作协议落地，根据网络安全实际需求调整合作内容，聚焦能力建设、最佳实践与信息知识共享；持续为欧盟与英国、北约等的网络安全对话提供支撑，并为欧盟参与 G7 网络安全工作组工作提供欧盟层面的专业技术支持；（2）新的关注与优先领域。2026 年起将为西巴尔干地区欧盟

候选国提供网络安全能力建设支持，同时推动数字欧洲计划关联第三国的欧盟网络安全储备机制落地，负责该机制的评估、管理与运营工作，此外还将在合规前提下探索与更多理念相近国际伙伴的网络安全合作。（来源：欧盟网络安全局）

15. 美国 CISA 发布指南，帮助关键基础设施用户采用更安全的通信方式

2 月 10 日，美国网络安全和基础设施安全局（CISA）发布《安全运营技术通信的障碍：为何约翰尼无法完成身份验证》指南，帮助运营技术（OT）所有者与运营商实施安全通信，并为 OT 制造商提供克服安全通信落地障碍、提升产品可用性的建议。指南内容基于对多个行业控制系统利益相关方、资产所有者及运营商的访谈，涵盖水务与污水处理系统、交通系统、化工、能源以及食品与农业等领域。

指南深入剖析了安全通信未能普及的原因，并为 OT 所有者、运营商及制造商提供了可操作的行动建议，以克服以下关键障碍：（1）采购、部署与维护环节的成本与复杂性问题；（2）延迟与带宽顾虑；（3）加密导致的检查难题；（4）互操作性及遗留产品问题。资产所有者与集成商可依据本指南避免安全通信引发的运行中断，并明确采购新组件时的优先事项。（来源：美国网络安全和基础设施安全局）

16. 美国 CISA 发布《2025 年度回顾》，在关键基础设施领域拦截 3.71 亿次攻击

2 月 11 日，美国网络安全和基础设施安全局（CISA）发布《2025 年度回顾》，重点介绍 CISA 2025 年在加强国家网络与实体安全方面取得的显著成就，为保护国家关键基础设施提供了有力支撑。

2025 年 CISA 取得了诸多重要成果，主要包括：（1）强化协同防御能力。通过 CISA 的全天候运营中心发布 1600 余份安全通告，处置 30000 多起安全事件，有力维护关键系统安全；（2）构建威胁拦截网络。成功阻断针对联邦民用网络的 26.2 亿次恶意连接企图，并在关键基础设施领域拦截 3.71 亿次攻击；（3）全域备战能力提升。牵头开展 148 场网络与实体安全演练，吸引超万名参与者，助力各级组织完善应急预案并增强国家韧性等。（来源：美国网络安全和基础设施安全局）

17. 欧盟委员会发布 ICT 供应链安全工具箱

2 月 13 日，欧盟推出全新的信息通信技术（ICT）供应链安全工具包，为欧盟提供一套识别、评估和降低整个 ICT 供应链网络安全风险的方法。该工具包由欧盟成员国、欧盟委员会以及欧盟网络安全局（ENISA）组成的 NIS 2 指令合作小组开发，并将在一年后对其进展情况进行审查。该工具包详细列出风险场景，并推荐相应的缓解措施，其中包括对关键供应商的评估、采用多供应商策略的重要性，以及如何减少对高风险供应商的依赖等方法。（来源：欧盟委员会）

18. 印度政府新规生效，加强人工智能生成内容及深度伪造管控

2 月 20 日，印度政府新修订的《信息技术（中介机构准则与数字媒体道德规范）规则》生效，旨在遏制人工智能与深度伪造技术的网络滥用，并推动平台对有害或误导性内容采取更快速行动。

新规要求平台必须确保所有使用人工智能工具生成的内容获得清晰显著的标注，同时要求用户声明其上传内容是否经过人工智能生成或修改。新规指出，社交媒体平台需确保向用户明确披露人工智能生成或篡改的内容。政府同时强制要求社交媒体平台部署工具与验证机制以核验用户声明，若人工智能生成内容未按规定披露，平台将承担相应责任。

印度政府表示，只要中介机构遵循新规要求，其依据《信息技术法》享有的“避风港原则”保护权不受影响。该条款意味着平台不对第三方发布的内容承担法律责任，前提是履行了法定审核义务。（来源：印度电子与信息技术部）

19. 因个人信息泄露，韩国 PIPC 对 Tmoney 处以 5.34 亿韩元罚款

1 月 29 日消息，韩国个人信息保护委员会（PIPC）近日宣布，因个人信息泄露，对交通支付服务运营商 Tmoney 公司处以总计 5.34 亿韩元罚款，并责令其整改相关违法行为。

PIPC 表示，本案调查始于 2025 年 4 月 11 日的一起个人信息泄露报告。经调查确认，2025 年 3 月 13 日至 25 日期间，一名黑客采用所谓“凭证填充攻击”手段入侵“Tmoney Card & Pay”网站并获取用户账户访问权限，导致 51691 名用户的个人信息遭到泄露。PIPC 认定，Tmoney 在运营“Tmoney Card & Pay”网站过程中未能履行《个人信息保护法》规定的安全保护义务，导致大规模个人信息泄露事件发生。因此，PIPC 决定对该公司处以罚款并下达整改命令。

PIPC 同时指出，近年来“凭证填充攻击”呈现明显增多趋势，相关机构和企业应当对异常访问行为加强监测和防护，包括完善异常登录检测与阻断机制，并建立针对可疑行为的快速响应措施。（来源：The financial news）

20. 欧盟委员会就中央移动基础设施遭网络攻击事件作出回应

1 月 30 日，欧盟委员会负责管理移动设备的中央基础设施发现网络攻击痕迹，可能导致部分工作人员的姓名和手机号码泄露。委员会迅速采取应对措施，事件在 9 小时内得到控制，并完成系统清理，未检测到移动设备遭受入侵。

2 月 6 日，欧盟委员会作出回应，高度重视其内部系统和数据的安全性与抗风险能力，并将持续监测事态发展。委员会将采取一切必要措施确保系统安全，对此事件进行全面复盘审查，并为持续增强网络安全防护能力提供依据。面对欧洲关键服务和民主机构每日遭遇的

网络攻击及混合攻击，欧盟委员会承诺将进一步强化欧盟网络安全防御体系和应对能力。（来源：欧盟委员会）

21. 因提供人工智能生成虚假判例，美国第十巡回上诉法院对一律师罚款 1000 美元

2 月 10 日，美国第十巡回上诉法院对马里兰州律师库斯敏 •L •阿马尔辛格作出制裁决定：因其在上诉简报中使用生成式人工智能 ChatGPT 起草并引用了多条虚构判例，法院对其罚款 1000 美元，同时驳回其上诉请求，并将相关命令与判决副本移送至其执业地马里兰州的律师纪律监管部门。

承办法官哈里斯 • L • 哈茨在未公开的裁决意见中指出，阿马尔辛格的上诉简报存在“严重缺陷”，主要问题是依赖 ChatGPT 生成多个并不存在的案例引用，并且对真实案例的命题与引文也出现错误归属。法院在发现问题后要求其解释并更正，阿马尔辛格承认使用 ChatGPT 辅助研究与起草，且该工具生成了七条捏造的判例引用。

法院强调，适用《联邦上诉程序规则》第三十八条进行制裁时，关键不在于律师是否主观恶意，而在于其行为是否客观上构成对法庭义务的“故意或鲁莽漠视”。法院认定阿马尔辛格的行为属于“鲁莽”，因为其未履行律师最基本的核验职责——确认所引案例真实存在、确能支持主张，并准确引用权威资料。尽管其表示无意歪曲法律或案卷记录，承诺避免重犯，并已完成关于人工智能使用伦理的继续法律教

育课程，法院仍认为应予以制裁，但也对其坦诚与改进意愿表示认可。

（来源：Bloomberg Law）

行业前沿观察：各地协会动态

导读：各地协会活动精彩纷呈，举办高级研修班、研讨会、考察活动，举行主题党日、论坛活动等。北京网络空间安全协会举办网络安全领域职称评审与科学技术奖申报咨询会；广东省网络空间安全协会举办广东省信创适配测试工作座谈会；海南省网络安全和信息化协会举办“破界出海·全域增长”联合主题党日暨技术交流沙龙活动；清远市网络文化协会举办民主评议党员暨组织生活会；南宁市信息网络安全协会开展走访交流；沈阳市网络安全协会举办“凝聚监督合力·优化营商环境 ——‘沈警综合工作站’网络安全专题宣讲”活动；

关键词：咨询会、座谈会、沙龙、走访交流

1.北京网络空间安全协会举办网络安全领域职称评审与科学技术奖申报咨询会

2 月 4 日，北京网络空间安全协会举办的线下申报咨询会圆满落幕，三十多名会员单位员工和个人会员齐聚协会报告厅参与活动，最终都带着满满的收获返程。现场答疑环节气氛热烈，学员踊跃发问，主讲人逐一细致回应，有效解决了学员的申报中的困惑。两类课程各有侧重、相互补充，全面覆盖申报全流程关键节点。

2.广东省网络空间安全协会举办广东省信创适配测试工作座谈会

2 月 11 日，广东省信创适配测试工作座谈会在广东省网络空间安全协会多媒体室成功召开。协会相关代表及全省多家信创适配测试中心负责人、业务骨干齐聚一堂，围绕信创适配测试工作进展、现存问题展开深度交流，共商行业未来发展路径与合作机制，为广东省信创产业高质量发展凝聚协同力量。

3.海南省网络安全和信息化协会举办“破界出海 ·全域增长”联合主题党日暨技术交流沙龙活动

为深入探索党建引领与业务发展协同共进的新模式，近日，海南省网信协会党支部与优米出海（海南）科技有限公司在海口招商局大厦举办“破界出海 • 全域增长”联合主题党日暨技术交流沙龙活动。活动将党建工作与业务研讨有机融合，组织协会海南正邦、神州希望、世纪网安等会员单位党员代表、协会专家与有关企业家共同围绕自贸

港政策与技术出海实践等议题展开深度对话，旨在以组织优势凝聚发展共识，以技术交流激发创新动能。

4.清远市网络文化协会举办民主评议党员暨组织生活会

2 月 27 日下午，清远市网络文化协会党支部在清远市青果传媒有限公司会议室召开民主评议党员暨组织生活会。清远市互联网行业党委专职副书记郑福志列席指导，会议由支部书记陈志龙主持，支部全体党员参会。全体党员首先以书面形式集中学习习近平总书记关于党的建设的重要思想。随后，支部书记通报会前筹备情况，并代表支部作对照检查。会上，全体党员逐一开展批评与自我批评，直面问题、坦诚交流。会议还开展民主评议党员工作，参会人员认真填写测评票并提出初步评定意见。

5.南宁市信息网络安全协会赴广西互联网协会开展走访交流

为进一步加强行业协作，凝聚网络安全发展合力，近日，南宁市信息网络安全协会秘书长何毅一行赴广西互联网协会开展走访交流。双方围绕网络安全新趋势、新挑战及未来合作方向进行了深入探讨，并共同展望了 2026 年网络安全工作的协同路径。

6.沈阳市网络安全协会举办“凝聚监督合力·优化营商环境——‘沈警综合工作站’网络安全专题宣讲”活动

2 月 4 日，沈阳市工商联会同沈阳市公安局网安支队、沈阳市网络安全协会，成功举办“凝聚监督合力·优化营商环境 ——‘沈警综

合工作站'网络安全专题宣讲”活动，政企校多方齐聚一堂，共话高校网络安全防护新路径，共谋沈阳市营商环境优化新篇章。市工商联法律服务部部长王威，市公安局网安支队安全监管大队安全监察中队中队长汪猛，沈阳市众多高校网络保障中心负责人、网络安全企业代表参加活动。