中国信通院安全研究所研究报告

深度研究报告

研究时间：2026-05-12 | 所属领域：网络与数据安全、信息通信安全、产业政策支撑 | 研究对象类型：工信部直属科研机构下属安全研究机构

作者: Hermes Agent

> 研究时间：2026-05-12 I 所属领域：网络与数据安全、信息通信安全、产业政策支撑 I 研究对象类型：工信部直属科研机构下属安全研究机构

一、一句话定义

中国信息通信研究院安全研究所，简称「中国信通院安全所」，是中国信通院体系内面向信息通信网络、工业互联网、数据安全、车联网、新型网络基础设施和数字安全服务的专业研究与测试评估机构。它的核心价值，集中在政策支撑、标准研制、技术验证、测试评估、产业组织和公共服务平台六类能力上。

从公开资料看，安全所的角色有三个层次。

第一层是政策与监管技术支撑。它面向国家主管部门，参与网络信息安全发展战略、政策文件、管理规范、行业标准与试点任务的研究和落地。

第二层是技术验证与评测。它把5G、工业互联网、车联网、算力网络、人工智能安全等新技术场景转化成可测试、可评估、可对标的能力体系，为运营商、设备商、工业企业、车企和安全企业提供测评依据。

第三层是产业连接。它通过白皮书、标准体系、联盟活动、公共服务平台、联合实验室和行业会议，把政策要求、技术标准、企业实践和市场需求连接起来。

这类机构的研究价值，并不只在于某一项安全技术本身，更在于它处在「监管—标准—评测—产业」之间的枢纽位置。理解安全所，就能理解中国信息通信安全治理体系里一条重要的技术支撑链路。

二、机构定位与基本事实

2.1 母体：中国信通院的位置

中国信息通信研究院是工业和信息化部直属科研事业单位，前身可追溯到1957年成立的邮电部邮电科学研究院。此后经历邮电部电信科学研究院、信息产业部电信研究院、工业和信息化部电信研究院等阶段，2014年更名为中国信息通信研究院。

这一沿革很关键。信通院长期深嵌通信行业，从传统电信网络、互联网、移动通信、云计算、大数据，到人工智能、工业互联网、车联网、算力网络，始终承担政策研究、标准制定、测试认证、产业组织和国际交流任务。安全所的业务边界，也是在这条通信与数字经济主线上逐步扩展出来的。

2.2 安全所的成立与职责

公开搜索摘要和百度百科条目均显示，中国信通院安全研究所成立于2012年11月，是专门从事信息通信领域安全技术研究的科研机构。其主要职责包括：开展信息通信安全防护的战略性和前瞻性问题研究，加强信息通信新技术新业务评估，为国家主管部门有关网络信息安全发展战略、决策、规范的制定提供技术支撑。

百度百科对安全所的公开信息做了进一步汇总：安全所聚焦信息通信安全领域的战略研究、技术评估与标准制定，拥有工业互联网安全技术试验与测评工信部重点实验室；下设10个部门，员工230余名；现任所长为谢玮，副所长包括魏薇、孟楠，副总工程师为何异舟。由于百度百科属于二手资料，这些组织人数与职务信息应以中国信通院官网或正式会议资料为准。中国信通院官网组织机构页面在本次访问中触发错误页，搜索摘要与多个行业页面能相互印证安全所成立时间和职责描述。

2.3 公开可核验的核心人物

公开期刊页面《信息通信技术与政策》在2025年1月「网络安全」专题导读中给出了谢玮简介：谢玮为中国信息通信研究院安全研究所所长、正高级工程师，长期从事网络和数据安全、工业互联网安全、车联网安全等领域研究工作，牵头建设多个国家级和部级重要支撑平台，支撑信息通信领域网络安全政策文件的制定及重大任务落实，承担科技部、国家发展改革委、工业和信息化部等重大课题，主持并负责大量网络安全国际标准、国家标准和行业标准制定，相关科研成果和标准获得省部级以上奖励二十余项。

通信世界网在2024年12月报道，安全所副所长魏薇发布并解读《算力网络数据安全研究报告（2024年）》。同一报道显示，该报告关注算力网络发展现状、数据安全风险与应对思路，提出「三横一纵」的算力网络安全保护体系框架。

通信世界网在2023年12月报道，安全所副所长孟楠在2024中国信通院ICT深度观察报告会上接受采访，讨论卫星互联网、算力网络、6G等新型网络基础设施带来的安全挑战，并提到传统安全技术升级、内生安全技术成熟、人工智能辅助安全运维、6G安全架构等方向。

这些公开材料能说明，安全所的专家画像集中在三类能力：政策与重大任务支撑、前沿通信网络安全研究、标准与测评体系建设。

三、纵向发展：从通信安全支撑到数字安全枢纽

3.1 2012年前后：安全所成立的制度背景

安全所成立于2012年11月。这个时间点处在中国信息通信业从3G向4G跃迁、移动互联网迅速扩张、网络安全监管体系逐步强化的阶段。

2012年前后，通信网络安全的核心矛盾已经超出传统电信网的可靠性和可用性范畴。智能终端、移动应用、云服务、互联网平台开始进入通信网络，电信网与互联网的边界逐渐变得复杂。主管部门需要一个熟悉通信网络、懂标准、懂测试、能连接企业和监管的专业机构，来承担新技术新业务安全评估、政策研究、标准规范和技术支撑。

安全所由信通院内部成长出来，天然继承了信通院的通信产业基础。这决定了它早期的重点集中在信息通信网络安全、运营商网络安全、防护体系、标准评估和监管支撑。

3.2 2014—2018：伴随信通院更名与移动通信升级，进入更宽的ICT安全议题

2014年，工信部电信研究院更名为中国信息通信研究院。更名背后是研究范围的扩大：从传统电信技术与监管支撑，扩展到信息通信、互联网、数字经济、工业互联网、云计算、大数据、人工智能等综合领域。

安全所也随之进入更宽的ICT安全议题。公开资料显示，其研究方向覆盖通信网安全、数据安全、工业互联网安全、应用安全、互联网安全、重要通信等领域。2018年，安全所参与的「基于5G网联的安全无人机能力系统」项目在「绽放杯」5G应用征集大赛中获得一等奖。该案例体现出安全所已开始把安全能力放进5G应用场景中验证，研究对象从网络设备或传统信息系统扩展到垂直行业应用。

这一阶段可以看作安全所从「通信网络安全支撑机构」向「ICT融合安全研究机构」过渡。它开始接触5G、物联网、工业互联网和垂直行业应用，安全对象从网络设备扩展到应用场景、业务系统、数据流动和产业生态。

3.3 2019：工业互联网安全与自动化响应进入视野

2019年前后，工业互联网安全成为安全所的重要方向。工信部等十部门发布《加强工业互联网安全工作的指导意见》，提出制定工业互联网行业企业分类分级指南，对企业实施分类分级管理。安全所相关业务页面显示，其「工业互联网安全公共服务平台」建设目标，是落实《国务院关于深化“互联网+先进制造业”发展工业互联网的指导意见》《加强工业互联网安全工作的指导意见》等文件精神，构建公共服务平台，为工业互联网相关行业、企业、政府部门、研究机构提供专业、全面、便捷、可靠的安全服务，支撑工业互联网安全建设、运营、监管和研究工作。

同年11月，安全所与安恒信息在第九届电信和互联网行业网络安全年会上联合发布《网络安全先进技术与应用发展系列白皮书——安全编排自动化与响应（SOAR）》。SOAR的出现，说明安全所开始关注安全运营自动化、威胁响应编排和企业侧安全能力建设。

这一阶段的关键词是「平台化」与「体系化」。工业互联网安全要求处理设备、网络、平台、应用、数据、企业责任、监管要求等多重对象。单点检测已难支撑复杂场景，公共服务平台、分类分级、标准体系、试验与测评能力成为政策落地的重要工具。

3.4 2020：5G安全测评的国际化节点

2020年11月，安全所获得GSMA认可，成为GSMA网络设备安全保障框架NESAS下全球首家全面具备5G基站和核心网安全检测评估资质的机构。通信世界网报道显示，安全所搭建了灵活的端到端5G安全测试环境，可适配不同测试需求场景，配备完备测试工具，完成了对华为、中兴、大唐、爱立信等国内外主流设备企业5G基站和核心网设备的安全测试。

这一事件的意义有两层。

一层是能力层面。5G安全评测需要理解无线接入网、核心网、网络切片、边缘计算、虚拟化、协议栈和设备生命周期等复杂对象。获得NESAS认可，说明安全所的检测流程、测试环境和能力体系进入国际框架。

另一层是信任层面。5G网络建设牵涉运营商设备选型、网络安全建设、垂直行业应用和国际供应链。安全所参与IMT-2020(5G)推进组，联合基础电信企业、设备企业、安全企业制定与国际接轨的5G设备安全保障规范，体现出它在中国5G安全治理中的桥梁作用。

2020年的GSMA资质，是安全所纵向发展中的标志性节点。它把安全所从国内政策支撑与行业测评机构，推到了国际安全评估框架的可见位置。

3.5 2021—2022：工业互联网、车联网与公共服务平台扩展

2021年以后，工业互联网安全的政策体系持续细化。工信部发布工业互联网企业网络安全分类分级管理试点相关通知，2024年印发《工业互联网安全分类分级管理办法》。全国工业互联网安全分类分级管理平台公开页面显示，分类分级管理要集中力量指导、监管重要行业、重点企业，夯实企业网络安全主体责任。

安全所在这一过程中承担的角色，集中在公共服务平台、标准研究、试验验证和行业支撑。服务平台页面将「业务部门」标注为安全研究所，说明该平台与安全所业务直接关联。

2022年11月，中国信通院推出「重光」系列之车联网安全评估评测服务平台。C114通信网转载中国信通院信息显示，该平台基于多年车联网安全研究基础和检测评估实践，服务车联网企业安全合规、风险发现和防护能力提升。平台覆盖车端、车辆服务平台、车内外通信等核心对象，支持企业开展网络安全自查、安全风险评估和漏洞隐患检测；内置车联网安全标准库、检测评估指导库、漏洞库，覆盖ISO/SAE 21434、汽车网关信息安全技术要求、车联网信息服务数据安全技术要求、联网汽车信息安全技术要求、车联网服务平台网络安全防护要求等国内外标准或要求。

车联网安全把安全所推向另一个复杂场景：通信网络、汽车电子、道路交通、云平台、移动应用、数据合规和漏洞检测交织在一起。安全所的优势仍然是把复杂对象转化为评估流程、标准库、工具集和可生成报告的服务平台。

3.6 2023—2025：算力网络、6G、AI安全与数字安全服务

2023年12月，孟楠谈到卫星互联网、算力网络、6G等新型网络基础设施对网络安全提出新挑战。他提到，传统密码、防火墙、入侵检测、安全审计等技术会持续升级；拟态防御、可信计算等内生安全技术将逐步成熟；人工智能大模型可增强威胁分析能力和安全运维效率；在6G发展初期，全球产业界已将安全、隐私和韧性纳入关键指标。

2024年12月，魏薇发布并解读《算力网络数据安全研究报告（2024年）》。报告聚焦算力网络架构下的数据安全问题，认为算网融合带来异构节点增多、网络互联升级、资源调度智能化，数据安全、网络安全和新技术安全相互渗透。报告提出「三横一纵」保护体系，并提出明确职责划分、数据安全能力编排与融合调度、隐私计算、数字水印等关键措施。

公开资料还显示，安全所近年来推出「信通卫士」数字安全服务平台。搜索摘要显示，该平台与数字安全服务能力相关，但本次未能获取到足够完整的一手页面，报告中只将其作为待进一步核验的线索。

这一阶段，安全所的研究对象从5G与工业互联网继续向算力网络、6G、卫星互联网、生成式人工智能安全运营等方向延伸。安全边界从网络设备和企业系统，扩展到数据要素流通、算力调度、跨主体协作、智能编排和未来网络架构。

四、当前能力图谱：安全所到底做什么

4.1 通信网与5G安全评测

5G安全是安全所最具标识度的能力之一。服务平台页面写明，安全所提供5G设备、系统、网络、业务安全能力测试，以及5G设备的软件应用、信息安全等测试服务。其5G安全测评中心建立5G安全标准框架和评测体系，建设与国际接轨的测评能力，完成主流设备厂家5G设备安全测试，并成为GSMA认可的安全检测实验室。

这一能力的对象包括5G基站、核心网、协议安全、信令风暴验证、关键设备安全检测、行业应用安全分级评估、测试验证和试点示范。它的客户或服务对象，既包括设备企业，也包括基础电信企业和垂直行业用户。

4.2 工业互联网安全公共服务

工业互联网安全公共服务平台的建设目标，直接指向工业互联网安全建设、运营、监管和研究。它服务企业、政府部门、研究机构等多方主体，承担分类分级、风险评估、能力提升、监管支撑等任务。

工业互联网安全的治理难点在于对象高度异质：工业控制系统、企业内网、工业互联网平台、标识解析、边缘设备、生产数据、供应链和人员流程同时存在。安全所的价值在于将政策要求转换为可执行的评估与服务流程。

4.3 数据安全与算力网络安全

《算力网络数据安全研究报告（2024年）》体现了安全所在数据安全方向的最新关注。报告把算力网络分为基础设施层、编排管理层、运营服务层等维度分析风险，强调算力消费者、算网运营者、算力供应者的责任划分，并提出能力登记、需求解析、编排管理、融合调度等数据安全能力编排步骤。

这类研究把数据安全从静态合规审查推进到动态基础设施场景。算力网络中的数据跨节点、跨系统、跨主体流转，安全责任、审计溯源、权限控制、隐私计算和数字水印都需要嵌入调度和运营过程。

4.4 车联网安全评估评测

「重光」车联网安全评估评测服务平台显示出安全所对车联网安全的工程化能力。平台覆盖车端、服务平台、车内外通信，内置标准库、指导库、漏洞库和工具集，支持漏洞扫描、配置核查、固件检测、APP安全扫描、容器镜像扫描、接口测试等。

车联网安全的特点是跨行业。汽车产业原有的功能安全、质量体系和供应链管理，与网络安全、数据安全、通信安全、云平台安全逐渐融合。安全所通过标准库和评估平台，将通信安全和数据安全方法带入汽车数字化场景。

4.5 新型网络基础设施与前沿安全

孟楠关于卫星互联网、算力网络、6G的公开采访，展示了安全所对新型网络基础设施的关注：泛在接入、多源异构、天地一体、边界模糊、内外交互频繁，会提高安全防护难度。6G安全、隐私、韧性、AI使能安全、量子密钥分发、隐私计算、内生安全等方向，已成为全球产业界和标准组织关注的议题。

安全所的路径通常是：在新技术大规模部署前，先开展安全需求、架构、关键技术、标准和测试验证研究，再通过产业组织和平台推动共识形成。

五、横向对比：安全所处在什么生态位

5.1 与国家工业信息安全发展研究中心

国家工业信息安全发展研究中心同为工信部直属事业单位，前身可追溯到1959年的电子科学技术情报研究所。公开资料显示，它是我国工业领域国家级信息安全研究与推进机构，围绕工业信息安全、产业数字化、软件和知识产权、智库支撑等板块开展工作，具备安全审查、检验检测、风险评估、应急处置、等保测评、司法鉴定、质量管理体系认证、工程咨询等资质。

相较国家工信安全中心，安全所更深地嵌入信通院的信息通信与数字基础设施主线。国家工信安全中心在工业信息安全、工控安全、工业领域安全监测、产业数字化等方面具有更强工业侧色彩；安全所则在通信网、5G、6G、工业互联网平台、车联网、算力网络、数据安全和ICT标准评测上更具通信产业连接能力。

二者在工业互联网安全上存在交叉，但侧重点不同。国家工信安全中心更像工业安全治理与产业安全支撑机构，安全所更像ICT安全标准评测和通信数字基础设施安全支撑机构。

5.2 与CNCERT

CNCERT/CC成立于2001年8月，是中国计算机网络应急处理体系中的牵头单位。其官网显示，CNCERT按照「积极预防、及时发现、快速响应、力保恢复」方针，开展互联网网络安全事件的预防、发现、预警和协调处置，运行国家信息安全漏洞共享平台CNVD，维护公共互联网安全，保障关键信息基础设施安全运行。CNCERT在中国大陆31个省区市设有分支机构，并通过网络安全企业、学校、社会组织、研究机构、骨干网络运营单位、域名服务机构等构建应急体系。

CNCERT的核心词是「应急协调、监测预警、漏洞共享、事件处置」。安全所的核心词是「政策支撑、标准研究、测试评估、平台服务、产业验证」。

两者都涉及网络安全标准和评测，但CNCERT更贴近事件与态势，安全所更贴近新技术新业务的安全评估与治理规则形成。

5.3 与CESI、中国工业互联网研究院等工信部体系机构

中国电子技术标准化研究院（CESI）偏电子信息技术标准化、合格评定、认证认可、质量与可靠性。它在国家标准、电子信息产品质量、软件工程、数据管理、信息安全标准化等方面有强积累。

中国工业互联网研究院偏工业互联网战略、规划、政策、标准、标识解析、网络、平台、数据与安全体系。它面向工业互联网整体体系建设，安全是其中重要组成部分。

安全所与这些机构的关系，可以理解为同一政策体系中的分工协同：CESI强调电子信息标准化与合格评定，中国工业互联网研究院强调工业互联网整体基础设施与体系建设，安全所强调信息通信和数字基础设施中的安全研究、评测与产业支撑。

5.4 与NIST、ENISA、ETSI、ITU等国际机构

NIST是美国商务部下属机构，承担测量科学、标准、技术和产业竞争力相关任务。NIST CSRC提供大量网络安全与隐私项目、出版物、指南和框架；其Cybersecurity and Privacy Reference Tool旨在帮助用户识别、比较和定制NIST网络安全与隐私标准、指南和框架内容。NIST NCCoE则强调政府、产业和学术界协作，解决组织面临的网络安全挑战。

ENISA是欧盟网络安全局。其官网显示，ENISA依据欧盟2019/881号《网络安全法案》获得永久授权，围绕欧洲共同网络安全水平、认证、标准、事件响应、风险管理、技能和漏洞披露等开展工作。

ETSI是欧洲电信标准协会，会员制ICT标准组织。其网站强调标准制定、互操作测试、开源支撑、研究创新支撑、政策事务等能力。ITU-T SG17是国际电信联盟电信标准化部门下的安全研究组，长期承担电信安全、网络安全、身份管理等国际标准工作。

安全所与这些国际机构相比，具有更强的中国主管部门技术支撑属性和产业落地属性。NIST偏通用框架和指南，ENISA偏欧盟政策协调与能力建设，ETSI/ITU偏标准组织，安全所则把政策研究、标准研制、测试评估、产业平台和监管支撑聚合在同一个机构体系内。

5.5 与商业安全厂商

奇安信、深信服、安恒信息、360、阿里云、腾讯安全、华为安全、绿盟科技、启明星辰等安全厂商，主要以产品、解决方案、云安全服务、攻防能力、托管运营和客户项目交付为主。它们服务政府、央国企、运营商、金融、能源、制造、互联网等行业客户，核心竞争力来自产品能力、项目经验、渠道、交付和安全运营。

安全所与商业厂商的关系更接近「规则、验证和产业组织」关系。安全所可能与厂商联合发布白皮书、参与测试、组织标准、共建实验室或推动行业试点，但其身份并非商业产品供应商。它的影响力来自政策支撑位置、标准话语权、评测可信度和产业连接能力。

六、横纵交汇洞察

6.1 安全所的历史路径塑造了今天的生态位

安全所的历史路径很清晰：从通信网络安全出发，经由5G、工业互联网、车联网，进入算力网络、6G、卫星互联网和AI安全运营。每一次扩展都沿着信息通信基础设施的演进展开。

这让安全所形成了独特的生态位。它对单一安全产品的依赖较低，对「新型基础设施如何安全部署」的依赖很高。只要中国数字基础设施继续升级，安全所就会持续获得新的研究对象和支撑任务。

5G安全测评是一个典型例子。它既要求理解国际框架NESAS和3GPP安全测试用例，也要求理解中国运营商、设备商和垂直行业的现实部署。安全所能把国际框架、国内产业、监管目标和测试能力连接起来，这种能力很难由单一商业厂商替代。

6.2 优势来自「制度位置+工程验证」的组合

安全所的优势来自制度位置与工程验证的组合，研究报告和实验室测试都服务于这组能力。

制度位置让它能较早接触主管部门关注的安全议题，参与政策和标准前期研究。工程验证让它能把抽象政策要求转化为测试环境、评估流程、平台工具和验证案例。二者结合后，安全所能在产业尚未形成成熟市场时先建立评估语言。

工业互联网分类分级、5G安全检测、车联网安全评估、算力网络数据安全都符合这一逻辑。它们早期都有共同难题：对象复杂、主体多元、标准分散、责任边界模糊。安全所的工作，是把这些模糊问题拆成可讨论、可测试、可治理的框架。

6.3 主要风险来自透明度、边界与市场化效率

安全所的风险同样来自其机构属性。

第一个风险是公开透明度不足。官网页面访问不稳定，组织架构、团队、项目、证书、平台能力、标准参与情况等公开信息较分散，很多事实需要通过搜索摘要、转载报道、会议页面和百科条目拼接。对于一个承担公共技术支撑和行业评测的机构来说，更清晰的公开资料有助于提升行业信任。

第二个风险是业务边界容易被外界误读。信通院内部不同研究所、泰尔实验室、云大所、技术与标准所、产业互联网所等都参与数字安全相关工作，外部企业常把「信通院」作为整体引用。安全所真实负责的范围，需要在正式项目、平台页面、报告署名和会议材料中逐项核验。

第三个风险是市场化效率。安全所的强项是标准、评测、政策支撑和公共服务，商业厂商的强项是产品迭代、客户交付和安全运营。若某些公共平台要长期服务企业，需要在权威性、便利性、响应速度和工具更新之间保持平衡。

6.4 未来三种情形

基准情形：安全所继续沿着新型数字基础设施安全主线扩展。5G-A、6G、卫星互联网、算力网络、工业互联网、车联网、人工智能安全运营、数据流通安全将成为持续议题。安全所会继续发布研究报告、参与标准、建设评测能力和公共服务平台。

乐观情形：安全所把现有评测与平台能力进一步产品化、开放化和国际化。5G NESAS资质曾经带来国际可见度，如果在6G安全、算力网络数据安全、车联网标准符合性评估、AI安全评测等领域形成更透明的证书体系、公开案例库和国际互认机制，安全所的影响力会超出国内政策支撑范围，进入国际数字基础设施安全治理网络。

风险情形：如果安全所的信息公开、平台服务体验、标准与评测更新速度跟不上产业变化，商业厂商、国际组织、行业联盟和地方实验室会分散其影响力。尤其在人工智能安全、云原生安全、数据要素流通和车联网攻防等快速变化领域，评测方法滞后会削弱权威机构的实践价值。

七、结论

中国信通院安全所是一类典型的中国式数字安全支撑机构。它的价值不宜用商业安全公司、单一实验室或纯学术研究机构来衡量。更准确的观察方式，是把它放在国家数字基础设施建设和安全治理体系中：它负责把政策目标、技术标准、产业实践和测试验证连接起来。

从2012年成立到今天，安全所经历了通信网安全、5G安全、工业互联网安全、车联网安全、算力网络数据安全和未来网络安全的连续扩展。它的主线始终围绕信息通信基础设施展开，安全对象随基础设施演进而变化。

未来，安全所的关键看点有四个：6G与卫星互联网安全架构，算力网络与数据安全能力编排，车联网与智能网联汽车安全评估，人工智能辅助安全运营与AI系统安全评测。如果这些方向能够形成公开、可复用、可验证的标准和平台，安全所会在中国数字安全治理中继续保持枢纽位置。

八、信息来源

1. 中国信息通信研究院业务服务平台：《5G应用安全测试》，https://service.caict.ac.cn/ywjs/202011/t20201126_1208.html，访问时间：2026-05-12。
2. 中国信息通信研究院业务服务平台：《工业互联网安全公共服务平台》，https://service.caict.ac.cn/ywjs/202107/t20210716_3333.html，访问时间：2026-05-12。

3. 通信世界网：《中国信通院获得GSMA 5G设备安全国际检测评估资质》，https://www.cww.net.cn/article?from=timeline&id=479178&isappinstalled=0，访问时间：2026-05-12。
4. C114通信网：《中国信通院正式推出“重光”系列之——车联网安全评估评测服务平台》，https://www.c114.com.cn/news/16/a1215134.html，访问时间：2026-05-12。
5. 通信世界网：《信通院魏薇发布并解读〈算力网络数据安全研究报告（2024年）〉》，https://www.cww.net.cn/article?id=596574，访问时间：2026-05-12。
6. 通信世界网：《信通院孟楠：卫星互联网、算力、6G等为网络安全带来新挑战》，https://cww.net.cn/article?id=585866，访问时间：2026-05-12。
7. 《信息通信技术与政策》：《专题导读：网络安全》，http://ictp.caict.ac.cn/CN/abstract/abstract1344.shtml，访问时间：2026-05-12。
8. 工业和信息化部：《工业和信息化部关于印发〈工业互联网安全分类分级管理办法〉的通知》，https://www.miit.gov.cn/jgsj/waj/wjfb/art/2025/art_72d3dab251474245908611263f50b096.html，访问时间：2026-05-12。
9. 全国工业互联网安全分类分级管理平台，https://www.ciisec.org.cn/，访问时间：2026-05-12。
10. 国家互联网应急中心：《CNCERT简介》，https://www.cert.org.cn/publish/main/34/index.html，访问时间：2026-05-12。
11. NIST Computer Security Resource Center，https://csrc.nist.gov/，访问时间：2026-05-12。
12. NIST Cybersecurity and Privacy Reference Tool，https://csrc.nist.gov/projects/cprt/learn，访问时间：2026-05-12。
13. ENISA：《ENISA Mandate and Regulatory Framework》，https://www.enisa.europa.eu/about-enisa/regulatory-framework/legislation，访问时间：2026-05-12。
14. 百度百科：《中国信息通信研究院安全研究所》，https://baike.baidu.com/item/中国信息通信研究院安全研究所/49762667，访问时间：2026-05-12。该来源用于补充组织人数、领导与发展节点线索，正式引用时建议以中国信通院官网或正式会议资料复核。
15. 中国信通院：《网络安全产业白皮书（2021年）》PDF，https://www.caict.ac.cn/kxyj/qwfb/bps/202201/P020220124544366719425.pdf，访问时间：2026-05-12。该PDF已下载，因本地PDF文本抽取依赖受限，本报告未对其具体页码内容作展开引用。