国盟信息安全通报

2019 年 12 月 09 日第 207 期

国盟信息安全通报

（第 207 期）

国际信息安全学习联盟

2019 年 12 月 09 日

国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 402 个，其中高危漏洞 91 个、中危漏洞 276 个、低危漏洞 35 个。漏洞平均分值为 5.59。本周收录的漏洞中，涉及 0day 漏洞 125 个（占 31%），其中互联网上出现“vBulletin 远程命令执行漏洞（CNVD-2019-42750）、Jobberbase SQL 注入漏洞”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 1893 个，与上周（2044 个）环比减少 7%。

主要内容

一、概述 4
二、安全漏洞增长数量及种类分布情况 4
➢漏洞产生原因（2019 年 11 月 25 日—2019 年 12 月 09） 4
➢漏洞引发的威胁（2019 年 11 月 25 日—2019 年 12 月 09） 5
➢漏洞影响对象类型（2019 年 11 月 25 日—2019 年 12 月 09） 5
三、安全产业动态 6
➢努力开创网络安全和信息化工作新局面 6
➢做好数据治理 更快更好地推进数字化转型 12
➢最高人民法院发布《中国法院的互联网司法》白皮书 15
➢重要信息系统安全检查实施方法与技术措施 20
四、政府之声 28
➢教育部印发《高等院校管理服务类教育移动互联网应用专项治理行动方案》 28
➢三部门发布《网络音视频信息服务管理规定》 29
➢中国人民银行银保监会发布《系统重要性银行评估办法（征求意见稿）》 32
➢2019 年 11 月全国受理网络违法和不良信息举报 970.8 万件 33
五、本期重要漏洞实例 34
➢Google Chrome AppCache 安全限制绕过漏洞 34
➢Linux kernel 拒绝服务安全漏洞 34
➢Huawei Honor Play 信息泄露漏洞 35
➢Cisco DNA Spaces:Connector 命令注入漏洞 36
六、本期网络安全事件 37
➢勒索软件渗透纽约警察局的指纹数据库 导致系统关闭 37
➢五千多张人脸照片标价 10 元 “四要素”照片 4 元一份 38
➢美商用短信服务商 TrueDialog 数据泄露 涉数千万条短信 40
➢8 人团伙被抓！安全技术人员变身黑客，专黑金融网站数据库 41
➢谷歌技术故障导致美国三大航空公司网站短暂宕机 43
➢两名俄罗斯黑客入侵美国银行系统，盗取 2100 万，遭 FBI 起诉 45

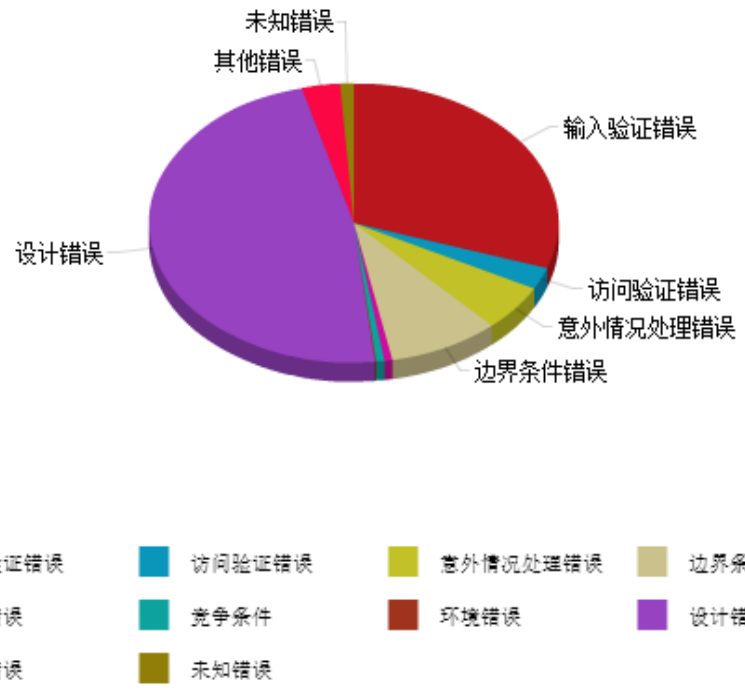
注：本报根据中国国家信息安全漏洞库（CNNVD）和各大信息安全网站整理分析而成。

一、概述

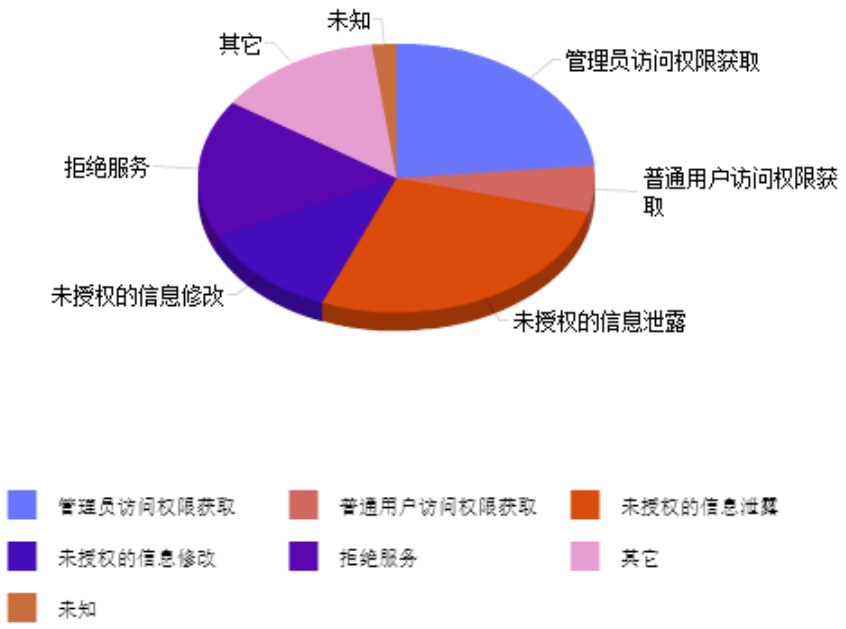
国盟信息安全通报是根据国家信息安全漏洞共享平台（以下简称 CNVD）本周共收集、整理信息安全漏洞 402 个，其中高危漏洞 91 个、中危漏洞 276 个、低危漏洞 35 个。漏洞平均分值为 5.59。本周收录的漏洞中，涉及 0day 漏洞 125 个（占 31%），其中互联网上出现“vBulletin 远程命令执行漏洞（CNVD-2019-42750）、Jobberbase SQL 注入漏洞”等零日代码攻击漏洞。本周 CNVD 接到的涉及党政机关和企事业单位的事件型漏洞总数 1893 个，与上周（2044 个）环比减少 7%。

二、安全漏洞增长数量及种类分布情况

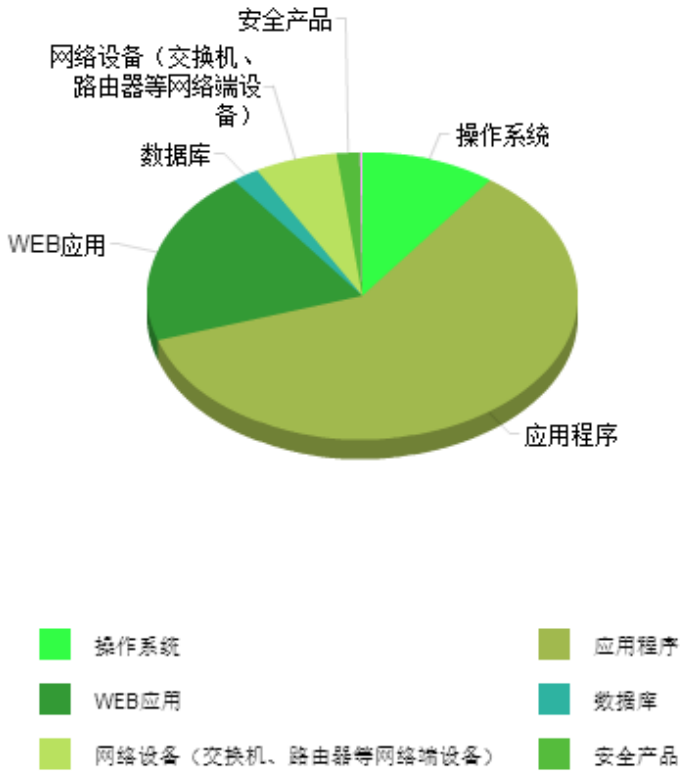
➢ 漏洞产生原因（2019 年 11 月 25 日—2019 年 12 月 09）



➢ 漏洞引发的威胁（2019 年 11 月 25 日—2019 年 12 月 09）



➢ 漏洞影响对象类型（2019 年 11 月 25 日—2019 年 12 月 09）



三、安全产业动态

➢ 努力开创网络安全和信息化工作新局面

党的十八大以来，习近平总书记着眼信息时代发展的时与势，站在实现“两个一百年”奋斗目标和中华民族伟大复兴中国梦的历史高度，就网络安全和信息化工作提出了一系列新理念新思想新战略，系统阐述事关网信事业发展的一系列重大理论和实践问题，形成了关于网络强国的重要思想。习近平总书记强调，“信息化为中华民族带来了千载难逢的机遇”，“我们必须敏锐抓住信息化发展的历史机遇”，推进网络强国建设。深入学习贯彻习近平总书记关于网络强国的重要思想，要求我们必须从中华民族波澜壮阔的历史进程中准确把握时代坐标，从信息化发展带来的机遇挑战中深刻认识职责使命，全面推进网信事业发展，加快建设网络强国，为实现“两个一百年”奋斗目标和中华民族伟大复兴作出应有贡献。

观大势，深刻认识信息时代的机遇和挑战

从社会发展史看，人类经历了农业革命、工业革命，正在经历信息革命。农业时代，我国曾经是世界强国，创造了辉煌灿烂的文明，独领风骚数千年，但在欧洲发生工业革命、世界发生深刻变革的时期，丧失了与世界同进步的历史机遇，逐渐落到了被动挨打的境地。当前，信息革命的时代潮流正加速向各领域广泛渗透，正在全球开启一次具有全局性、战略性、革命性意义的数字化转型，带动人类社会生产方式变革、生产关系再造、经济结构重组、生活方式巨变，极大提升了人类认识世界和改造世界的能力。特别是信息时代人类科学技术伟大革命和中华民族伟大复兴发生历史性交汇，为我国发展带来了新的历史机遇，我们比历史

上任何时期都更接近、更有信心和能力实现中华民族伟大复兴的中国梦。

数据资源成为“新生产要素”。农业时代，土地是最重要的战略资源，国家、民族之间的战争几乎都围绕着争夺土地展开。工业时代，以煤炭、石油为代表的能源矿产成为最重要的战略资源，能源控制权往往成为国家争夺的焦点。进入信息时代，随着信息技术和人类生产生活交汇融合，互联网快速普及，全球数据呈现爆发增长、海量集聚的特点，数据日益成为重要战略资源和新生产要素，对经济发展、国家治理、社会管理、人民生活都产生重大影响，数据掌控能力日益成为衡量国家竞争力的关键因素。

信息技术领域成为“新创新高地”。当前，以互联网为代表的新一代信息技术是全球研发投入最集中、创新最活跃、应用最广泛、辐射带动作用最强的科技创新领域，是全球技术创新的竞争高地。移动互联网、大数据、云计算、物联网、人工智能、区块链等新兴技术加速向各领域渗透融合，深刻改变人们生产生活方式，网络连接从人人互联迈向万物互联，技术应用从侧重消费环节转向更加侧重生产环节。

互联网、工业互联网、物联网等成为“新基础设施”。互联网是信息时代的新基础设施，是经济社会发展的“大动脉”。传统基础设施带来的是“乘数效应”，而互联网带来的是“幂数效应”。当前正处于全球网络信息技术加速创新变革、信息基础设施快速演进升级的关键“窗口期”，人工智能、工业互联网、物联网、大数据中心等新型基础设施将对经济社会发展产生更为重要的推动作用。

数字经济成为“新经济引擎”。当今世界，信息技术创新的扩散效应、信息和知识的溢出效应、数字技术释放的普惠效应日益凸显。各国加紧发展数字经济，推动新技术向实体经济各领域渗透融合，使新技术成为放大生产力的重要因素，为经济长期持续增长提供了强劲内生动力，数字技术正从助力经济发展的辅助工具向引领经济发展的核心引擎转变。

信息化成为“新治理手段”。新一代信息技术日新月异，为提升国家治理体系和治理能力现代化水平提供了有利条件。比如，移动互联网丰富了公共服务的渠道和范围，云服务为电子政务系统提供了更加灵活的建设和运维模式，大数据日益成为支撑政府科学决策、精准管理的重要工具。世界主要国家都把推进电子政务作为构筑比较优势、提升国家竞争力的战略举措，数字政府建设步伐全面提速。

同时也要清醒地看到，互联网是“双刃剑”，既为我国经济社会发展注入强劲动力，也带来很多风险挑战和不确定因素。比如，互联网日益成为各类风险的策源地、传导器、放大器，维护意识形态安全的任务更加艰巨；核心技术受制于人的状况尚未得到根本改变，“卡脖子”的风险愈加突出；前沿技术发展带来的网络安全新风险逐步凸显，传统网络安全威胁

与新型网络安全威胁相互交织；网络空间军事化态势愈演愈烈，网络空间国际规则的脆弱性和不确定性不断显现；等等。这就要求我们必须明辨方向、把握大势，抓住机遇、应对挑战，引领变局、争取主动，不断开创网络强国建设新局面。

守阵地，牢牢掌握网络意识形态工作领导权

互联网已经成为意识形态斗争的主阵地、主战场、最前沿，网络意识形态安全直接关系国家政治安全。必须科学认识网络传播规律，提高用网治网水平，牢牢掌握网络意识形态工作领导权，使互联网这个最大变量变成事业发展的最大增量。

坚持正能量是总要求。只有正面宣传强劲有力，网上才能正能量充沛，才能让党的声音引领网络空间，也才能有效挤压负面信息的渠道和空间。要坚持高举旗帜，切实以习近平新时代中国特色社会主义思想统领网络宣传舆论工作全局，充分发挥互联网传播优势，不断提升网上宣传效果，让党的创新理论通过互联网“飞入寻常百姓家”，广泛凝聚全党全国各族人民实现“两个一百年”奋斗目标的思想共识和智慧力量。坚持正确的政治方向、舆论导向、价值取向，把政治要求体现到网络意识形态工作各个方面、各个环节，确保网络意识形态工作责任制落到实处。做大做强网上正面宣传，深入宣传新中国成立 70 年来的巨大成就特别是党的十八大以来取得的新成绩新进展，持续做好网上重大主题宣传策划，培育积极健康、向上向善网络文化，用社会主流思想价值和道德文化滋养人心、滋润社会。大力推进网上宣传理念、内容、形式、方法、手段创新，深耕网上内容，注重用户体验，不断提升主流思想舆论的传播力、引导力、影响力、公信力，唱响主旋律，提振精气神，让党的声音成为网络空间最强音。

坚持管得住是硬道理。建立网络综合治理体系，是党的十九大明确提出的一项重要任务，是管网治网的根本之策。要加快建设网络综合治理体系，形成党委领导、政府管理、企业履责、社会监督、网民自律等多主体参与，经济、法律、技术等多种手段相结合的综合治网格局，做到系统性谋划、综合性治理、体系化推进，提高管网治网的系统性和有效性。建立健全网上风险防范机制，及时批判网上错误思潮，坚决清理网上谣言、暴恐音视频等有害信息，全面提升技术治网能力和水平。坚持党管新媒体，压实互联网企业主体责任。充分发挥人民主体作用，走好网上群众路线，积极拓展网络交流沟通渠道，自觉接受广大网民监督，切实形成齐抓共管的整体合力。

坚持用得好是真本事。要发挥传统媒体和新兴媒体各自优势，实现优化整合、深度融合，打造一批具有强大影响力、竞争力的新型主流媒体。要改造传统军，着力推进主流媒体的网络化、数字化转型，强化理念塑造、技术运用和流程再造，为传统媒体注入新活力、拓展新

空间、构筑新优势。要壮大主力军，着力打造新型主流媒体“航母”和“旗舰”，推动信息内容、技术应用、平台终端、人才队伍和管理服务共享融通，把资源、技术、力量向移动端倾斜。要整编生力军，加强对网络媒体平台资本、资质、资格管理，切实把宣传舆论工作的重点转移到互联网这个主战场上，实现媒体融合发展的“转型突围”。

促发展，充分发挥信息化驱动引领作用

习近平总书记指出：“网信事业代表着新的生产力和新的发展方向，应该在践行新发展理念上先行一步。”我们要充分发挥信息化驱动引领作用，以信息化培育新动能、用新动能推动新发展，让互联网发展成果更好服务社会、造福人民。

加快核心技术突破。核心技术是国之重器，要下定决心、保持恒心、找准重心，坚定不移地走自主创新之路，加速推动信息领域核心技术突破。加强网络信息领域基础研究，打通基础研究和技术创新衔接的绿色通道，力争以基础研究带动应用技术群体突破。瞄准国家重大战略需求，加强关键核心技术攻关，集中资源和力量补齐核心芯片短板，攻克人工智能等关键核心技术，着力突破量子计算等前瞻性技术研发。加快建立自主产业生态体系，做好体系化技术布局，打通创新链、产品链、价值链，强化产业链上下游衔接互动，完善金融、财税、国际贸易、人才、知识产权保护等制度环境，更好释放各类创新主体创新活力。

加快信息基础设施建设。当前，信息基础设施对经济社会转型发展的战略性、基础性和先导性作用日益凸显，以卫星互联网、5G、IPv6 等为代表的新一代基础设施与经济社会各领域深度融合，成为我国经济社会数字化转型的战略基石和重要支撑。要把建设新一代信息基础设施作为重点，加快建设我国自主可控的卫星互联网，加快推进 5G 商用部署，加快北斗卫星导航系统建设应用，加快推进基于 IPv6 的下一代互联网规模部署，推动人工智能、工业互联网、物联网等新型基础设施建设，抢占新一代信息基础设施发展的主动权。

加快数字经济发展。我国经济已由高速增长阶段转向高质量发展阶段，要围绕建设现代化经济体系、实现高质量发展，继续在推动数字产业化、产业数字化两端集中发力、精准施策，助推经济结构调整和新旧动能转换。要深入推进数字产业化，发挥数据、信息、知识作为新生产要素的作用，积极发展云计算、大数据、物联网、人工智能，广泛开展应用和模式创新，不断完善网络生态体系。要加快推动产业数字化，培育数字经济领域重大项目建设和优势企业，推动工业互联网应用创新，加快制造业、农业、服务业的数字化、网络化、智能化，推动互联网、大数据、人工智能和实体经济深度融合。

加快信息便民惠民。网信事业发展必须贯彻以人民为中心的发展思想，把增进人民福祉作为信息化发展的出发点和落脚点。要深化信息领域创新成果应用，鼓励和支持新技术、新

应用、新手段在教育、医疗、交通、环境等民生领域的应用，促进基本公共服务均等化。统筹推进政务信息系统整合共享与公共信息资源开放，加快国家电子政务建设。深入推进城乡信息化融合发展，加快新型智慧城市、数字乡村建设，提升乡村地区信息基础设施建设水平。发挥互联网在精准扶贫、精准脱贫中的独特作用，推进网络扶贫工程向纵深发展。

保安全，切实筑牢国家网络安全屏障

习近平总书记指出：“没有网络安全就没有国家安全，就没有经济社会稳定运行，广大人民群众利益也难以得到保障。”要统筹推进网络安全工作，坚持网络安全为人民、网络安全靠人民，坚持网络安全教育、技术、产业融合发展，坚持促进发展和依法管理相统一，坚持安全可控和开放创新并重，切实保障国家网络安全和公民个人信息安全。

强化关键信息基础设施防护。关键信息基础设施是经济社会运行的神经中枢，涉及国家安全、国计民生以及公共利益，对于国家网络安全和信息化建设意义重大。要严格落实《中华人民共和国网络安全法》、网络安全工作责任制要求，夯实关键信息基础设施防护责任，强化不同地区、不同行业、不同领域关键信息基础设施之间的威胁信息共享和协同应对，建立完善关键信息基础设施安全保障体系。加强网络安全检查，明确保护范围和对象，及时发现隐患、修补漏洞，做到关口前移，防患于未然。

强化数据安全管理。在积极开发利用数据资源、充分释放数据效能的同时，切实保障数据安全，强化关键数据资源保护能力。健全管理和运用数据资源的法律制度和政策措施，推动出台数据安全管理办法，依法保护数据资源。加大个人信息保护力度，规范个人信息的收集、处理和利用，完善保护机制，依法坚决打击各种形式的网络诈骗、侵犯知识产权、侵犯公民隐私等网络违法犯罪活动。督促企业加强数据安全风险评估，加强对大数据企业的监督管理和责任追究，打造安全可靠的数据生态环境。

强化网络安全应急处置能力。加强网络安全信息统筹机制、手段、平台建设，实时监测预警网络安全重大事件，既掌握网络空间当前状态，又分析下一步动态，为科学决策指挥提供依据。加强网络安全事件应急指挥能力建设，健全完善网络安全监测预警响应机制，提升网络安全态势感知、事件分析、追踪溯源以及遭受攻击后的快速恢复能力。

强化网络安全工作基础。大力发展网络安全产业，加强网络安全产业统筹规划和整体布局，培育扶持一批具有国际竞争力的网络安全企业。加强网络安全教育，加快推进国家网络安全人才与创新基地建设，积极开展一流网络安全学院建设示范项目。深入开展网络安全知识技能宣传普及，办好国家网络安全宣传周，不断提高广大人民群众网络安全意识和防护技能。

谋共赢，积极推动构建网络空间命运共同体

当前，网络空间国际治理进入深水区，单边主义和保护主义呈现蔓延趋势，网络空间国际规则的脆弱性凸显，对维护网络空间国际秩序产生不利影响。我们要与国际社会携起手来，积极推进全球网络空间治理体系变革，构建网络空间命运共同体，推动网络空间国际治理朝着更加公正合理的方向迈进。

加强习近平总书记国际治网理念宣传阐释。习近平总书记提出的推进全球互联网治理体系变革的“四项原则”和构建网络空间命运共同体的“五点主张”，反映了世界绝大多数国家特别是广大发展中国家的共同心声，赢得了国际社会广泛认同和支持，为全球互联网发展治理贡献了中国智慧和中国方案。要围绕“四项原则”、“五点主张”，加强理论研究、宣介阐释和国际传播，积极推动我治网理念成为国际共识、转化为国际规则。

积极参与网络空间国际治理进程。瞄准关键环节和前沿领域，主动参与网络空间国际规则制定。依托联合国互联网治理论坛、互联网名称与数字地址分配机构、世界经济论坛等平台，深度参与网络空间国际治理多边活动。推动亚太经合组织等框架下数字经济和网络安全合作，加强对网络空间国际治理的进程引导，共同构建和平、安全、开放、合作的网络空间。

广泛开展网络空间合作交流。巩固和推进网络空间交流合作，运筹好大国网络关系，深化同新兴市场国家、发展中国家网信合作交流。深入推进同“一带一路”沿线国家的数字经济和信息化建设合作，推动“一带一路”数字经济国际合作倡议落实。积极发展网络空间全球伙伴关系，推动数据资源有序流动、开放共享，打造覆盖全球、深度融合、互利共赢的合作新格局，让互联网发展的机遇和成果更多惠及世界各国人民。

新时代肩负新使命，新征程展现新作为。全国网信系统要更加紧密地团结在以习近平同志为核心的党中央周围，深入学习贯彻习近平新时代中国特色社会主义思想特别是关于网络强国的重要思想，坚持党对网信工作的全面领导，增强“四个意识”、坚定“四个自信”、坚决做到“两个维护”，巩固扩大“不忘初心、牢记使命”主题教育成果，坚定不移推进全面从严治党，坚持以政治建设为统领全面加强党的各项建设，坚决彻底肃清鲁炜流毒和恶劣影响，着力打造一支忠诚、干净、担当的网信铁军，高举旗帜、开拓进取、真抓实干、无私奉献，努力开创网络安全和信息化工作新局面，为实现“两个一百年”奋斗目标和中华民族伟大复兴的中国梦提供良好网络舆论环境、有力信息化支撑和可靠网络安全保障。（来源：本文系中共中央宣传部副部长，中央网络安全和信息化委员会办公室主任、国家互联网信息办公室主任庄荣文在《人民论坛》刊发的署名文章）

➢ 做好数据治理 更快更好地推进数字化转型

2019 年 12 月 1 日，由新华社瞭望智库、财经国家周刊主办的“第四届中国新金融高峰论坛 2019”在京举行，中国人民银行科技司司长李伟发表主旨演讲。他表示，当前，以人工智能、区块链等为代表的数字技术不断涌现，快速向经济社会各领域融合渗透，以数据为核心的数字化转型已是大势所趋；金融业是数据密集型行业，在生产经营过程中积累了海量的数据资源，只有做好数据治理，才能更快、更好地推进数字化转型。

数据治理之“困”

在谈到当前的数据治理之“困”时，李伟表示，主要有四方面：

第一，存在信息孤岛，有数不能用。当前，金融业数据治理过程中普遍存在“不愿、不敢、不能”共享的问题，导致海量数据散落在众多机构和信息系统中，形成一个个“数据烟囱”。一是不愿共享，多数机构都将数据作为战略性资源，认为拥有数据就拥有客户资源和市场竞争力，主观上不愿意共享数据；与之类似，机构内部数据权属分割，数据所有权和事权密切相关，部门宁愿将数据“束之高阁”，也不愿轻易拿出来共享。二是不敢共享，部分金融数据具有一定敏感性，涉及用户个人隐私、商业秘密甚至国家安全，数据共享可能存在法律风险，客观上给机构间共享数据带来障碍。三是不能共享，由于各机构数据接口不统一，不同机构的数据难以互联互通，严重阻碍数据开放共享，导致数据资产相互割裂、自成体系。

第二，数据质量不高，有数不好用。金融科技背景下，高质量数据成为金融服务与创新

的重要基础，也是大数据提升金融精准施策能力的关键前提。然而，当前金融业整体数据质量不高现象依然突出，给数据深入挖掘与高效应用带来困难。在完整准确性方面，由于缺乏统一的数据治理体系，有些金融机构在数据采集、存储、处理等环节可能存在不科学、不规范等问题，导致错误数据、异常数据、缺失数据等“脏数据”产生，无法确保数据的完整性和准确性。在一致性方面，由于业务条线繁杂、业务种类多样，多个部门往往数据采集标准不一、统计口径各异，同一数据源在不同部门的表述可能完全不同，看似相同的数据实际含义也可能大相径庭，数据一致性难以保障。这给全局数据建模、分析、运用造成障碍，数据挖掘效果大打折扣。

第三，融合应用困难，有数不会用。金融数据来源众多、体量庞大、结构各异、关系复杂。从如此繁杂的海量金融数据中挖掘高价值、关联性强的高质量数据，需要高效的信息技术支撑和可靠的基础设施保障。然而，部分金融机构科技研发投入相对不足、科技人员占比失调，利用数据建模分析解决实际问题的能力有待提高。信息资源利用大多停留在表面，数据应用尚不深入、应用领域相对较窄、数据与场景融合不够，导致数据之“沙”难以汇聚成“塔”，海量数据资源无法盘活，数据潜力得不到充分释放。

第四，治理体系缺失，有数不善用。我们常说，“技术本身是中性的，技术运用的善恶完全取决于人”，这一结论对数据同样适用。科技要向善，数据也同样要向善。然而，由于法律法规尚不健全、数据治理体系还不完善、机构合规意识不足，数据“不善用”的问题较为突出。从业机构违法违规成本低，为谋求商业利益而置现有管理规定于不顾，过度采集数据、违规使用数据、非法交易数据等问题屡见不鲜。例如，某些 APP、网站，用户不授权提供手机号、通讯录、地理位置等信息，就无法继续使用和浏览，通过“服务胁迫”来达成“数据绑架”。此外，部分机构数据保护意识、内部管理、技防能力薄弱，数据泄露事件时有发生，用户成为“透明人”，电信欺诈、骚扰电话、暴力催收等屡禁不止，严重侵害用户权益。

数据治理之“道”

面对上述困难和挑战，金融业如何解困破局、实现数据有序治理和高效利用，是需要共同探讨的重点议题。对此，李伟认为，数据治理应遵循四大基本原则。

首先，依法合规，保障安全。数据作为重要的生产要素，确保数据安全应是始终恪守的底线。金融业是对信息安全高度敏感的行业，应建立健全数据安全管理长效机制和防护措施，严防数据泄露、篡改、损毁与不当使用，依法依规保护数据主体隐私权在数据治理过程中不受侵害，不能因开展跨部门数据融合应用而突破现有法律法规与监管规则。

其次，物理分散，逻辑集中。由于历史原因，很多机构往往存在“N”个数据中心（数

据源），呈现出多个业务条线数据分散存储、分散运行的局面，若采用“推倒重来”的方式显然成本太高、阻力太大。因此，应在保持现有数据中心职能不变的前提下，维持当前数据物理存放位置和运行主体不变，充分利用各数据中心 IT 设施和人财资源，构建“1 个数据交换管理平台+N 个数据中心（数据源）”的数据架构格局。在此基础上，制定实施统一的数据管理规则，实现数据的集中管理。

再次，最小够用，用而不存。数据治理的一大难点就是如何在保障数据所有权基础上实现数据的融合应用。应消除数据所有方因信息“所有权让渡”造成“事权转移”的顾虑，规范数据使用行为，严控数据获取和应用范围，确保数据专事专用、最小够用、未经许可不得留存，杜绝数据被误用、滥用。在满足各方合理需求前提下，最大限度保障数据所有方权益，确保数据使用合规、范围可控。

最后，一数一源，一源多用。当前，无论是金融管理部门还是金融机构，各业务条线数据分散现象或多或少存在，数据多头收集时有发生。这不但增加信息报送、采集、存储成本，也导致数据责任主体不明，数据安全、数据质量难以保障。应明确源数据管理的唯一主体，保障数据完整性、准确性和一致性，减少重复收集造成的资源浪费和数据冗余。同时，建立数据规范共享机制，提升数据利用效率和应用水平，实现数据多向赋能。

数据治理之“术”

就如何做好数据治理工作，李伟也阐述了自己的四点意见。

其一，做好顶层设计，把数据规划好。数据治理是一项长期、复杂的系统工程，要在组织、机制和标准等方面加强统筹谋划。一是优化组织架构。充分认识数据的重要战略意义，将数据治理纳入企业中长期发展规划，及时调整组织架构，明确内部数据管理职责，理清数据权属关系，自上而下推动数据治理工作。二是完善应用机制。在保障各方数据所有权不变前提下，统筹规划全局数据架构，完善跨机构、跨领域数据融合应用机制，实现数据规范共享和高效应用。三是构建标准体系。建立涵盖金融数据采集、处理、使用等全流程的标准体系，打造金融数据的“通用语言”，提升金融数据质量，为数据互通、信息共享和业务协同奠定坚实基础。

其二，健全治理体系，把数据管理好。一是做好数据资产管理。根据统一的数据标准体系，建立全局数据模型和科学合理的数据架构。在此基础上，管理维护全局数据资产目录，实现对数据资产的全面梳理和有效管控，解决数据质量不高、数据利用不足等问题。二是做好数据分级管理。综合国家安全、公众权益、个人隐私和企业合法利益等因素，制定数据分级标准，基于全局数据资产目录将数据进行分级。针对不同等级数据采取差异化的控制措施，

实现数据精细化管理。三是做好数据共享管理。规范数据共享流程，确保数据使用方在依法合规、保障安全前提下，根据业务需要申请使用数据。数据所有方按规则审核确定数据使用范围、共享方式等，通过数据交换机制实现数据有序流转和安全应用。

其三，加强安全管控，把数据保护好。要遵循“用户授权、最小够用、全程防护”原则，充分评估潜在风险，把好安全关口，加强数据全生命周期安全管理，严防用户数据的泄露、篡改和滥用。在采集环节，要向被采集用户进行明示，明确告知采集和使用的目的、方式以及范围，在获取用户授权后方可采集。在存储环节，通过特征提取、标记化等技术将原始信息进行脱敏，并与关联性较高的敏感信息进行安全隔离、分散存储，严控访问权限，降低数据泄露风险。在使用环节，借助模型运算、多方安全计算等技术，在不归集、不共享原始数据前提下，仅向外提供脱敏后的计算结果。

其四，强化科技赋能，把数据应用好。数据治理的核心环节是数据应用，要从算力、算法、存储、网络等维度加强技术支撑，切实增强数据应用能力。在算力方面，加快分布式架构转型，充分发挥云计算等技术高性能、低成本、可扩展的优势，满足海量数据分析处理对计算资源的巨大需求。在算法方面，基于深度学习、神经网络等技术设计数据模型和分析算法，提升数据洞察能力和基于场景的数据挖掘能力，为数据插上翅膀，让数据在金融领域展翼翱翔。在存储方面，探索与互联网交易特征相适应、与金融信息安全要求相匹配的数据存储方案，稳步推动分布式数据库金融应用，实现数据高效存储和弹性扩展。在网络方面，运用物联网技术丰富数据采集维度，利用 5G 技术带宽大、速度快、延时低等优势提升数据流转效率，打造金融数据“高速公路”。

最后李伟说，当前金融科技蓬勃发展，金融业正处于以科技赋能实现大发展、大变革的关键时期。要深刻认识数据资源对金融业数字化转型的重要意义，切实把金融数据规划好、管理好、保护好、应用好，深挖数据价值、释放数据潜能，推动金融实现高质量发展。（来源：新华网 中国人民银行科技司司长李伟）

➢ 最高人民法院发布《中国法院的互联网司法》白皮书

2019 年 12 月 4 日上午，最高人民法院在浙江乌镇召开《中国法院的互联网司法》白皮书新闻发布会，发布《中国法院的互联网司法》白皮书。

各位记者朋友：

大家上午好！感谢各位出席这次新闻发布会，也特别感谢大家一直以来对人民法院司法改革工作的关注、支持和宣传。今天《中国法院的互联网司法》白皮书（以下简称《白皮书》）跟大家正式见面了，这是中国法院发布的首部互联网司法白皮书，也是世界范围内首部介绍互联网时代司法创新发展的白皮书。当前，人类社会进入了互联网时代，信息技术在深刻改变人们生产生活的同时，也给司法带来了前所未有的机遇和挑战。面对时代发展、技术进步、法治需求和群众期待，人民法院紧扣时代脉搏，立足国情实际，大力探索互联网时代司法新模式，推动信息技术与司法工作全方位深度融合，促进审判体系和审判能力现代化。

下面，我从三个方面介绍白皮书的基本情况。第一，什么是互联网司法，与我们通常所说的智慧法院建设有何区别与联系？第二，为什么选择在这个时间节点发布互联网司法白皮书？第三，白皮书的主要内容。

一、关于互联网司法的涵义与特征

习近平总书记指出，“没有信息化就没有现代化”“要善于运用互联网技术和信息化手段开展工作”。近年来，大数据、云计算、人工智能、区块链、5G 等信息技术飞速发展，既为人类认识世界、改造世界提供了新工具、新思维和新方法，也催生了许多具有新特点、体现新趋势的纠纷类型。

面对互联网发展的机遇和挑战，人民法院坚持以新应新、以变应变，积极拓展更深入、更便民、更高效的应用场景，推动实现全业务网上办理、全流程依法公开、全方位智能服务，这些技术应用和诉讼平台的健全完善，一般被统称为智慧法院建设，包括智慧审判、智慧执行、智慧服务、智慧管理等方面。

随着智慧法院建设加速推进，传统的审判流程从线下转移到线上，数据信息从纸面转移

到“云”上或“链”上，对应的立案、调解、送达、庭审、举证、质证等诉讼环节都发生了深刻变化，需要建立相应在线诉讼规则。与此同时，人民法院依法审理涉互联网的新类型案件，通过典型个案裁判确立了一系列治理规则。上述模式和规则的有机统一，就是我们所说的互联网司法。互联网司法大致包括三部分内容：第一，与互联网技术深度融合的审判模式。即传统审判流程在互联网上的升级改造、网络科技在司法场景中的融合锻造，如跨域立案、在线缴费、电子送达、区块链存证、智能类案推送等。第二，体现互联网特点的在线程序规则。即以在线诉讼为核心，构建一套电子诉讼规则和证据规则。例如，当事人不按时参加在线庭审的，根据规则如何处理；庭审中擅自退出的，对当事人会产生何种法律后果；电子送达适用范围、条件和效力，等等。第三，确立互联网依法治理的实体裁判规则。人民法院通过典型个案裁判，逐步确定网络空间行为规范、权利边界和责任体系，推进网络空间治理法治化，这些规则也为进一步完善相关立法提供了重要素材和参考。

总之，互联网司法与智慧法院既有联系又有所区别。互联网司法侧重机制创新、规则确立，智慧法院建设注重技术运用、平台搭建，二者相辅相成，都是互联网治理体系的重要组成部分。

二、关于《白皮书》的发布时间节点

2019 年是互联网诞生 50 周年，也是中国全功能接入互联网 25 周年。选择在这个时间节点发布中国法院的互联网司法白皮书，我想，主要有以下几点理由：

第一，制度框架初步建立。随着司法体制改革和智慧法院建设深入推进，互联网司法发展逐步体系化、制度化、规范化。“四五改革纲要”和“五五改革纲要”均将加强信息化建设，推进互联网技术与司法工作深度融合列入改革规划。近年来，人民法院针对互联网司法的机构设置、审理机制、技术标准、诉讼规则等，陆续制定出台一系列制度规范。目前，互联网司法制度的总体框架已初步搭建完成。

第二，规模效应初步形成。总体上看，互联网司法已从早期的单点突破、各自为战，转向顶层规划、整体推进。应用广度从单一领域向全方位拓展，探索主体从互联网法院向全国法院延伸，变革内容从数字化向网络化、智能化升级，工作重心从机制创新向规则确立演进。随着改革不断深入，互联网技术在司法领域的落地场景越来越多，与诉讼制度和审判模式实现了有机融合。

第三，改革成效逐步显现。经过 6 年的探索实践，互联网司法对于强化便民机制、提升审判效率、保障审判质量、破解执行难题、服务保障大局等方面的作用日益明显，也得到广大人民群众的认可。

综上，我们认为，现阶段有必要、有条件以白皮书形式，总结回顾中国互联网司法的创新举措和主要成效。

三、关于互联网司法白皮书的主要内容

《白皮书》为中英文双语版，中文全文约 1.6 万字，由前言、正文、结语、附录四部分组成，图文并茂地反映了中国法院互联网司法发展的基本路径、价值取向、主要举措和重要成果，具体有以下五个方面：

一是机构职能有创新，构建专业化审判体系。2017 年 8 月 18 日，我国设立全球首家互联网法院——杭州互联网法院；2018 年 9 月，又先后增设北京、广州互联网法院。设立互联网法院是互联网司法发展历程中具有里程碑意义的事件，开辟了互联网时代司法发展的全新路径，标志着我国互联网司法探索实践正式制度化、系统化。三家互联网法院利用自身组织优势、政策优势、技术优势和人才优势，充分发挥互联网司法“试验田”和“样板间”作用，在案件审理、平台建设、诉讼规则、技术运用、网络治理等方面，形成了一批可复制可推广的经验，取得显著成果。

在互联网法院建设不断深化的同时，我们也在全国范围布局推进互联网司法工作。天津、上海、湖北、江苏、四川、福建、贵州等地法院，结合辖区内互联网纠纷和互联网产业特点，积极组建互联网审判庭、合议庭或审判团队，科学设置组织机构、集中优质审判资源、合理确定受案范围，不断丰富互联网司法的实践样本，为构建我国互联网审判专业化体系奠定了良好基础。

二是司法裁判树规则，促进网络治理法治化。互联网法院利用管辖集中化、案件类型化、审理专业化的优势，审理了一批具有广泛社会影响和规则示范意义的案件。比如，北京互联网法院审理的全国首例“暗刷流量案”，有力打击网络黑色产业，保护公平竞争的网络营商环境；杭州互联网法院审理的全国首例大数据权属案，确立了数据资源确权、流通、交易的行为规范；广州互联网法院审理的“网络游戏著作权案”，回应了计算机软件生成内容是否具有著作权及如何保护等问题。

各地法院互联网审判庭或审判团队针对辖区互联网纠纷特点，在规范网络交易行为、界定网络平台责任、规制网络侵权行为、遏制互联网垄断和不正当竞争、维护个人信息安全、加强网络空间知识产权保护、打击网络刑事犯罪等方面，作出了一系列具有规则确立意义的判决，有力推动了互联网司法裁判规则体系的完善，有效发挥依法治网功能作用。此次，我们精心挑选了 10 个互联网审判典型案例，作为《白皮书》附录，以期为同类型互联网纠纷提供可借鉴的审判思路，也为社会公众依法维护自身合法权益，规范互联网从业者行为提供

指引，推动网络空间治理法治化。

三是诉讼规则作探索，推动建构现代化诉讼制度。互联网司法的深入发展是推动诉讼制度从工业化时代向信息化时代转型的强大动力。2018 年 9 月，最高人民法院制定印发《关于互联网法院审理案件的若干问题的规定》，有效明确了身份认证、在线立案、电子证据、在线庭审、电子送达、电子卷宗等在线诉讼规则，为完善在线诉讼程序和规则作出了有益探索。三家互联网法院和各地法院陆续制定出台诉讼规程、诉讼指南、审判手册等文件，细化在线审理规程、明确在线诉讼规范，有力推动在线诉讼规则体系逐步完善，实现互联网司法实践成果有效转化为程序规则和长效制度。

四是技术应用重实效，推动诉讼模式深层变革。互联网法院依托电子诉讼平台、有效实现起诉、调解、立案、举证、质证、庭审、宣判、送达、执行等诉讼环节全流程在线完成，大多数案件当事人足不出户即可完成诉讼，实现诉讼流程从“线下”到“线上”转变。2019 年 3 月，我们在 12 个省（区、市）开展“移动微法院”试点，依托微信小程序打造电子诉讼平台，将部分诉讼环节迁移到手机移动端办理，实现线上线下有机融合、无缝衔接，让当事人和法官充分感受到指尖诉讼、掌上办案的便利。截至 2019 年 10 月 31 日，移动微法院实名注册用户达 116 万人，注册律师 7.32 万人，在线开展诉讼活动达 314 万件。

各地法院广泛运用大数据、云计算、人工智能、区块链、物联网等前沿科技，全面推进信息技术在司法中的深度应用。在区块链领域，最高人民法院已建设“人民法院司法区块链统一平台”，完成超过 1.94 亿条数据上链存证固证，利用区块链技术分布式存储、防篡改的特点，有效保障证据的真实性，极大减轻法官认定证据的难度。在大数据领域，最高人民法院建设了人民法院大数据管理和服务平台，可以实时汇集全国 3507 个法院的审判执行、人事政务、研究信息等数据，2019 年 10 月 31 日，已汇集全国法院 1.925 亿案件数据，目前已成为全世界最大的审判信息资源库。在人工智能领域，各地法院积极开发了各类智能化审判辅助系统，不同程度实现案件繁简甄别分流、案件智能画像、庭审自动巡查、法条及类案精准推送、自动生成文书、文书瑕疵自动纠错、裁判风险偏离度预警等功能，成为法官办案和群众诉讼的有力辅助。

五是司法便民有突破，打造立体化诉讼服务。依托互联网覆盖面广、精准度高、信息传输快、交流渠道丰富等特点，我们大力推进“互联网+诉讼服务”，着力打造一站式多元解纷机制和一站式诉讼服务中心，推动形成线上线下相融合、诉讼与非诉讼解纷机制相衔接的诉讼服务体系。“一站式诉讼服务”依托线上诉讼平台和线下诉讼服务大厅，集成整合多项服务内容和多个服务渠道，能够集中办理跨域立案、多元解纷、诉讼咨询、信息查询、费用缴

纳、材料提交、涉诉信访等事项，实现当事人“最多跑一次”，甚至“一次都不用跑”。“一站式纠纷解决机制”以诉讼服务中心为平台载体，在线汇集人民调解、律师调解、行业调解、行政调解等多方解纷力量，为当事人提供多种解纷渠道和选择，多元调解成功的可以及时申请法院司法确认，调解不成功的可以迅速登记立案转入诉讼，解纷效率大大提升。“两个一站式”建设从根本上重塑了法院与当事人及社会公众之间的信息交流模式，真正让司法更便民、诉讼更亲民、解纷更高效。

以上五个方面反映了人民法院推进互联网司法的核心举措和主要成效，更多具体内容在《白皮书》有详细介绍，希望大家多多关注和宣传，《白皮书》中英文双语版可在最高人民法院官网、官微下载。

互联网司法作为新生事物，还处在不断生长和成熟过程中，它代表着未来司法发展的方向，标志着崭新司法纪元的开端。站在新一轮科技革命的时代潮头，人民法院将顺势而为、乘势而上，积极拥抱科技、大胆开拓创新，为推进网络强国战略，推动构建网络空间人类命运共同体，实现网络空间治理体系和治理能力现代化贡献更大力量。

我的介绍就到这里，谢谢大家。（来源：最高人民法院）

- **《中国法院互联网司法》白皮书**
- **全文：**http://wlf.court.gov.cn/upload/file/2019/12/03/11/40/20191203114024_87277.pdf

➢ 重要信息系统安全检查实施方法与技术措施

重要信息系统存储着海量的敏感数据和信息，承载着国计民生相关的核心业务，关系到国家安全、社会公共安全、人民群众根本利益，保障重要信息系统的安全运行是国家战略的重要组成部分。2003 年 9 月，《国家信息化领导小组关于加强信息安全保障工作的意见》对加强信息安全保障工作提出了“ 坚持积极防御、综合防范的方针，全面提高信息安全防护能力，重点保障基础信息网络和重要信息系统安全，创建安全健康的网络环境，保障和促进信息化发展，保护公众利益，维护国家安全” 的总体要求。2007 年 6 月，《信息安全等级保护管理办法》提出了“ 信息系统运营、使用单位及其主管部门应当定期对信息系统安全状况、安全保护制度及措施的落实情况进行安全检查。信息系统安全状况未达到安全保护等级要求的，运营、使用单位应当制定方案进行整改” 的具体要求。2017 年 6 月，《中华人民共和国网络安全法》正式实施，明确指出国家实行网络安全等级保护制度，对重要行业和领

域，在网络安全等级保护制度的基础上，实行重点保护。

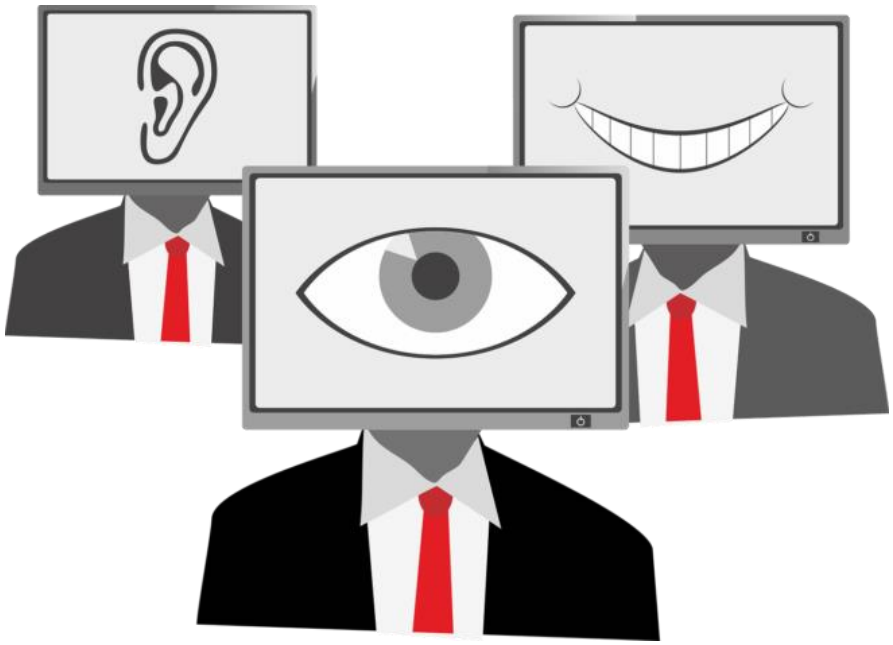
本文以落实国家等级保护制度为出发点，以等级保护安全检查为重心，提出开展等级保护安全检查工作的方法和措施。

一、安全检查规划

拥有重要信息系统的主管单位/责任单位，首先要根据等级保护制度的管理要求，对重要信息系统的安全检查进行规划，有针对性地制定安全检查方案，落实相应的岗位职责，周期性地开展安全检查工作。

安全检查是遵循等级保护的相关标准规范，对重要信息系统的安全管理和安全技术进行自我检测评估、查找隐患、堵塞漏洞、规范管理、完善措施、落实整改、通报情况的一项重要工作，由主管单位/责任单位自己组织检查。相对于等级保护测评的专业化操作，可适当降低技术难度，也可以委托专业安全测评机构协助检查。对于本单位的安全检查人员也可以制定相应的培训计划，提高其专业素质。

安全检查方法：包括人员访谈、文档查阅和技术检测。人员访谈是以交流、座谈和询问的方式了解掌握检查对象的总体安全规划、组织架构、岗位设置、建设管理、运维管理和应急保障等方面情况；文档查阅是以调阅和查看文档资料的方式了解掌握检查对象的安全规划、安全建设、安全运行、安全制度等相关工作过程记录和落实情况；技术检测是以现场人工查验和工具检测的方式了解掌握检查对象的安全配置、身份鉴别、访问控制、数据保护、安全审计、边界隔离等安全技术防护措施和系统的脆弱性、风险点等情况。



二、安全检查内容

安全检查内容应以等级保护基本要求国家标准为基础，结合本主管单位/责任单位的安全管理和安全技术的需要，制定符合自身系统特点、技术上可行的安全检查内容。通常可根据等级保护基本要求的分类方式编排检查内容，并形成文档，在检查内容列表中将相应的检查方法对应编写进去。

根据等级保护基本要求，安全检查内容可分为管理类和技术类两部分。管理类检查内容包括安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理；技术类检查内容包括安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心，以及新技术新应用方面的云计算、移动互联、工业控制、物联网、大数据等内容。

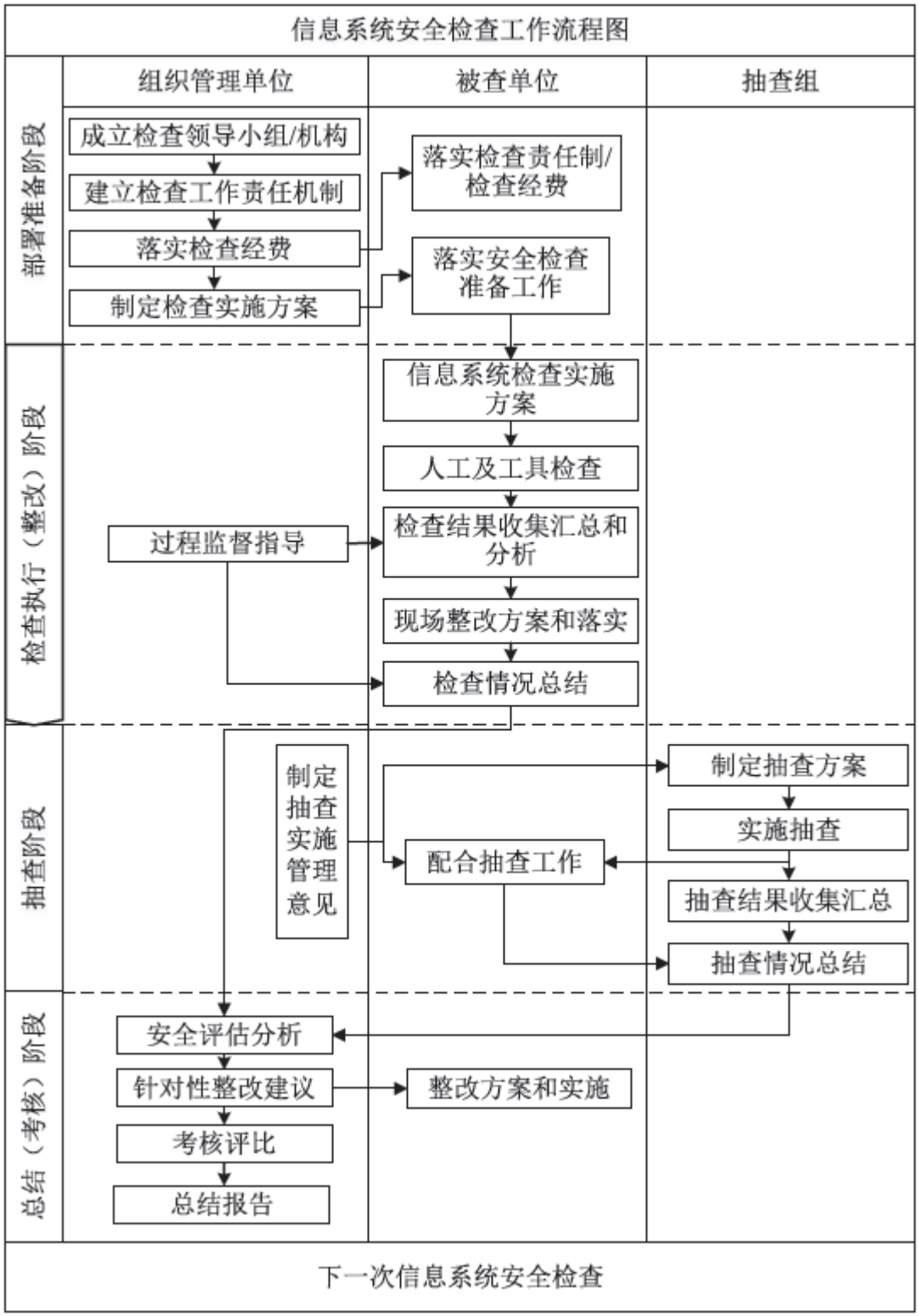
管理类检查：应重点关注安全管理工作的过程和执行情况，如网络安全员开展督促、检查和指导日常工作情况；网络安全工作计划和方案的落实情况；网络安全管理规章制度的执行情况；网络安全经费实际投入情况；参加网络安全技能培训情况；重要岗位网络安全和保密协议签订情况；安全事件处理过程及总结情况；安全通报的接收、发布等安全管理系统的基本运行情况；应急预案、演练和安全事件应急处置情况等。

技术类检查：应重点关注基本安全防护项和技术落实情况，同时关注对网络安全影响较大的专项。例如，检查网络边界安全防护的有效性，包括边界接入网络架构、业务系统接入、登记注册、安全防护强度等情况；检查外网接入情况，包括互联网访问日志分析、抗拒绝服务攻击、网页防篡改等；检查电子邮箱使用情况，包括非本部门人员特别是无关人员的使用情况等；检查计算机终端安全防护，包括集中安全管理措施、账户口令强度和更新情况；检查敏感信息的存储、传输和加密情况等。

安全检查工作可根据检查对象对新技术的使用情况，参照国标中的新技术扩展要求选择安全检查内容。

三、安全检查工作流程

安全检查工作可分为部署准备、检查执行（整改）、抽查和总结（考核）4 个阶段，涉及组织管理单位、被查单位、抽查组及相关人员。组织管理单位主要是主管单位/责任单位；被查单位主要是信息系统运行维护单位；抽查组由组织管理单位和信息系统运行维护单位临时组成，如果需要也可以协调专业测评机构参与。参与人员包括各级单位的安全管理员、参与现场检查的安全检查员，本单位的专业技术人员和受委托的第三方测评机构专业人员等。工作流程如图 1 所示。



信息系统等级保护安全检查工作流程

四、安全检查实施方法

安全检查工作分阶段实施。检查执行（整改）阶段中，对适合现场整改的项目可选择开展现场整改；抽查阶段可以根据安全检查的规模、覆盖区域和工作需要选择开展；总结（考

核）阶段中的考核可以根据工作需要选择开展。

4.1 部署准备阶段

4.1.1 部署准备阶段主要工作内容

1）成立安全检查领导机构。安全检查工作应包括主管单位/责任单位的所有重要信息系统，应建立统一的领导机构，负责安全检查工作的组织协调、指导、通报、总结和考评。

2）建立安全检查责任制。制定安全检查工作制度，责任到人。

3）制定安全检查方案。检查方案包括范围、内容、进度安排和要求等，其中检查内容可由主管单位/责任单位统一制定并下发执行，也可以统一要求，由系统运行维护单位自行制定。

4）配备安全检查工具。明确安全检查工具的类型及功能，可以制定相应的信息系统等级保护安全检查工具规范。

5）开展安全检查培训。制定培训计划，内容包括信息系统等级保护基本要求、安全检查实施方案、安全检查方法、安全检查工具使用、安全检查结果收集汇总上报等。

6）落实安全检查工作经费。主要用于安全检查培训、安全检查工具配备、专业网络安全机构服务等。

7）工作情况报告。可统一制定报告模版供信息系统运行维护单位遵照执行。

4.1.2 部署准备阶段各人员职责

1）主管单位/责任单位安全管理员。制定安全检查计划、方案和工作要求，组织、参加安全检查培训，检查所属信息系统运行维护单位对安全检查工作的准备情况。

2）信息系统运行维护单位安全管理员。组织、参加安全检查培训，填报本部门等级保护安全检查部署准备工作情况报告表。

3）安全检查员。参加安全检查培训，熟悉安全检查方法和安全检查工具的使用。

4.2 检查执行（整改）阶段

检查执行（整改）阶段工作是开展安全检查的核心工作，通过检查执行（整改）工作了解掌握信息系统的真实安全情况，发现信息系统存在的安全问题，采取相应的安全措施。

4.2.1 检查执行（整改）阶段主要工作内容

1）信息系统检查实施方案。根据信息系统的组成、结构和运行状态制定有针对性的安全检查实施方案，如果有统一下发的安全检查内容，则按照执行；如果需要自行制定检查内容，则根据等级保护相关标准和工作要求制定检查内容，再执行检查。

2）检查记录表单和工具准备。整理检查中可能用到的各类管理和技术文档，落实检查

工具，准备必要的软硬件条件。例如，安全检查员应准备好现场检查记录表单，安排系统管理员现场配合，准备部署检查工具的检查服务器、各类驱动程序等。

3）人工及工具检查。通过人员访谈、查阅文档和技术检查等多种方式对信息系统进行现场检查并记录检查结果。

4）检查结果收集汇总和分析。安全检查员对检查结果记录进行整理，可参照等级保护相关标准规范[5]对检查结果进行分析，有条件的可以建立自动化等级保护安全检查分析系统，最终形成安全检查报告。

5）现场整改方案制定和落实（选项）。根据安全检查结果数据，对于可以简单快速处理的安全问题，如通过安全配置、过滤、软件升级、重新授权等提高安全性的问题，可以及时制定方案进行整改。

6）检查情况总结。编写安全检查工作总结报告，应包括安全检查工作组织情况、安全检查内容、安全检查工作实施步骤、信息系统安全状况、安全检查发现的主要问题及对问题的整改情况等。

4.2.2 检查执行（整改）阶段各人员职责

1）主管单位/责任单位安全管理员。对信息系统运行维护单位开展的安全检查工作进行过程监督指导，对信息系统运行维护单位的分析报告和总结报告进行审核。

2）信息系统运行维护单位安全管理员。对本部门的安全检查结果和记录进行审核、汇总和分析，编写本单位的安全检查分析报告和检查情况总结报告。

3）安全检查员。负责现场具体安全检查工作实施，填写信息系统安全检查记录表。

4.3 抽查阶段（选项）

抽查阶段是开展安全检查工作的一个重要环节，是对整个安全检查工作成果的抽样考核。组织管理单位可以根据本主管单位/责任单位的实际情况选择是否开展抽查阶段的工作。

4.3.1 抽查阶段主要任务内容

1）成立抽查组。由组织管理单位制定抽查工作计划，包括抽查对象、抽查人员和抽查时间安排等，组织相关管理人员、技术人员成立抽查组。

2）制定抽查方案。抽查组根据抽查对象制定抽查方案，包括目的、内容、范围、时间安排、现场实施步骤及工作要求等内容。

3）实施抽查。抽查组依据抽查方案，通过人员访谈、查阅文档、人工检查、工具检查、在线检查等多种方式对抽查对象进行检查并记录结果。

4）分析总结及通报。抽查组对抽查结果进行汇总分析，编写抽查分析报告和总结报告，组织管理单位对提交的报告进行审核，同时形成最终的抽查分析总结报告，并对抽查结果进行通报。

4.3.2 抽查阶段各人员职责

1）组织管理单位。制定抽查计划，成立抽查组，对上报的文档资料进行审核，编写本主管单位/责任单位抽查分析报告和抽查工作总结报告，对抽查结果在本主管单位/责任单位内进行通报。

2）抽查组。制定抽查方案，准备抽查工具，对被抽查单位的信息系统进行安全检查，对抽查结果进行分析总结，编写本组的抽查分析报告和总结报告。

3）被抽查单位。准备抽查对象的管理和技术文档、软硬件设施，安排管理和技术人员配合抽查组开展工作。

4.4 总结（考核）阶段

在总结（考核）阶段，主管单位/责任单位对所属信息系统安全性进行综合评价。

4.4.1 总结（考核）阶段主要工作内容

1）结果数据汇总分析和通报。对所有安全检查和抽查结果进行汇总统计，分析信息系统存在的主要问题，对分析结果和问题进行通报。信息系统运行维护单位应制定相应的整改计划和实施方案进行整改。

2）安全检查考核。安全检查工作结束后，应对安全检查工作开展情况进行量化考核。考核内容包括安全检查工作完成情况、信息系统安全管理合规情况等。

3）安全评估和总结。编写信息系统安全检查报告，内容可包括安全检查工作的实施过

程、安全检查（含抽查）数据统计分析、安全问题分析、安全风险评估等。编制安全检查总结报告，内容包括组织部署情况、工作成效、工作措施、主要问题、下一步工作考虑、考核情况等。

4.4.2 总结（考核）阶段各人员职责

1）组织管理单位。汇总各单位、各部门安全检查的检查数据和抽查数据，对数据进行分析处理；对安全检查工作进行总结和考核；通报安全检查的工作情况和存在的问题，督导各部门各单位针对问题进行整改。

2）信息系统运行维护单位。根据安全检查、抽查所反映出的安全问题，有针对性地制定整改计划和实施方案，及时进行整改。

五、安全检查技术措施

对于有较多重要信息系统的主管单位/责任单位， 为便于开展信息系统安全检查工作，可以自建相关的安全检查管理平台和安全检查工具系统。

安全检查管理平台可部署在主管单位/责任单位的办公内网或专网上，管理平台具有信息系统注册管理、安全检查任务管理、用户权限管理、安全检查内容库、安全检查知识库、检查模板管理、通知通报管理、数据管理、统计分析、安全态势评估、工作考核管理等安全检查相关管理功能。安全检查管理平台可以采用集中部署方式，也可以采用分级部署方式。

安全检查工具系统是用于现场安全检查的一套管理和检测系统， 具有安全检查任务管理、检测工具管理、检查结果统计、安全状态分析、检查报告生成和数据接口管理等功能。安全检查工具系统可以与安全检查管理平台配合使用， 可以接受管理平台创建的安全检查任务、安全检查内容、安全检查方法（知识库），也可以将安全检查数据及统计分析结果上传到管理平台统一管理。安全检查工具系统配套使用的检测工具可预先配置相应的数据接口。检测工具可以根据安全检查的工作重心和工作方案选择使用，主要包括漏洞扫描类、敏感信息检测类、安全配置检查类、流量分析类等。

六、结束语

本文从重要信息系统安全保障的迫切需求出发， 依据国家等级保护相关政策和标准，以安全检查实践活动为基础， 提出了重要信息系统等级保护安全检查的工作方法、工作内容、工作流程、实施步骤和技术措施，为开展和部署重要信息系统的安全检查提供参考。（来源:《信息网络安全》 作者：郑国刚 公安部信息安全等级保护评估中心）

四、政府之声

➢ 教育部印发《高等院校管理服务类教育移动互联网应用专项治理行动方案》

2019 年 11 月 27 日，教育部印发《高等院校管理服务类教育移动互联网应用专项治理行动方案》（下称《方案》），要求各高校严控 app 数量，采集人脸等个人生物识别信息的教育 App 应组织伦理性、安全性论证；超半年未更新的 App 将被整合关停。

治理行动的对象为高等院校服务于学校教育教学和广大师生工作生活的管理服务类教育移动应用，包括学校自主开发、自主选用和上级部门要求使用的教育移动应用（以下简称“教育 App”）。方案要求，各高等院校应逐条对照、排查存在的问题，在 12 月 31 日前完成自查；2020 年 1 月 31 日前，教育部将开展重点抽查，针对问题较为严重或整改不力的学校将进行约谈、通报；2020 年 3 月 31 日前完成总结提升。


English | 微言教育

中华人民共和国教育部
Ministry of Education of the People's Republic of China

当前位置：首页 > 教育部司局机构 > 科学技术司

教育部网络安全和信息化领导小组办公室关于印发《高等院校管理服务类教育移动互联网应用专项治理行动方案》的通知

教技司〔2019〕265号

各省、自治区、直辖市教育厅（教委）、新疆生产建设兵团教育局，部属各高等学校：

《高等院校管理服务类教育移动互联网应用专项治理行动方案》已经教育部网络安全和信息化领导小组审定同意。现印发给你们，请认真贯彻落实。

高校 App 泛滥困扰师生

教育移动互联网应用给学生学习带来不少便利，但也让校园 App 泛滥现象成为社会关注的焦点。有不少学生反映说自己被 App 绑架了，特别是在高校，打热水用一个 App，跑步使用一个 App，连 WIFI 用一个，刷网课用一个，甚至湖南一所高校还爆出“扫码洗澡”的规定……让不少学生觉得“闹心”。

据悉，今年 3 月，教育部针对该问题开展了一次专项调研，抽取了一百所高校，了解教育 App 的应用情况。教育部科学技术司司长雷朝滋表示，从调研结果看，总体情况还是好的，89 所高校 App 数量都在 5 个以下；但确实也有少数高校开发引进的 App 超过了 20 个，

存在 App 泛滥问题，给师生造成了困扰。9 月 5 日，在教育部发布会上，对于高校 App 泛滥问题，雷朝滋回应新京报记者称，要严控学校 App 数量，不得擅自开发和选用 App。

教育部指出，《方案》的制定，就是为了切实整治高校因形式主义导致管理服务类教育移动互联网应用程序泛滥问题。

采集人脸等生物信息的 App 需经伦理论证

《方案》要求，各高校系统梳理本单位开发和选用的教育 App，形成名录并完成提供者和使用者备案工作。选用教育 App 应报职能部门审核同意，开发教育 App 应经职能部门立项。单位内设机构及所属单位不得擅自选用、开发未经审核、立项的教育 App。不得选用未完成提供者备案的教育 App。对要求统一使用和大范围采集个人信息的教育 App，应在履行立项和审核程序的基础上，充分征求用户意见，并经领导班子审定同意。《方案》还特别强调，采集人脸等个人生物识别信息的教育 App，应在上述要求基础上组织科学性、伦理性、安全性论证。

严控 App 数量 超半年未更新的 App 将被整合关停

《方案》指出，各高等院校应严格控制本单位管理服务类教育 App 的数量，统筹规划小程序、企业号等应用。据《方案》，面向公众提供服务的整合成一个应用；面向教职工提供管理服务的整合成一个应用；面向学生提供办事服务的整合成一个应用。此外，各高等院校应建立“一数一源”的数据共享制度，所有教育移动应用使用个人基本信息应从基础数据库中共享，不得向用户重复采集个人基本信息。《方案》还提出，建立教育 App 退出机制，超过半年未更新的教育 App 应予以整合、关停。（来源：新京报）

- **《高等院校管理服务类教育移动互联网 应用专项治理行动方案》的通知**
- **全文**：http://www.moe.gov.cn/s78/A16/s8213/A16_gggs/201911/t20191126_409694.html

➢ 三部门发布《网络音视频信息服务管理规定》

2019 年 11 月 29 日，国家互联网信息办公室、文化和旅游部、国家广播电视总局联合印发了《网络音视频信息服务管理规定》(以下简称“《规定》”)。国家互联网信息办公室有关负责人，就《规定》相关问题回答了记者的提问。

问：请您介绍一下《规定》出台的背景?

答：出台《规定》是促进网络音视频信息服务活动健康有序发展的需要。当前，网络音

视频信息服务迅速发展，用户规模不断壮大。有关数据显示，国内网络音视频行业正在持续高速发展，当前，我国网络音乐用户规模已达 6.08 亿，网络视频用户规模已达 7.59 亿。但与此同时，也带来了传播违法和不良信息、侵犯人民群众合法权益等风险隐患，特别是随着“深度伪造”等新技术新应用在网络音视频领域的运用，这些风险进一步集聚、放大，可能被利用从事危害国家安全、破坏社会稳定、扰乱社会秩序、侵犯他人合法权益等法律法规禁止的活动，造成政治安全风险和国家安全、公共安全风险，对社会稳定造成不良影响。

因此，亟需出台有针对性的管理规定，明确网络音视频信息服务提供者及其技术支持的主体的信息内容安全管理责任，规范网络音视频信息服务提供者关于利用深度学习、虚拟现实等新技术新应用的管理要求，为网络音视频信息服务及其相关技术的提供、使用、管理等提供有效的依据。

问：《规定》对网络音视频信息服务发展和管理提出了什么样的总体要求？

答：一是明确管理对象，界定了网络音视频信息服务、网络音视频信息服务提供者和网络音视频信息服务使用者的含义。二是明确管理机制，各级网信、文化和旅游、广播电视等部门依据各自职责开展网络音视频信息服务的监督管理工作。三是明确总体要求，网络音视频信息服务提供者和使用者应当坚持正确政治方向、舆论导向和价值取向。四是明确行业自律，国家鼓励和指导互联网行业组织加强行业自律，建立健全行业标准和行业准则。

问：为了更好地落实信息内容安全管理主体责任，《规定》对网络音视频信息服务提供者明确了哪些要求？

答：一是明确网络音视频信息服务提供者的资质要求，网络音视频信息服务提供者应当依法取得法律、行政法规规定的相关资质。二是明确信息内容安全管理主体责任要求，网络

音视频信息服务提供者应当建立健全用户注册、信息发布审核、信息安全管理等制度。三是明确真实身份信息认证要求，网络音视频信息服务提供者应当依照《中华人民共和国网络安全法》的规定对用户进行真实身份信息认证。四是明确信息安全要求，任何组织和个人不得利用网络音视频信息服务以及相关信息技术从事法律法规禁止的活动，侵害他人合法权益。

问：为了确保新技术新应用安全，维护人民群众合法权益，《规定》对基于深度学习、虚拟现实等的新技术新应用制作、发布、传播音视频信息明确了哪些要求？

答：一是明确安全评估要求，网络音视频信息服务提供者基于新技术新应用上线具有媒体属性或者社会动员功能的音视频信息服务，或者调整增设相关功能的，应当按照国家有关规定开展安全评估。二是明确标识要求和新闻信息管理要求，网络音视频信息服务提供者和网络音视频信息服务使用者利用新技术新应用制作、发布、传播非真实音视频信息的，应当以显著方式予以标识，不得利用新技术新应用制作、发布、传播虚假新闻信息。三是明确违法违规信息管理要求，网络音视频信息服务提供者应当部署应用违法违规音视频以及非真实音视频鉴别技术。四是明确辟谣要求，网络音视频信息服务提供者应当建立健全辟谣机制，及时采取辟谣措施。

问：为了更好地落实平台管理主体责任和技术支持的主体的安全义务，《规定》对网络音视频信息服务提供者及技术支持的主体明确了哪些要求？

答：一是明确签订协议要求，网络音视频信息服务提供者应当与网络音视频信息服务使用者签订服务协议，要求其遵守法律规定，对违反法律规定和服务协议的服务使用者依法依约采取相应的处置措施。二是明确受理投诉举报要求，网络音视频信息服务提供者应当设置便捷的投诉举报入口，及时受理并处理公众投诉举报。三是明确对技术支持主体的要求，为网络音视频信息服务提供技术支持的主体应当遵守相关法律法规规定和国家标准规范。

问：为了更好地落实《规定》，《规定》对相关部门开展监督检查提出了哪些要求？《规定》明确了哪些法律责任？

答：一是明确监督检查要求和执法协助要求，各级网信、文化和旅游、广播电视等部门应当建立日常监督检查和定期检查相结合的监督管理制度，网络音视频信息服务提供者应当配合监管部门开展执法工作。二是明确了法律责任，网络音视频信息服务提供者和网络音视频信息服务使用者违反本规定的，由网信、文化和旅游、广播电视等部门依照相关法律法规规定处理。（来源：中国网信网）

- **关于印发《网络音视频信息服务管理规定》的通知**
- **全文：**http://www.cac.gov.cn/2019-11/29/c_1576561820967678.htm

➢ 中国人民银行银保监会发布《系统重要性银行评估办法（征求意见稿）》

2019 年 11 月 26，为完善我国系统重要性金融机构监管框架，建立系统重要性银行评估与识别机制，人民银行会同银保监会起草了《系统重要性银行评估办法（征求意见稿）》（以下简称《评估办法》）。日前，正式向社会公开征求意见。

2008 年国际金融危机后，宏观审慎政策逐渐成为反思危机教训、完善金融监管体制的核心内容。其中，加强中央银行对系统重要性金融机构的监管是强化宏观审慎管理、维护金融稳定的重点领域。按照党中央、国务院决策部署，2018 年 11 月 27 日，人民银行与银保监会、证监会联合发布了《关于完善系统重要性金融机构监管的指导意见》（银发〔2018〕301 号文，以下简称《指导意见》），对我国系统重要性金融机构的识别、监管和处置作出了总体性的制度安排。《评估办法》作为《指导意见》的实施细则之一，是我国系统重要性银行认定的依据，也是对系统重要性银行提出附加监管要求、实施宏观审慎管理、建立特别处置机制的前提，符合我国金融监管体制改革的总体方向和要求。

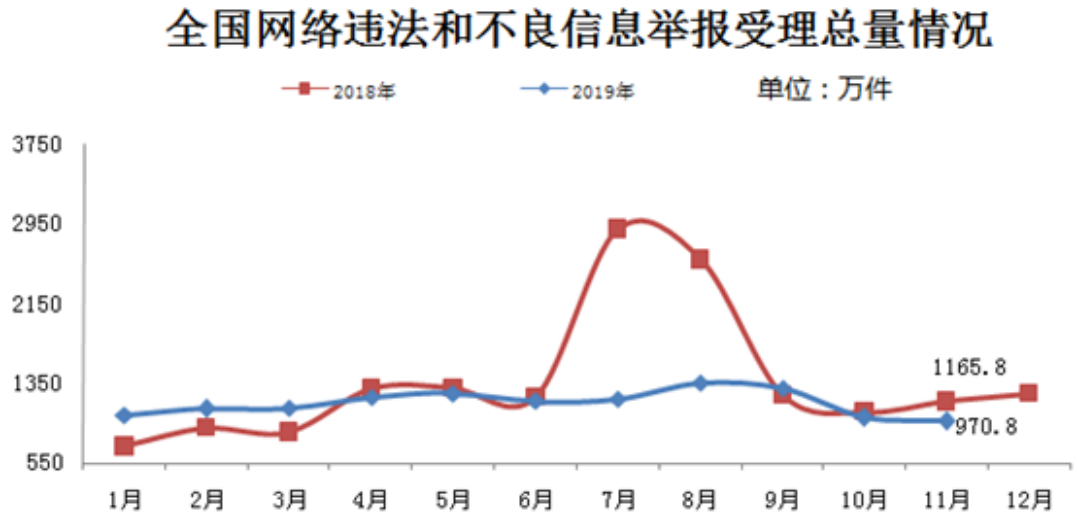
《评估办法》共四章、二十条，主要内容包括：一是确定评估目的和范围。识别出我国系统重要性银行，每年发布系统重要性银行名单，根据名单对系统重要性银行进行差异化监管，以降低其发生重大风险的可能性。二是确定评估流程。包括确定参评银行范围、向参评银行收集数据、计算系统重要性得分、进行监管判断、确定并公布名单。三是确定评估方法。采用定量评估指标计算参评银行的系统重要性得分，并结合其他定量和定性信息作出监管判断。定量评估的一级指标包括“规模”、“关联度”、“可替代性”和“复杂性”，指标权重均为 25%，每个一级指标下设若干二级指标。四是确定阈值和分组。得分达到一定分值的银行被纳入系统重要性银行初始名单，并对不同组别的银行实行差异化监管。五是明确任务分工。银保监会根据《评估办法》制作数据报送模板和数据填报说明，向参评银行收集数据并计算系统重要性得分。人民银行、银保监会可提出将得分低于 300 分的银行加入系统重要性银行名单的监管判断建议。名单提交金融委审议后，由人民银行、银保监会联合发布。

公开征求意见结束后，中国人民银行、银保监会将会同有关部门根据反馈意见进一步修改完善《评估办法》。（来源：人民银行）

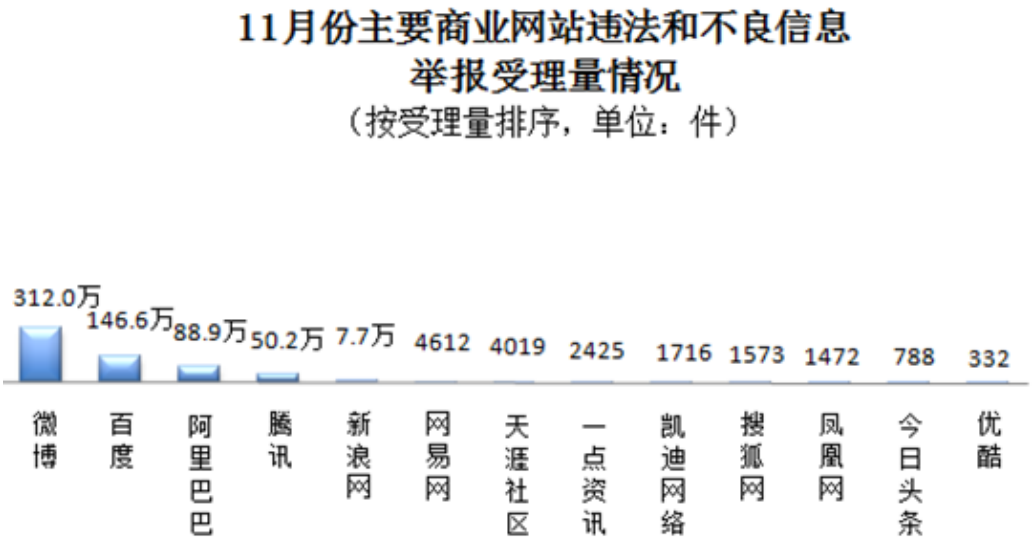
- **《系统重要性银行评估办法（征求意见稿）》**
- **全文：**http://www.pbc.gov.cn/tiaofasi/144941/144979/3928076/index.html

➢ 2019 年 11 月全国受理网络违法和不良信息举报 970.8 万件

2019 年 11 月 6 日，国家网信办举报中心通报 2019 年 11 月，全国各级网络举报部门受理举报 970.8 万件，环比下降 3.3%、同比下降 16.7%。其中，中央网信办（国家互联网信息办公室）违法和不良信息举报中心受理举报 14.1 万件，环比下降 8.9%、同比下降 51.5%；各地网信办举报部门受理 147.8 万件，环比增长 8.2%、同比下降 8.0%；全国主要网站受理 808.9 万件，环比下降 5.1%，同比下降 17.8%。



在全国主要网站受理的举报中，微博、百度、腾讯、阿里巴巴、新浪网等主要商业网站受理量占 75.0%，达 607.0 万件。



在各级网信部门指导下，目前全国各主要网站不断畅通举报渠道、受理处置网民举报。欢迎广大网民积极参与网络综合治理，共同维护清朗网络空间。（来源：国家网信办举报中心）

五、本期重要漏洞实例

➢ Google Chrome AppCache 安全限制绕过漏洞

发布日期：2019-11-25
更新日期：2019-12-05
受影响系统：
Google Chrome < 76.0.3809.87
描述：

CVE(CAN) ID: CVE-2019-5862
Google Chrome 是由 Google 开发的免费网页浏览器。
Google Chrome 76.0.3809.87 之前版本，在 AppCache 的数据验证中存在安全漏洞，远程攻击者通过构造的 HTML 页面，可能绕过站点隔离。
<*来源：vendor
*>
建议：

厂商补丁：
Google

目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载：
https://chromereleases.googleblog.com/2019/07/stable-channel-update-for-desktop_30.html

➢ Linux kernel 拒绝服务安全漏洞

发布日期：2019-11-30
更新日期：2019-12-03
受影响系统：
Linux kernel <= 5.4.1
描述：

CVE(CAN) ID: CVE-2019-19462
Linux kernel 是开源操作系统 Linux 所使用的内核。
Linux kernel 5.4.1 及之前版本，kernel/relay.c 文件的 relay_open 中存在安全漏洞。通过触发 alloc_percpu NULL 结果，本地攻击者可利用该漏洞造成拒绝服务。

<*来源：vendor
*>

建议：

厂商补丁：
Linux

目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载：
20191129013745.7168-1-dja@axtens.net/"
target="_blank">https://lore.kernel.org/lkml/20191129013745.7168-1-dja@axtens.net/
https://syzkaller-ppc64.appspot.com/bug?id=1c09906c83a8ea811a9e318c2a4f8e243becc6f8
https://syzkaller-ppc64.appspot.com/bug?id=b05b4d005191cc375cdf848c3d4d980308d50531
https://syzkaller.appspot.com/bug?id=e4265490d26d6c01cd9bc79dc915ef0a1bf15046
https://syzkaller.appspot.com/bug?id=f4d1cb4330bd3ddf4a628332b4285407b2eedd7b

➢ Huawei Honor Play 信息泄露漏洞

发布日期：2019-11-27
更新日期：2019-11-29
受影响系统：
Huawei Honor Play < 9.1.0.333(C00E333R1P1T8)
不受影响系统：
Huawei Honor Play 9.1.0.333(C00E333R1P1T8)
描述：

CVE(CAN) ID: CVE-2019-5309
Huawei Honor Play 信息泄露漏洞是一款智能音箱产品。
华为某些智能手机上存在一个信息泄露漏洞。攻击者在未解开屏幕锁的情况下，通过一系列操作之后，可查看手机上的某些信息。

<*来源：vendor
链接：https://www.huawei.com/cn/psirt/security-advisories/huawei-sa-20191127-02-smartphone-cn
*>

建议：

厂商补丁：
Huawei

Huawei 已经为此发布了一个安全公告（huawei-sa-20191127-02-smartphone）以及相应补丁:
huawei-sa-20191127-02-smartphone：涉及某些华为手机的信息泄露漏洞
链接：https://www.huawei.com/cn/psirt/security-advisories/huawei-sa-20191127-02-

smartphone-cn

➢ Cisco DNA Spaces:Connector 命令注入漏洞

发布日期：2019-11-20
更新日期：2019-11-22
受影响系统：
Cisco DNA Spaces: Connector < 2.0
描述：

CVE(CAN) ID: CVE-2019-15997
Cisco DNA Spaces 是一套室内定位服务平台。Cisco DNA Spaces:Connector 是其中的一个用于支持 Cisco 无线控制器通信的连接器。
Cisco DNA Spaces: Connector 2.0 之前版本，由于未对发送到特定 CLI 命令的参数进行充分的验证。本地攻击者可借助恶意的输入利用该漏洞在底层操作系统上以 root 权限执行任意命令。

<*来源：Cisco
*>

建议：

厂商补丁：
Cisco

目前厂商已经发布了升级补丁以修复这个安全问题，请到厂商的主页下载：
https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191120-dna-cmd-injection

六、本期网络安全事件

➢ 勒索软件渗透纽约警察局的指纹数据库 导致系统关闭

2019 年 11 月 27 日，据外媒 Softpedia 报道，在一个承包商连接到网络以配置数字显示器后，勒索软件感染了运行纽约警察局（NYPD）指纹数据库的计算机。该事件发生在 2018 年 10 月，导致 NYPD 在总共 23 台计算机上发现感染后，关闭了 LiveScan 指纹跟踪系统。但是，该部门官员声称该感染“从未执行”，这意味着勒索软件没有造成任何损害，但是 NYPD 出于谨慎考虑而决定使该系统关闭。NYPD 官员在接受《纽约邮报》采访时表示，该软件已重新安装在 200 台计算机上，并且指纹数据库于第二天早上恢复上线。NYPD 负责信息技术的副局长 Jessica Tisch 表示：“我们想深入了解这一点。对于我们来说，深入了解这一点真的很重要。到周六清晨—我记得它仍然尚未恢复—我们正在使系统上线。”

勒索软件通常会锁定文件的访问权限，直到受害者支付解密密钥的费用为止。当承包商插入他们用来配置数字显示器的 NUC 微型 PC 时，该勒索软件便感染了 NYPD 网络。NYPD 表示，他们确实对此事件对承包商提出了质疑，但未给予任何处罚。

此外，NYPD 声称其网络中只有约 0.1％的计算机受到了影响，而没有任何文件被锁定。该机构尚未共享有关感染背后的黑客团体，勒索软件和操作被感染设备的承包商的详细信息。

然而尽管 NYPD 已经避免了一场网络噩梦，但该部门网络中潜在的勒索软件感染可能会带来灾难性的影响。NYPD 数据库还连接到更大的州级别自动指纹识别系统，该系统拥有大约 700 万个文件，如果被勒索软件感染可能会被锁定，并且在恢复之前可能将使系统连续数天保持脱机状态。（来源：cnBeta）

➢ 五千多张人脸照片标价 10 元 “四要素”照片 4 元一份

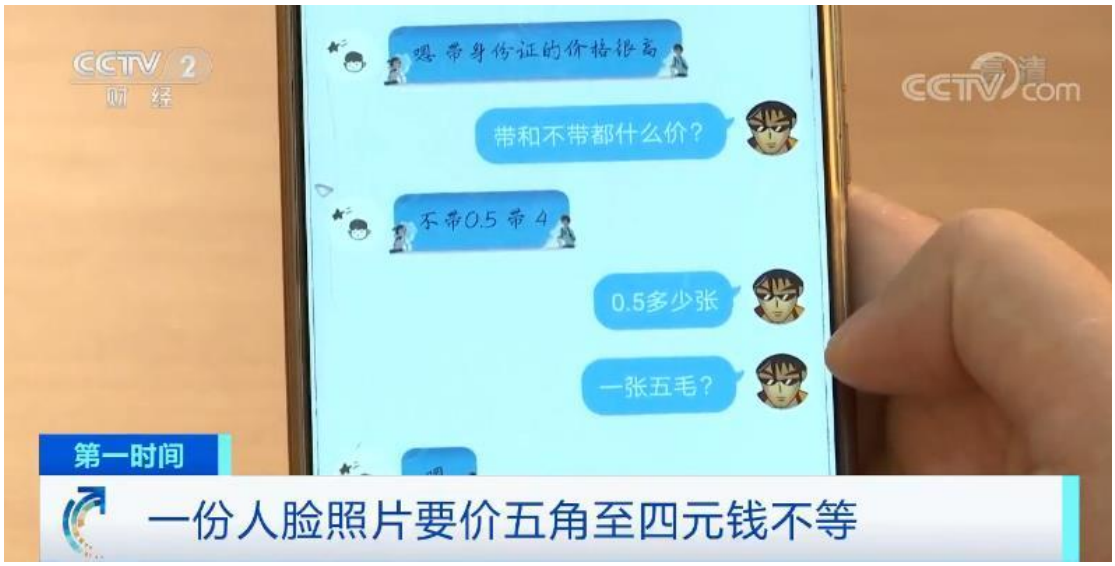
2019 年 12 月 1 日，随着人工智能和大数据的发展，人脸信息成为越来越重要的个人信息。它既可以用于刷脸支付，也可以用作安防准入等场景。不过，记者调查发现，就是这样对于每个人如此关键的数据信息，却在网上被公开兜售，而且价格低廉。

记者在互联网平台“转转”上以关键词“人脸数据集”搜索相关信息，迅速弹出了这样一件产品。商品名为“人脸相关算法训练数据集”，标价 10 元。记者打开商品介绍后看到，这个数据集包含五千多张人脸照片。很多还是一个人不同表情的脸部照片。

记者通过平台的聊天功能和销售者取得了联系。当记者询问销售者是否经过照片所有者的授权时，销售者表示，“经过授权的肯定不是这个价了”。就这样，没有经过照片所有人授权的人脸照片在互联网平台被公开兜售。

中国人民大学法学院副院长 杨东：非法交易的话对我们个人的隐私数据的侵犯是非常严重的。而且没有经过我们的允许。它会跟其它的一些个人的一些数据信息呀进行整合以后，非常精准地能够对人画像，从而从事非法的各种交易。

记者在百度一个名为“快眼”的贴吧，也发现有销售者在兜售人脸数据。记者联系到这位 qq 网名为“泯灭”的销售者，他告诉记者，不带身份证的大头照五毛钱一张，高清，还有一种是姓名、身份证照片、银行卡和手机号都有的，号称“四要素”，四块钱一份。记者了解到，这些数据可能被用于申请信用贷款，甚至注册公司，给泄露信息的用户，带来巨大损失。



多款 APP 无协议采集人脸数据信息

不仅仅是非法兜售，记者在调查中还发现，多款 APP 还存在着随意收集人脸数据信息的情况。

这款名为“人脸打分”的 APP，需要用户上传照片后，方能对用户的外表进行评价。但记者发现，这款 APP 却没有任何协议来确保用户上传的人脸照片不被滥用。而这款名为“证件照随拍”的 APP 同样如此。就这样，在没有任何使用协议的情况下，多款此种类型的 APP 在随意采集用户的人脸数据信息。

中国政法大学传播法研究中心副主任 朱巍：一个 APP 用户在使用的时候，按照我们国家关于 APP 的这种规定必须得有网民协议，这个网民协议（包括）搜集个人信息范围，内容使用的方式，以及删除的方式都必须做出具体的规定，这个显然是没有的。而且最重要一点用户没有办法控制使用用途。

记者还发现，有的 APP 对于用户的人脸数据信息采集过程中存在过度索取权利的问题。这款名为“颜值排行”的 APP 在使用条款里，就明确要求：“用户在任何时间段在 APP 发表的任何内容（包括自拍）的著作财产权，用户许可 APP 开发者在全世界范围内免费地、长期性地、不可撤销地、可分许可地和非首批地使用的权利。”使用的权利也包括多个方面，包

括但不限于复制权、发行权、出租权、展览权等。

中国政法大学传播法研究中心副主任 朱巍：就不管你把你这个图像、头像人脸识别的内容，用作什么内容你都不得干预，就相当于免费给它使用一样，而且不得撤回，所以这个是一个违反法律的规定，不管是按照消费者权益保护法还是按照网络安全法甚至按照合同法的规定，都已经严重违法了。（来源：央视网）

➢ 美商用短信服务商 TrueDialog 数据泄露 涉数千万条短信

2019 年 12 月 2 日，由美国企业短信服务提供商 TrueDialog 管理的一个包含有数千万条企业向潜在客户发送短信的数据库被泄露到网上。该数据库存储有 TrueDialog 客户数年来收发的短信，由于没有密码，数据也没有经过加密，任何人都可以获得该数据库内容。

TechCrunch 通过查看该数据库部分内容发现，数据库不但包含短信内容，还包含有电话号码。有的短信甚至包含大学的财务信息、带有折扣码的企业促销信息、以及双因素认证码和其他安全信息，用户的网络帐户可能因此被黑客访问。另外，数据库中还包含有 TrueDialog 客户的用户名和密码。

互联网时代，信息泄露可谓防不胜防。优衣库、万豪酒店、华住酒店等知名企业和品牌都曾发生程度不等的信息泄露事件。（来源：凤凰网科技）

➢ 8 人团伙被抓！安全技术人员变身黑客，专黑金融网站数据库

2019 年 12 月 4 日，从广州市公安局获悉，今年以来，广州警方严厉打击网络突出违法犯罪，强力整治网络违法有害信息，整改网络安全风险隐患，取得显著成效。侦破网络主侦案件 1500 余起，打掉团伙 224 个，依法刑事拘留犯罪嫌疑人 5313 名，缴获被泄露窃取买卖的公民个人信息 13 亿余条，极大地震慑了网络犯罪分子的嚣张气焰。

据了解，今年以来，广州警方发起侦破“净网”专案 7 次，参与全国专项集群战役 10 次，全链条打击黑客攻击破坏、侵犯公民个人信息等突出网络违法犯罪。

同时，对未履行网络职责和未落实网络安全技术措施和超范围采集公民个人信息的 266 个违法主体开展行政处罚，全面清理违法违规 APP，共下架 5.6 万余个违规恶意 APP。

此外，还全网域整治涉“黄赌毒”、涉枪爆刀、涉网络虚假信息等网络违法有害信息，今年共清理处置各类违法信息 10 万余条，封堵关闭网站 10192 个。对发布违法有害信息的网民及时予以处理，从源头上防范违法有害信息传播蔓延，共依法处理传播发布有害信息网民 592 人次，其中，教育训诫 567 人，行政处罚 23 人，刑事处罚 2 人。

典型案例网络安全技术人员竟成为“黑客”，专“黑”金融类网站

今年 2 月，广州市公安局网警支队通过对个别黑客攻击行为进行侦查分析，挖出一条指向某安全技术公司人员刘某的线索，其所在地为海珠区。

经侦查，这是一个“制售黑客程序工具—非法侵入、出售网站系统权限—非法获取数据—数据交易中介—数据使用者”的链条式团伙。该团伙成员有 8 人，其中黑客嫌疑人 2 人，侵犯公民信息嫌疑人 4 人，下游犯罪嫌疑人 2 人。而刘某涉嫌多种网络黑客犯罪行为，包括非法制作、提供黑客入侵扫描工具、买卖网站“后门”、非法获取系统数据库（“拖库”）和倒卖金融网站数据。

该团伙按照下家的需求，“量身定做”针对特定系统漏洞的黑客入侵工具。同时，利用

网络技术优势，非法入侵网络并获取网站“后门”权限，出售给下家客户。根据黑产市场的行情和下家的需求，多次拖取金融类网站（比如股票、基金、期货交易等）等具有高价值的数据库，出售给下家客户，1 个网站的数据卖到 10 几 20 万元。

此外，该团伙还层层转卖、非法流转公民信息数据。经侦查，这些数据多用于网络黑灰产或犯罪，最后的用途主要集中在“业务引流”、荐股诈骗、期货交易平台诈骗等网络黑灰产或犯罪的业务上。

在查清团伙组织架构和锁定相关犯罪证据后，今年 5 月，公安机关开展专案集中收网行动，一举摧毁上述团伙，抓获嫌疑人 8 人，涉案金额约 200 万元，查获金融类公民信息上千万条。此次全链条打掉该团伙，极大震慑了网络黑客、黑产犯罪群体。

其中涉嫌非法获取计算机信息系统数据罪的 2 名数据源头黑客，刘某是广州某安全技术公司员工，吕某是职业黑客，长期从事黑客活动并曾因黑客犯罪被判刑。据悉，刘某和吕某学历都不高，依靠网络论坛和自我摸索，掌握黑客技术后，专门研究网站的攻防漏洞。

警方提醒：针对黑客入侵，不要轻易点击他人在论坛、电子邮箱、聊天软件、手机短信中留下的链接；不轻易连接来历不明的 WIFI 网络；不轻易运行来历不明的软件，对不了解网页 ActiveX 控件与 JAVA 程序采取严防的态度；及时给电脑和手机系统加装补丁，安装安全软件，并保持更新；定期备份并删除重要资料，降低被侵入时的损害；没有文件共享需求的电脑，可关闭硬盘和文件夹共享。日常生活中，警惕收集个人信息的企业、个人或网站，一旦遇到侵权情况，及时记录相关信息，向有关部门提供有价值的线索。

为推广业务买卖、交换公民信息，缴获个人信息文稿达 1800 页

近年来，侵犯公民个人信息的犯罪活动日益猖獗，严重扰乱公民正常生活，甚至成为许多违法犯罪活动的上游犯罪。广州警方对公民个人信息的犯罪线索进行集中梳理，发现两个主要从事非法买卖、交换工商类公民信息团伙，其成员众多，分布在天河区、黄埔区等地。

经侦查，这两个团伙从事网上代运营的业务，团伙成员为满足业务推广的需要，通过加入 QQ 微信等交换、买卖资料的通讯群组，群内的都是全国各地、各行各业的从业人员或是专门从事买卖信息的人，通过在群里的交流，把自己整理的公民信息与有需要的人员买卖或者交换从而牟利。

公民个人信息种类繁多，包含公民身份信息、企业法人信息、工商注册信息、行业人员名册等信息。涉案人员每次买卖交换数据量均超 5000 条以上，有时甚至达十几万条，主要以微信转账的方式支付，购买 5000 条价格 1 万元。

今年 4 月，公安机关开展专案集中收网行动，一举摧毁上述团伙。现场抓获嫌疑人 124

人，扣押涉案手提电脑 17 台、台式电脑 8 台、手机 51 部及公民个人信息文稿 1800 页，折合信息约 100 万余条。经审讯，嫌疑人对非法获取公民个人信息的作案事实供认不讳。

警方提醒：任何在互联网上交换、买卖从而非法获得公民个人信息的行为，已构成涉嫌侵犯公民个人信息罪，需要承担经济损失和法律责任。请市民群众特别是掌握大量有价值信息的各行业从业人员，不要为蝇头小利而成为网络违法犯罪活动的工具。

QQ 群里发红包“赌博”？ 机器人软件操控后台

2018 年 12 月，天河区公安分局接到举报，有一个利用 QQ 群组开设赌场，以发红包“埋雷”的形式进行网络赌博的团伙。该团伙参赌人数多、红包数目多、金额大，初步估算涉案金额超 3000 万元，经初查是一个跨及 14 个省市，数十人组成的“开发推广—代理销售—开设赌场”全链条犯罪团伙。

通过深入排查，该赌博团伙开发一款名为“盛 X 面对面红包”的赌博机器人软件，并搭建 vps 服务器。该机器人软件通过图像比对及发送虚拟口令等方式，实现接收红包赌注，自动抢红包并统计抢包日志及金额，自动计数赔付，流水输赢情况查询、清屏，及踢出 QQ 群等操作。通过使用该款机器人软件，可以在短时间内聚集大量参赌人员在群里发送大量赌博红包，且金额不受限制。

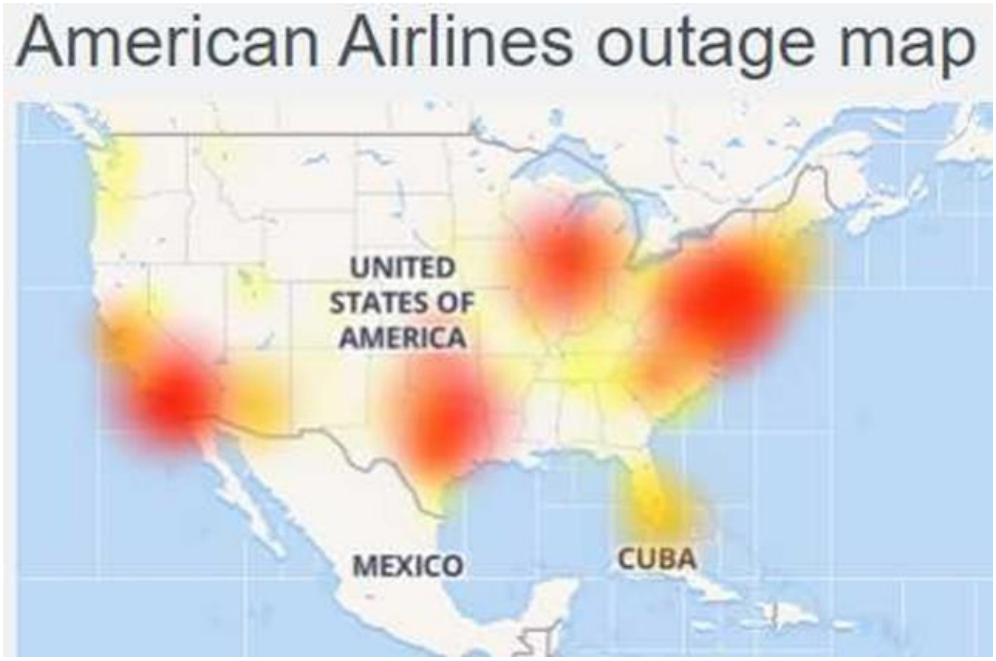
今年 7 月，公安机关在广州、惠州、中山、江西宜春等地统一收网，打掉这个开发推广、代理销售机器人软件并帮助开设 QQ 红包赌博群的犯罪团伙，共抓获犯罪嫌疑人 47 名，对软件开发人员、代理人员、开设赌场人员、参赌人员进行全链条打击。

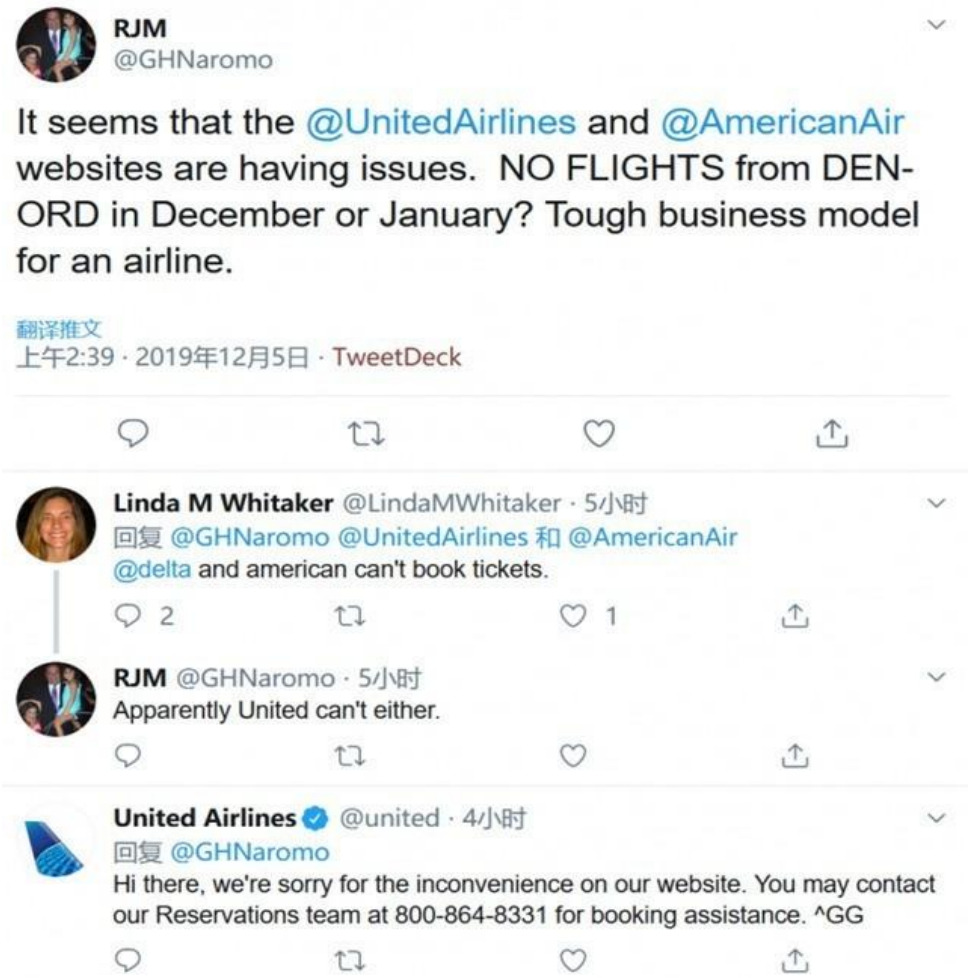
警方提醒：利用微信、QQ 等平台进行赌博属违法行为，开发售卖赌博软件、帮助他人搭建赌博平台性质更加恶劣，切勿以身试法。如发现相关赌博情况，请及时向公安机关举报。

（来源：广州日报）

➢ 谷歌技术故障导致美国三大航空公司网站短暂宕机

2019 年 12 月 5 日，由于谷歌提供的飞行数据软件发生技术故障，导致美国三大航空公司的网站周三短暂关闭。美国航空公司、达美航空公司和美国联合航空公司网站周三都遭遇宕机。





“我们的机票购买软件今天大约有 90 分钟出现故障，使我们的航空公司合作伙伴无法显示票价信息。我们现在已经解决了这个问题。”谷歌发言人在电子邮件中说。

美国航空在一份声明中表示，该问题并未影响其飞行运营。

从美国东部时间下午 1:30 开始，停运监视网站 DownDetector 显示的问题报告激增，然后逐渐减少，这些问题主要与网站有关。（来源：新浪科技）

➢ 两名俄罗斯黑客入侵美国银行系统，盗取 2100 万，遭 FBI 起诉

2019 年 12 月 5 日，美国联邦调查局（FBI）对两名俄罗斯公民正式提起诉讼，二人涉嫌谎称来自合法公司，通过网络钓鱼邮件，获得了进入美国银行电脑系统的权限。

据悉，这两名黑客分别为马克西姆和图拉舍夫，对美国的电脑系统发动了一系列攻击，而这一违法行为，使得二人净赚了 2100 多万人民币。检方称，马克西姆是黑客行动的主导者，而图拉舍夫是他的助手。目前二人均因在受侵者电脑上植入恶意软件，而获得美方指控。受到黑客攻击的地方，包括宾夕法尼亚州的一家银行、几家公司和该州的一个学区。二人在美国匹兹堡被起诉，但他们一直在俄罗斯生活。

原本被告的攻击目标是宾夕法尼亚州西部的沙伦市学区，但除此之外，他们曾成功地从一家石油公司的银行账户中调走了大量资金。

联邦检察官表示，除了宾夕法尼亚州的目标外，这两名黑客，还对其他地区的 11 个州发起了恶意软件攻击。总检察长助理布莱恩·本茨科夫斯基，在新闻发布会上表示，此次攻击是过去十年来，最严重的电脑黑客和银行欺诈计划之一。

他还补充说：“马克西姆是一个彻头彻尾的 21 世纪网络罪犯，他精心策划了这些如此大胆的犯罪计划，作案手法如此老练，如果不是这件事真实发生了，恐怕没人能想象得

到。”（来源：冰川思想库）

信息安全意识产品年服务

021-33663299