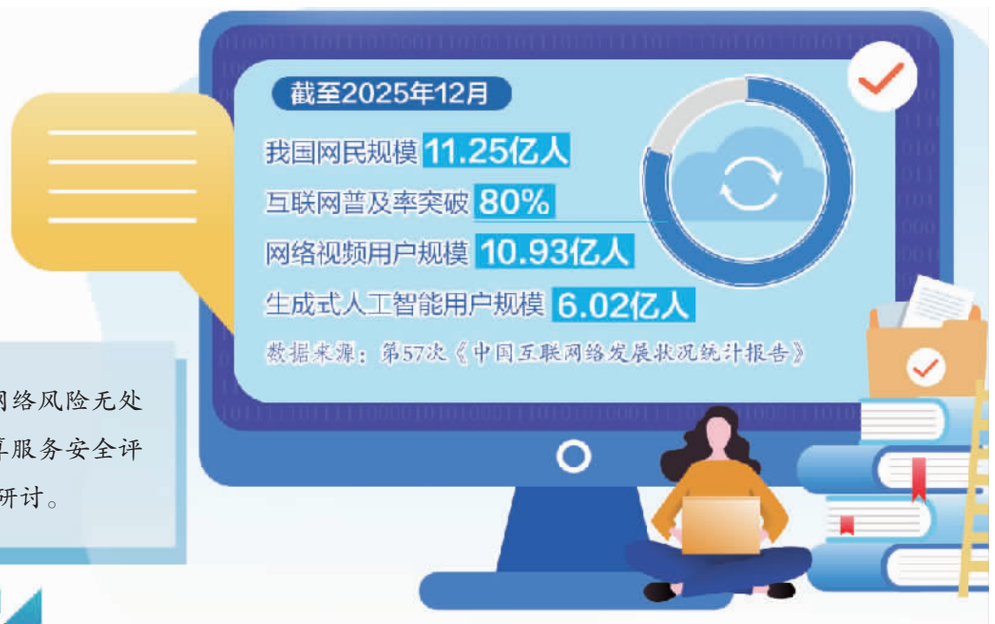
智库圆桌（第29期·总389期）

提升网络安全保障能力

网络安全事关国家安全和社会稳定，直接关系每一位网民的切身利益。从个人隐私泄露到网络诈骗，从数据丢失到系统瘫痪，网络风险无处不在。“十五五”规划纲要围绕“提升网络安全保障能力”作出具体部署，提出“健全关键信息基础设施安全防护、网络安全审查、云计算服务安全评估等基础制度，完善互联网内容管理、网络平台治理等法规”。如何不断筑牢防线、守护网络安全？本期特邀专家围绕相关问题进行研讨。



强化关键信息基础设施安全防护

为什么要推进关键信息基础设施安全防护？其他国家和地区采取了哪些举措？

王超（中国电子信息产业发展研究院网络安全研究所副所长）：网络安全牵一发而动全身，没有网络安全就没有国家安全。金融、能源、电力、通信、交通等领域的关键信息基础设施是经济社会运行的神经中枢，是网络安全的重中之重，也是可能遭到重点攻击的目标。当前，境外高级持续性威胁（APT）组织、国家级黑客力量频繁对我国发起攻击，攻击目标向金融、能源、交通等关键信息基础设施全面拓展，攻击手法持续升级，危害程度不断加深。据国家互联网应急中心监测发现，2024年境外国家级APT组织对我重要单位实施网络攻击事件超600起，涉及多家党政机关、高校和科研院所、重要行业企事业单位等。重大活动期间境外机构对我国关键信息基础设施攻击高发。中国国家计算机病毒应急处理中心监测数据显示，2025年哈尔滨亚洲冬季运动会期间，赛事信息系统遭境外网络攻击超27万次。

我国重点行业领域关键信息基础设施面临网络安全严峻挑战。如，在能源领域，针对性攻击呈现系统性、长期性特征。2025年，国家互联网应急中心发布调查报告，公布美国对我国某智慧能源和数字信息大型高科技企业的网络攻击详情，攻击者利用微软邮件服务器漏洞入侵，植入仅运行在内存中的隐蔽木马，以邮件服务器为跳板对内网重要设备发起攻击，窃取核心网络设备账号及配置信息、项目管理文件和敏感邮件数据。又如，在交通领域，智能网联技术发展推高安全风险。当前，智能网联技术与交通领域深度融合，在提升出行效率、保障交通安全及优化能源利用等方面发挥着重要作用，同时也不可避免扩大了网络威胁攻击面。如果存在安全漏洞，黑客便能追踪公交实时位置，对门控、发动机启动、空调乃至刹车系统发出远程指令。

世界各国高度重视关键信息基础设施安全，美欧等通过立法或发布政策文件将关键基础设施的网络安全保护提升到国家安全战略层面，主要采取了以下举措加强关键信息基础设施安全防护。

一是界定关键信息基础设施安全防护的对象范围。关键信息基础设施的概念是从关键基础设施发展而来，国际上对于关键基础设施的范围界定逐渐趋同。2023年，欧盟将关键基础设施的认定范围扩大到能源、交通、金融、医疗、饮用水、数字基础设施、太空、食品、制造等18个行业。2024年，美国白宫发布《关于关键基础设施安全和弹性的国家安全备忘录》，进一步明确美国关键基础设施行业及其对应的部门风险管理机构，涵盖通信、制造、能源、金融、化工、交通等16个关键基础设施行业。

二是建立关键信息基础设施安全防护的组织管理体系。关键信息基础设施保护涉及不同的行业和部门，需要充分调动利益相关方的积极性，明确管理组织机构及其责任。美国采取“政府—企业动态联盟”的分散式治理模式，由国土安全部下属的网络安全和基础设施安全局统筹负责，微软、谷歌等科技巨头深度参与政策制定。欧盟采取“超国家+国家”双层治理架构，欧盟网络安全局负责技术指导、政策协调和能力评估，各成员国配备计算机安全事件响应小组、主管国家网络和信息系统机构，加强所有成员国之间的合作，支持和促进成员国之间的战略合作和信息交流。

三是明确关键信息基础设施安全防护的标准要求。美国商务部国家标准与技术研究院发布《提升关键基础设施网络安全的框架》，其框架包括识别、保护、检测、响应和恢复5个部分。欧盟立法通过《关于在整个欧盟实现高度统一网络安全措施的指令》，涵盖治理、技术与运营层面，包括风险分析与信息安全政策、事件处理与响应机制、业务连续性与灾难恢复、供应链安全管理、安全开发与漏洞披露、有效性评估机制、网络卫生与安全培训、加密与密码管理、人员与访问控制策略、多因素认证与安全通信等内容。

关键信息基础设施是国家重要的战略资源，具有基础性、支撑性、全局性作用，保护关键信息基础设施安全是国家网络安全工作的重要内容。要深刻认识关键信息基础设施安全防护工作的重要性，严格落实安全主体责任，扎实做好网络安全威胁监测与处置、网络安全审查等相关工作。汇聚全社会力量开展网络安全关键技术攻关，积极利用云计算、大数据、人工智能等技术提升态势感知、漏洞挖掘等技术支撑手段，强化网络安全保障能力。常态化开展场景式、专题化、联合型关键信息基础设施安全应急演练，全面提升网络与数据安全防护和应急处置能力。

规范AI内容标识引导智能向善

当前，网络诈骗手法不断翻新，对人工智能生成合成内容，如何整治乱象、规范使用？

郝春亮（中国电子技术标准化研究院网络安全研究中心人工智能安全部主任）：当前，人工智能产业已步入快速增长阶段，2025年我国人工智能核心产业规模超过1.2万亿元，企业数量超过6200家，应用场景持续拓宽，展现出蓬勃的创新活力与广阔的应用前景。人工智能技术在赋能经济社会发展的同时，也带来了新的风险挑战。2025年第一季度，全国AI换脸、拟声诈骗案件数量环比激增高达45%。在人工智能深度融入社会运行的当下，网络空间的安全挑战正从传统的代码对抗升级为新型的智能化、算法化博弈。如何在促进创新发展与防范安全风险之间取得平衡，成为人工智能时代提升网络安全保障能力必须回答的问题。

以人工智能生成合成内容为例，近年来，随着生成合成技术的迅猛发展，普通公众有时难以分辨接收到的网络内容是由真实世界产生的还是由人工智能生成合成的。同时，诈骗手段从传统电信诈骗演化为换脸换声等新型模式，利用大模型技术制作虚假音视频，当“眼见”不再“为实”，网络空间生态面临极大挑战。

针对这一难题，我国已探索形成显隐双轨的人工智能生成合成内容标识技术方案。显式标识面向公众，重点解决“看得见”的问题。文字内容可以在起始、末尾或适当位置添加提示，音频可以通过语音提示或节奏提示，图片、视频、虚拟场景可以通过显著角标、画面提示、播放周边提示等方式降低公众混淆误认风险。隐式标识面向机器识别和责任追溯，重点解决“查得到”的问题，通过文件元数据记录生成合成属性、服务提供者名称或编码、内容编号等制作要素，在传播环节，还可写入传播平台名称或编码、内容编号等传播要素。显式标识保护公众知情权，隐式标识支撑平台治理，两者共同构成AI内容治理的基础坐标系。

当前，我国已构建起技管结合、逐层细化的人工智能生成合成内容标识制度体系，即“一部规范性文件、一项强制性国家标准、一套实践指南”的“1+1+N”标识体系。

第一个“1”是国家网信办、工信部等部门印发的《人工智能生成合成内容标识办法》（以下简称《标识办法》），从管理层面提出要求，明确生成合成内容制作传播各主体的责任义务，推动由生成合成到传播各环节的全流程安全管理，把“看得见的提醒”和“查得到的来源”结合起来，使普通用户获得辨别提示，使平台和部门具备核验、处置和追溯依据。

第二个“1”是配套《标识办法》的强制性国家标准《网络安全技术 人工智能生成合成内容标识方法》（以下简称《标识方法》）。如果说《标识办法》解决“应当做什么”，那么《标识方法》就是解决“具体怎么做”。《标识方法》把制度语言转化为技术语言，提出了标识具体实施方式和操作方法，指导相关主体规范开展标识活动，对文本、图片、音频、视频、虚拟场景等不同模态分别规定显式标识方式，对文件元数据隐式标识的要素、格式和预留字段作出安排，从而避免各平台各做一套、互不兼容。

“N”则是围绕《标识办法》和《标识方法》形成的配套生态。全国网络安全标准化技术委员会已发布7项网络安全标准实践指南，覆盖服务提供者编码、元数据安全防护指南、生成合成内容检测，以及文本、图片、音频、视频等内容的文件元数据隐式标识方法，为生成合成服务提供者和内容传播服务提供者提供参考。此外，与标识系列工作配套的人工智能生成合成内容标识服务平台开放了服务提供者编码、编码规则校验和多模态标识合规性检测等功能，为标准落地提供工具化支撑。以更广的视角来看，“N”是一个持续扩展的实施网络，哪里有新场景、新风险、新技术，哪里就可以形成新的指南、工具和实践。

“1+1+N”标识体系的意义，不只是给生成合成内容贴标签，而是为人工智能时代的网络空间建立一套可识别、可核验、可追溯的信任机制。标识体系把政策法规、标准规范、工程工具和社会共治连接起来，既回应了普通公众对辨别生成合成内容的需求，也为人工智能产业健康发展划定了清晰边界。智能向善不能只靠道德呼吁，更需要制度、标准和实践共同发力。人工智能生成合成内容标识，正是把“向善”落实到网络安全治理中的一项基础工程。

有效的人工智能安全治理不能仅靠单一主体或单一手段，需推动多元主体协同发力。政府部门持续完善配套法律法规，提供制度保障。企业主动承担主体责任，严守安全底线，确保产品与服务安全可用。公众主动学习人工智能安全知识，形成“看标识、辨来源”的网络素养，不随意泄露人脸、声音等信息，不恶意使用人工智能工具。此外，产学研用各方加强合作，推动标准迭代与技术创新同步，持续开展人工智能安全标准宣传与技能培训，提升全社会的人工智能安全意识与使用素养。

合力保卫家庭网络和数据安全

随着智能家居、物联网、车联网的普及，与家庭隐私紧密相关的设备产品存在哪些网络安全风险？如何避免？

杨韬（国家信息技术安全研究中心副总工程师）：伴随信息技术的发展，科技范式正在发生深刻变革，网络系统和产品的数字化、网络化、智能化水平不断增强，功能不断丰富拓展。近年来，在智能家居、物联网设备方面，用户规模逐年增多，细分品类层出不穷，持续优化改善了居民生活体验。在其他垂直领域方面，以智能网联汽车为代表的新产业新业态涌现，重塑着生产生活方式。与此同时，上述网络系统和产品的升级迭代，由于其联网需求、数据收集使用、智能技术应用等多种客观原因，引发或加剧了新型网络和数据安全风险隐患，主要体现在以下方面。

一是系统安全能力不健全，易引发网络攻击。以智能家居为代表的智能终端产品制造成本低、更新迭代快，生产过程中的安全机制设计不足、安全检测不充分，部分产品的嵌入式操作系统版本老旧、功能单一，硬件安全能力缺失，难以支持权限管控、加密保护等安全措施。同时，智能终端产品、智能网联汽车拥有复杂庞大的软硬件供应链，原始设备供应商安全能力参差不齐，部分功能模块、组件器件的安全水平堪忧，安全补丁的更新发布滞后。针对智能终端产品、物联网设备的网络攻击可以通过安全漏洞、弱口令等，远程侵入联网设备，进而实施数据窃取、设备控制等非法、高危操作。

二是数据收集使用不规范，易泄露敏感信息。当前，智能家居、物联网设备等实质上已经具备直接收集使用个人信息的客观条件，部分数据处理活动可能是其实现业务功能所必需的，但仍存在不规范、非必要的数据收集使用行为。在数据收集方面，部分智能终端、智能网联汽车存在预装大量应用的情况，部分终端预装应用高达数十款甚至上百款，其中既存在用户难以卸载的应用，也存在后台收集使用个人信息的应用，还存在无隐私政策的应用，用户对其收集使用个人信息的行为无感知，甚至部分应用收集的个人信息并非实现其基本功能服务所必需。在数据使用方面，智能终端、智能网联汽车的数据业态链条长、生态复杂，从用户侧收集的数据往往会流经不同类型的数据处理者，安全能力良莠不齐，数据的提供、委托处理、共同处理权责划分不清晰，部分存在与数据收集目的无关的数据使用场景。

三是智能技术应用不完善，易产生决策偏差。以生成式人工智能技术为代表的新技术飞速发展，网络系统和产品的智能化进程加快，但由于目前人工智能在伦理、技术方面还存在若干瓶颈问题，其直接应用于复杂决策处置还需审慎。如，部分智能终端缺乏信息校验机制，直接将网络内容反馈给用户，其中不乏虚假、违规信息。又如，人工智能技术的“黑箱”特性增大了事件溯源的难度，幻觉问题易导致生成错误知识和决策，普通用户可能难以甄别。上述问题在智能终端、智能网联汽车应用场景下同样存在，且风险可能被进一步放大。

近年来，随着网络安全法、数据安全法、个人信息保护法以及《网络数据安全管理条例》等法律法规的颁布实施，国家网络和数据安全的顶层设计日趋完善，国家网信办等有关部门持续加大个人信息保护等工作力度，开展系列专项行动，切实维护了人民群众的合法权益。2026年4月，国家网信办等部门发布《网络安全标识管理办法》，5月，国家网信办就《消费类网联摄像头网络安全标识实施规则》及相关标准公开征求意见，推动网络产品网络安全管理体系化、标识化、规范化。

还要看到，智能家居、物理联网设备、智能网联汽车等网络系统和产品，由于其产业生态复杂、品类多、用户广等特点，客观上大幅增加了网络和数据安全监管治理的难度。为破解此难题，促进智能终端产业高质量发展和高水平安全良性互动，需要政产研用各方形成合力，共同筑牢家庭网络和数据安全防线。

加强指导监督。围绕智能终端、智能网联汽车的业务链、供应链特点，强化产业梳理、标准规范制定和专项行动实施，针对性督促指导相关网络运营者、网络产品和服务提供者、数据处理者，特别是生态链上的中小型企业，不断提升安全能力及合规水平。

压实主体责任。对于智能终端、智能网联汽车生态链上的各类经营主体，严格依法落实安全责任，高度重视网络安全防护和数据安全保护能力建设，增强安全机制和措施建设应用的适应性、有效性，加强人工智能技术安全性研发与风险防控。

增强安全意识。对于购买智能终端、智能网联汽车的用户，加强案例和技术学习，在可行前提下修改默认口令、采用复杂口令，及时更新升级设备，尝试修改默认不安全配置、管理系统权限使用，降低遭受网络攻击风险。在法律允许的范围内灵活运用各种维权方式，对于发现的违法违规收集使用个人信息行为，可根据实际情况考虑拒绝、投诉、举报等操作。

个人信息保护重在防治结合

面对手机APP过度索权、平台违规收集信息或泄露，如何确保个人信息安全？

李慈强（华东政法大学经济法学院副教授）：加强个人信息保护是网络安全建设的重要议题，也是老百姓关心关注的话题。个人信息涵盖姓名、身份识别代码、联络方式、财产状况、行踪轨迹等内容，具备极强的私密性与人身依附性，直接关系公民的生活安宁与权益保障。

现实生活中，手机APP过度索权、平台违规收集信息、数据泄露事件频发，个人信息被违规收集或泄露，极易诱发电信诈骗、网络盗刷、恶意骚扰等违法犯罪行为，威胁群众人身与财产安全。此外，复杂的隐私政策和维权的高门槛，使得普通人在面对平台时常处弱势。造成个人信息侵权频发的原因是多方面的。例如，公民缺乏应有的信息安全防范意识，易遭遇钓鱼诈骗；企业为牟取不当商业利益违规超范围收集或处理个人信息，导致用户信息被不当披露或者泄露；大数据平台未尽安全保障义务，由此产生的信息安全风险，在平台“风险积聚效应”和“风险涟漪效应”的加持下被无限放大。

保护个人信息，是守护公民合法权益、维护社会秩序稳定的重要举措。于个体而言，防范个人信息侵权能够有效保护个人隐私与人格尊严，避免生活轨迹、消费习惯等被过度采集和滥用，遏制大数据杀熟等乱象。同时，还可防止他人冒名顶替进行违法犯罪活动，避免卷入不必要的法律纠纷。于社会而言，规范网络运营主体的信息处理行为可以遏制信息倒卖黑色产业链的滋生蔓延，净化网络空间生态，促进数字产业的健康发展与社会长治久安。

个人信息保护重在防治结合。为应对频发侵权事件，不能仅依赖特定主体、单一手段来加强个人信息保护，必须树立整体性思维，从防范与治理两方面着手，为个人信息保护筑起法治防线。

从防范的角度来看，公民要强化个人信息保护意识，主动学习侵权防范技巧，警惕各类主体以业务需要为名违规超范围收集个人信息，提升风险识别能力，筑牢自我防护屏障。企业应坚持合法、正当、必要、诚信的原则，遵守个人信息收集与处理的法定边界，依法公示隐私政策及权限授权规则，健全内部信息管控与流程约束机制，从源头上规避个人信息泄露、篡改及毁损风险。大数据平台需建立完备的个人信息分级分类管理体系，严格落实加密存储、去标识化等技术性防护措施，建立常态化合规管理与动态风险排查机制，落实个人信息全生命周期安全防护。国家机关尤其是网信部门应履行法定监管职责，积极开展个人信息保护法治宣传教育，提升全社会信息安全防护素养；严厉打击违规收集、非法处置及不当披露个人信息等违法行为，通过加强监管来确保个人信息安全。

从治理的角度来看，当前个人信息侵权行为呈现出隐蔽化、规模化、产业化的特征，传统的单一规制模式难以满足复合型风险治理需求，需要确立多元协同的系统治理理念，构建企业自治、行业自律、行政监管与司法救济相结合的共治格局。

在企业自治层面，企业在依法享有数据持有、使用和经营权益的同时，也要自觉承担起信息保护的主体责任，健全内部风险排查、权限管控与应急处置机制，从事前防范、事中管控到事后救济，全流程筑牢个人信息安全防线。

在行业自律层面，可借鉴上海市互联网行业个人信息保护自律联盟的有益经验，由行业联盟牵头制定统一的自律公约，形成行业内部自我约束、自我规范、自我监督的治理体系。

在行政监管层面，针对监管职权分散、权责交叉等问题，可依托专项治理统筹机制，组建跨部门的个人信息保护专项工作组，统一执法尺度、协同处置跨领域案件。对大量或高频处理敏感个人信息的主体实行备案准入，强化过程管理，从源头上压实主体责任。

在司法救济层面，针对算法黑箱导致的举证困难，应适度推行举证责任倒置，权利人初步证明损害事实即可推定因果关系，信息处理者则需举证免责事由；完善公益诉讼机制，规范个人信息保护公益诉讼案件办理，履行好公益诉讼检察的法定职责，弥补个体维权乏力的短板。

未来，亟须加强风险预防、健全多元主体协同共治体系，推动个人信息保护向事前防范、事中管控到事后救济全流程发展。在守住个人信息安全底线的同时，统筹兼顾数据要素合规流通与价值释放，实现权利保障、安全规制与产业发展的深度耦合与动态均衡。

本版编辑 聂 倩 常艳军 美 编 夏 祎 来稿邮箱 jjrbjjzk@163.com