2024年全国网民网络安全感满意度

新技术挑战与网络安全

专题调查报告

发 起 单 位 ： 全国135家网络社会组织及相关机构（网安联）
联合发起单位： 全国228家网安联志愿服务机构及相关志愿服务团队
牵 头 单 位 ： 北京网络空间安全协会
承 办 单 位 ： 长扬科技（北京）股份有限公司

2024年10月

编制撰写人

李庄、宋杰、吴优

组委会欢迎有关研究机构合作，深入挖掘调查数据价值，有需要者请与组委会秘书处联系。

报告查询（总报告及区域、专题、行业报告）：

网络安全共建网：www.iscn.org.cn　　“网安联”公众号：

目录

一、调查背景及对象分析

1.1. 调查背景

2024 年是习近平总书记提出网络强国战略目标和总体国家安全观 10 周年，也是习近平总书记作出网络安全工作“四个坚持”重要指示 5 周年。 在习近平总书记关于网络强国的重要思想指引下，我国网络安全工作不断取得新进展，网络安全政策法规体系不断健全，网络安全工作体制机制日益完善，关键信息基础设施保护、数据安全管理、个人信息保护、新技术新应用风险防范等能力持续加强，电信网络诈骗防范治理持续走深走实，人民群众利益得到切实保护，网络空间环境大幅改善，为维护国家在网络空间的主权、安全和发展利益提供了坚实保障。具体可从以下三个维度总结：

一是网络与数据安全制度体系不断完善。国家高度重视网络安全，在逐步落实《网络安全法》、《数据安全法》、《个人信息安全保护法》和《关键信息基础设施安全保护条例》基础之上，不断出台和完善相关法律法规，构建网络安全政策法规体系的四梁八柱”。例如，2024 年 8 月 30 日国务院第 40 次常务会议通过《网络数据安全管理条例》，自 2025 年 1 月 1 日起施行。该条例旨在规范网络数据处理活动，保障网络数据安全，促进网络数据依法合理有效利用，保护个人、组织的合法权益，维护国家安全和公共利益。

二是我国网络安全技术创新投入持续增加，产业规模不断扩大。网络安全保险等新业态加快发展，产品体系逐步完善。2023 年我国网络安全产业规模达到约 2200 亿元，上市企业达 28 家，产业综合实力显著增强。工信部持续加强政策引领，出台促进网络安全产业发展的指导意见、行动计划等，并会同其他部门先后印发文件，促进数据安全产业发展，促进网络安全保险规范健康发展。网络安全产业园区和创新示范区加快建设，集聚效应和辐射效应逐步显现。此外，人工智能带来了更多的网络安全新挑战和安全防护新需求，同时也催生了网络安全新技术和新产品，这些都在持续拓展网络安全产业发展的新空间，网络安全产业已成为支撑培育新质生产力的重要载体。

三是网络安全人才培养体系逐步完善。2016 年六部门联合印发《关于加强网络安全学科建设和人才培养的意见》，推动开展网络安全学科专业和院系建设，创新网络安全人才培养机制。目前全国 90 余所高校设立网络安全学院，200 余

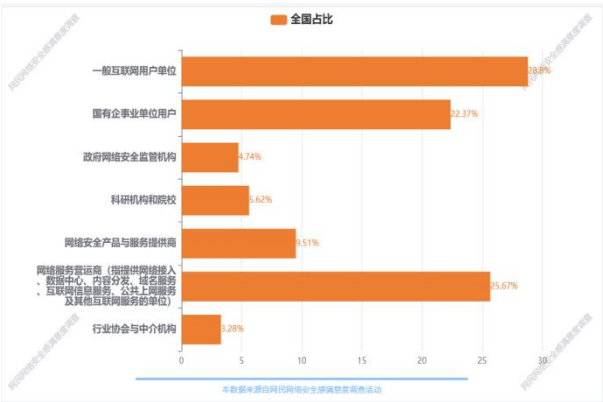
所高校设立网络安全本科专业，2024 年新一期一流网络安全学院建设示范项目高校名单公布，16 所高校入选。

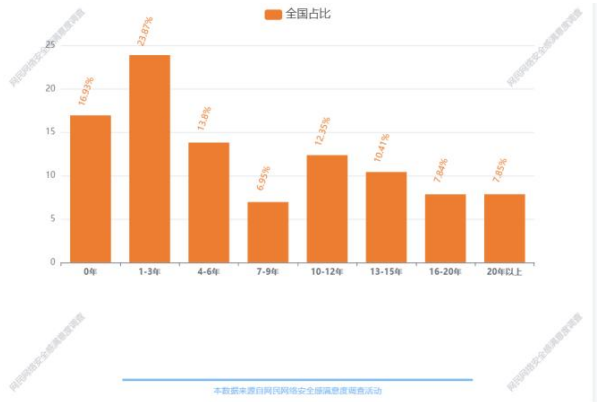
当下，我国在网络安全方面建设方面虽然取得了显著成效，但仍面临诸多挑战。尤其是随着物联网、人工智能、大数据、区块链、云计算等新一代信息技术的不断涌现，在为社会发展带来便利和发展机会同时，伴随的是黑客和恶意用户也找到了新的攻击手段。例如，物联网（IoT）设备的普及使得攻击者能够利用这些设备的漏洞进行攻击，甚至形成僵尸网络进行更大规模的恶意活动。云计算、大数据和人工智能导致的数据泄露、数据篡改和恶意软件等数据安全事件逐年递增等。由这些新技术而衍生的各种复杂网络安全问题，是网络安全建设战略规划及工作开展过程中需要解决的重点。

基于上述背景，特开展本次关于新技术挑战与网络安全专题调研活动，目的是通过调查和分析，了解新技术在网络安全领域的应用趋势和发展方向，从而制定更加有效的应对策略和措施，提升应对新技术挑战的能力。利用调查过程中收集到关于网络安全产业的市场需求、竞争格局和发展趋势等信息，为网络安全产业的发展提供有益的参考和指导，促进其健康发展。并基于调查结果，为我国新技术应用与网络安全保障提出可行性建议，促进网络安全的健康发展。

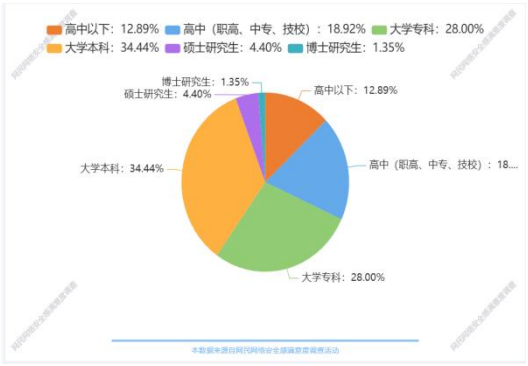
1.2. 调查对象分析

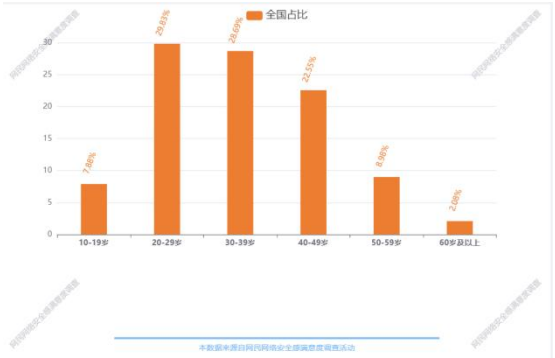
围绕网民网络安全感满意度调查—新技术挑战与网络安全专题，本次调研特选取了和网络安全强相关的从业人员，主要来自于互联网用户单位、网络服务营运商(指提供网络接入数据中心、内容分发、域名服务、互联网信息服务、公共上网服务及其他互联网服务的单位)、国有企事业单位用户、网络安全产品与服务提供商、政府网络安全监管机构、科研机构和院校、行业协会与中介机构，共计 59529 人。本次调研整体覆盖网络安全核心产业较为全面，专业性较高，其中83%人员为有相关经验从业者，从业时间跨度从 1 年到 20 年以上。





从本次调研对象学历结构来看，大专及本科以上学历占比达 68%，这与网安行业行业特点紧密相关。作为一个快速发展的新兴领域，要求其相关从业人员具有高度的专业性和综合性。同时，从业人员年龄梯队分布来看，以 20-49 岁的中青年为主，其中 20-29 岁阶段成为了行业的主力军。一方面是因为随着网络攻击事件的频发和网络安全意识的提高，企业对网络安全人才的需求不断增加，这为年轻人提供了更多的就业机会和发展空间。另一方面是因为政府对网络安全行业的支持力度不断加大，出台了一系列政策措施来推动行业的发展和人才的培养，人才是促进行业发展的基础，网络安全行业整体产业活力强。

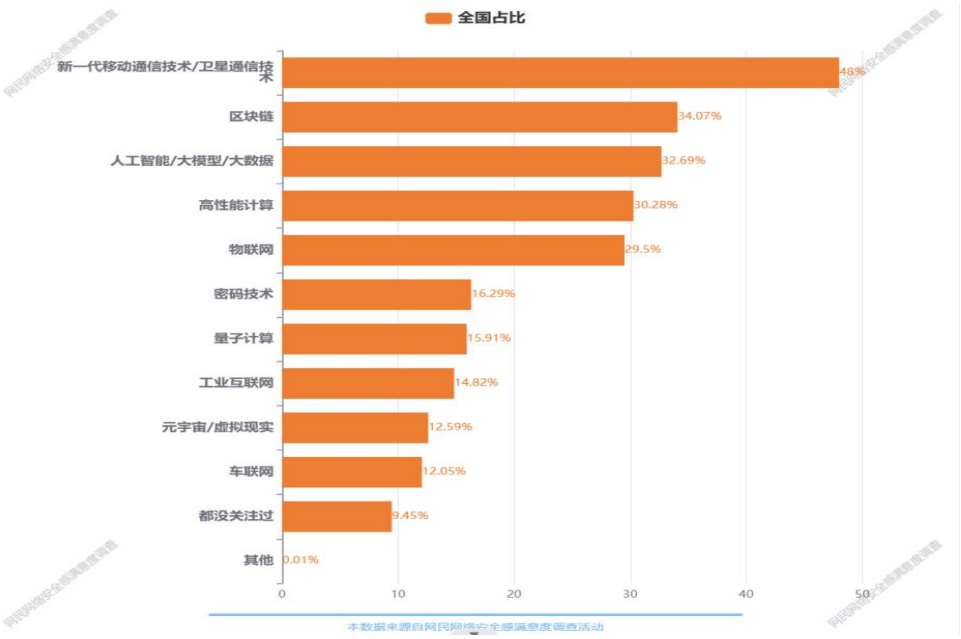




二、调查内容分析

2.1. 主要关注的新技术应用分析

本次活动共收回从业人员版网民网络安全感满意度调查问卷有效问卷 59529 份。经过对调查数据统计、分析后发现，针对目前新技术新应用的网络安全问题，呈现出以新一代移动通信技术/卫星通信技术方面为主，区块链、人工智能、大数据、高性能计算、物联网等其他新一代技术共同发展的趋势。新一代移动通信技术，特别是 5G 和即将到来的 6G 技术，具有更高的速度、更低的延迟和更大的容量的特点，能够支持更多并发用户和更丰富的多媒体应用。这些技术不仅推动了移动互联网的普及，还为人工智能（AI）、物联网（IoT）等新兴技术的发展提供了关键基础设施，作为当前科技发展的前沿领域，正引领着全球通信行业的变革。



2.2. 网安主要热点新技术方向

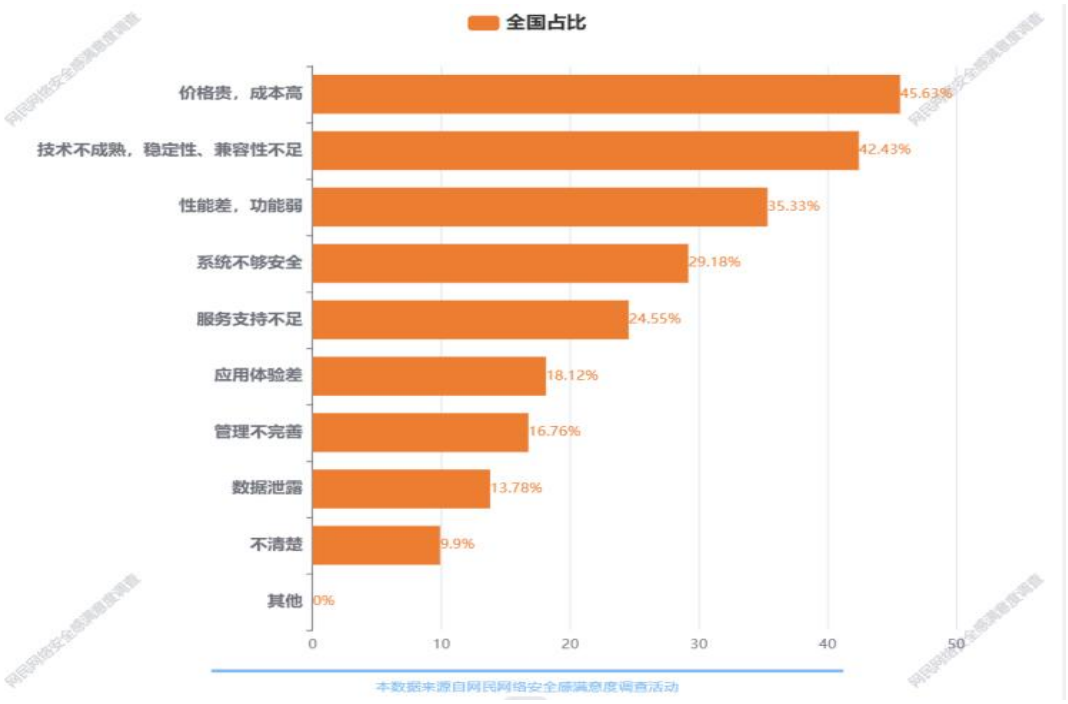
2.2.1. 信创安全

信创即信息技术应用创新，旨在针对硬件及云等基础设施、基础软件、应用软件、网络安全等 IT 产业链核心技术产品进行自主研发，为我国经济发展、社会运转构建安全可控的信息技术支撑，避免核心技术受制于人。信创建设从党政军局部起步，在应用实践中迭代产品性能，逐步扩展至金融、电信、电力等对国计民生有重要影响的关基行业。结合 2024 年受访者调研结果分析，信创目前存在主要问题依旧价格贵、成本高，极速不成熟、稳定性兼容性不足的问题。

信创本身属于本质安全的范畴，重点在于解决核心技术自主可控问题。从 2021 年，《“十四五”国家信息化规划》提出加快研发适应国内经济社会需要的核心技术产品，搭建适配认证平台并加快软硬件适配工作开始，经过 3 年的发展，信创基础软硬件的基本性能已满足日常办公所需。但是其核心部件，如芯片、操作系统、服务器等由于制作工艺、配套供应链、生态等方面的问题与国外技术依旧有较大差距，信创厂商面临产品开发技术难度大，产品适配、测试、验证工作细碎繁琐的双重难题。

综上所述，信创安全是国家发展的重要领域之一，对于保障国家信息安全、推动经济持续稳定增长和提升国家核心竞争力具有重要意义。应持续加强自主研发资源投入，突破核心技术瓶颈，提升信创产品的自主创新能力。同时完善供应

链安全管理，加强对开源软件的安全审查和评估，建立自主可控的供应链安全管理体系。



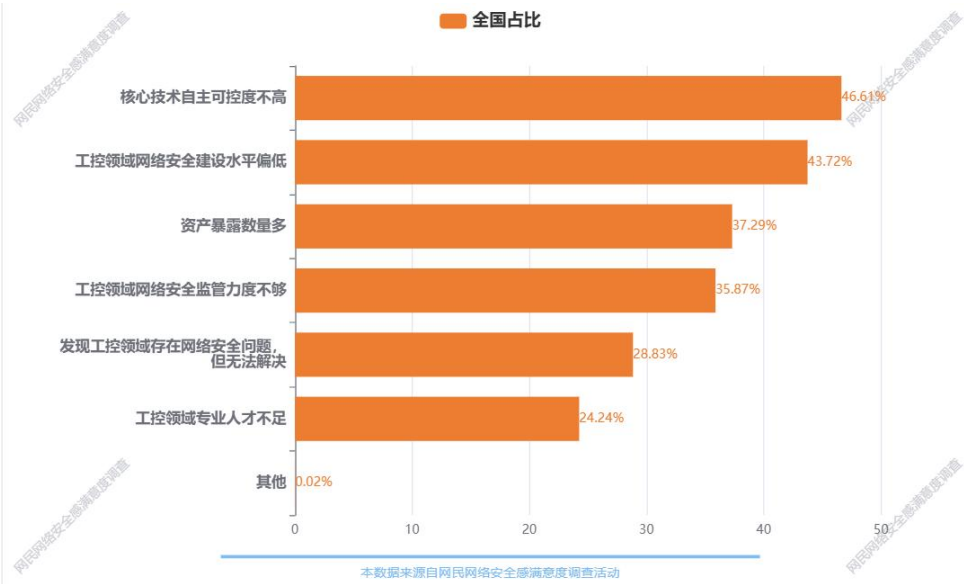
2.2.2. 工业控制系统安全

工业控制系统作为工业自动化控制的核心，其安全性直接关系到工业生产过程的正常运行，其中包括网络安全、通信安全、终端安全、数据安全、应用安全等方面。随着工业互联网、大数据、人工智能等新一代信息技术与制造技术的加速融合，数字化转型已成为企业提升竞争力的重要手段。然而，这种转型也带来了更多的安全风险，为了保障数字化转型的顺利进行、保护企业资产和数据安全、维护生产过程的稳定性和可靠性、防范新型安全威胁以及推动工业智能化和可持续发展，企业必须高度重视工业控制系统安全问题，并采取有效措施加强防护。

根据本次调研结果显示，46.6%的人员认为，当下我国工控安全发展存在核心技术技术自主可控度不高问题。还有 43.72%的人员认为我国工控领域网络安全建设水平偏低。回顾我国工控安全发展历程，在 2010 年之前，工控安全的概念在中国信息安全中是不存在的。2010 年 9 月，震网病毒事件，犹如一声惊雷，惊醒了中国政、产、学、研各界，“工业控制系统安全（Industry Control System Security）”开始进入大家的视野。当然，世界上多数国家也是从震网病毒事件开始有工业控制系统安全的意识。2011 年 10 月，工信部[2011]451 号文《关于

加强工业控制系统信息安全管理的通知》，是我国第一个关于工控安全的政府文件。经过过年发展，我国在工控安全行业也取得了不菲的成绩，目前在重要的工业行业，如电力、石油石化、轨道交通、水务、城市市政等关键信息基础设施行业领域，基于等级保护 2.0“同步建设、同步规划、同步使用”要求，工控安全防护产品已经成为新建项目的标配，存量项目则是处在逐步改造的过程。但是从全球来看，我国在工控安全领域起步依旧较晚，整体建设水平偏低的状态。

综上所述，我国工控安全行业要达到国际先进水平，仍就需要加强技术创新和产业升级，提升安全防护能力。同时，政府和企业还需要加强合作和信息共享，共同构建工控安全生态体系。此外，还需要加强人才培养和引进力度，提高工控安全领域的人才素质和数量。



2.2.3. 区块链安全

区块链技术作为一种分布式去中心化的技术，在无需第三方的情况下，使得未建立信任的交易双方可以达成交易。因此，区块链技术近年来也在金融，医疗，能源等多个行业得到了快速发展。然而，区块链为无信任的网络提供保障的同时，也面临着一些安全隐患。根据网络系统的安全需求，结合区块链的特点，区块链系统构建的基本安全目标是通过密码学和网络安全等技术手段，来保护区块链系统中的数据安全、共识安全、隐私保护、智能合约安全和内容安全，防止恶意攻击和数据篡改，确保区块链系统的顺利运行和数据安全。

根据调研结果显示，65.71%的人员了解区块链相关内容，其中还有 33.44%

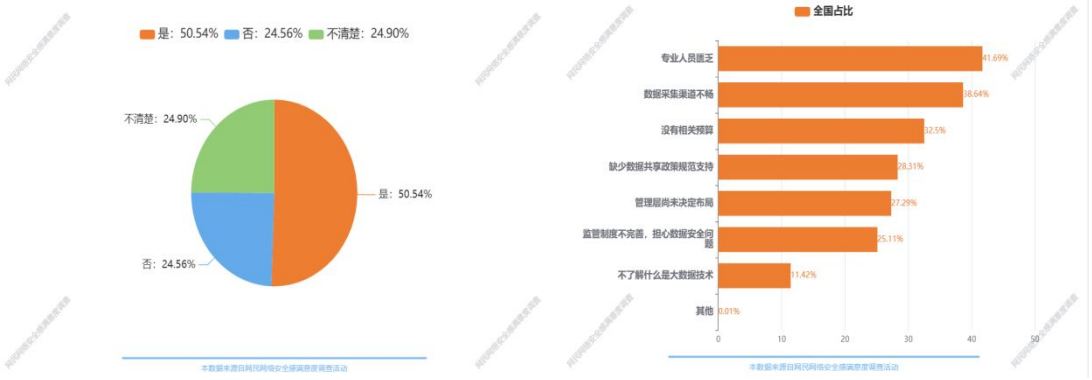
的人员非常了解或经常关注区块链相关资讯。由此可见，随着区块链技术的不断发展和应用深化，越来越多的企业、研究机构和行业相关人员已经关注或开始关注区块链技术的发展情况，正在推动区块链安全技术的创新和发展。但是区块链行业风风火火发展的同时，技术本身存在的共识安全薄弱、隐私泄露、系统漏洞等问题，阻碍区块链的发展。整体上来看，一方面应需要不断加强其安全技术的研究和应用，提高区块链系统的安全性和可靠性。另一方面也需要加强监管和人才培养等方面的工作，为区块链安全提供有力保障。同时，区块链当前主要场景还是在数字货币方面，要进一步推动其发展，还应加强在多个行业领域的应用场景的扩展。

2.2.4. 大数据安全

在数字经济快速发展的背景下，数据已成为企业和组织的重要资产，其安全性直接关系到企业的业务连续性、声誉和客户的信任。一旦数据泄露或被恶意利用，将对企业造成不可估量的损失。我国政府高度重视大数据应用的发展，出台了《“十四五”数字经济发展规划》和《“十四五”大数据产业发展规划》等文件推动其创新与应用，为大数据应用提供了有力的政策保障和支持，促进了大数据技术的研发与创新，推动了大数据在各行各业的广泛应用。结合调研结果也可以看到，超过 50%的人员所在的企业应用了大数据技术。

从目前大数据技术应用上存在的问题来看，大数据技术涉及多个复杂的系统和工具，如 Hadoop、Spark、Kafka 等，这些系统的配置、优化和维护需要专业的知识和技能。通过调研可以看到，41.69%的人员认为目前大数据技能的人才相对稀缺，这在一定程度上也限制了大数据技术的应用和发展。同时还有 38.64%的人员认为，目前数据采集渠道不畅也是大数据技术应用的重要难点，这是因为一些关键数据可能受到隐私保护、法律限制或商业保密的限制，数据的获取需要

耗费大量时间和资源。数据来源的多样性也导致数据质量参差不齐，数据在准确性、完整性和一致性等方面存在相应问题。总结来看，要充分发挥大数据技术的潜力，需要政府、企业和社会各界共同努力，加强技术研发、人才培养、法律法规建设等方面的工作。



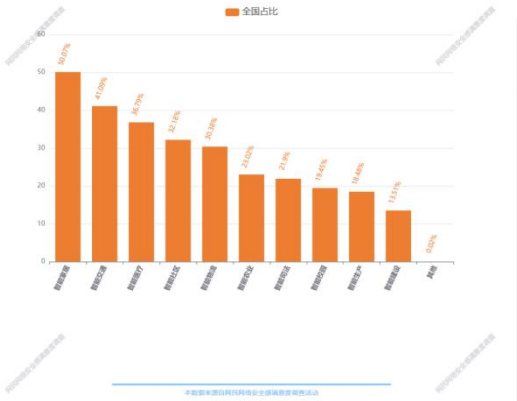
2.2.5. 物联网安全

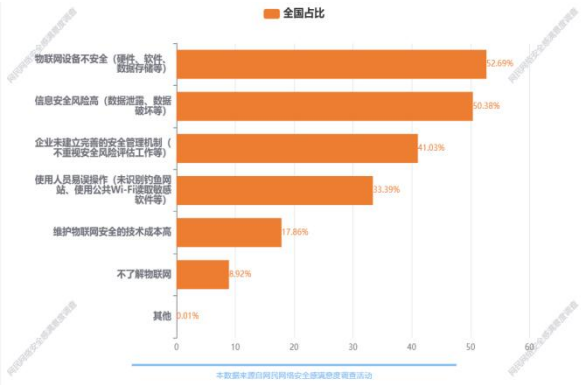
物联网通过互联网连接和控制各种物理设备的技术，使得这些设备能够自动化、智能化地运行、交互和管理。近年来，物联网应用已全面进入大众视野，各种以物联网技术为底层技术的应用呈现百花齐放局面，涵盖了家庭、城市、工业、农业、医疗等各个领域。例如智能家居，智能交通、智能农业、智慧医疗、智能社区、智能物流等，以及在工业中，物联网技术可以用于工业自动化、远程监控和故障诊断等多方面。结合调研可以发现，其中智能家居、智能交通和智能医疗位列前三，智能家居更是以整体占比 50.7%的比例位列榜首。

物联网作为连接物理世界与数字世界的纽带，其存在的安全挑战不容忽视。52.69%的人员认为，物联网安全风险主要存在物联网自身设备的不安全方面，包括硬件、软件、数据存储等。造成这种原因主要是因为物联网设备生态厂家众多，且种类繁多具有复杂性，产品安全防护策略难以统一，安全管理和安全防护的难度均比较大。另有 50.38%的认为其信息安全风险增高，包括数据泄露、数据破坏等风险较大。这主要是围绕数据处理过程中的安全风险和数据存储安全风险两方面。数据处理过程中的安全风险，即物联网设备收集大量数据并需要进行实时处理，数据处理过程中可能面临数据泄露、篡改或误操作等安全风险。数据存储安全风险，即物联网数据通常需要存储在云端或边缘设备上。这些存储介质可能面临黑客攻击、恶意软件等威胁，导致数据泄露或损坏。

综上所述来看，提高物联网的安全性需要从多个方面入手，例如提高设备的

安全性、加强生态系统的安全性、提升用户和企业的安全意识、制定统一的安全监管和标准以及应对特定的安全威胁等。

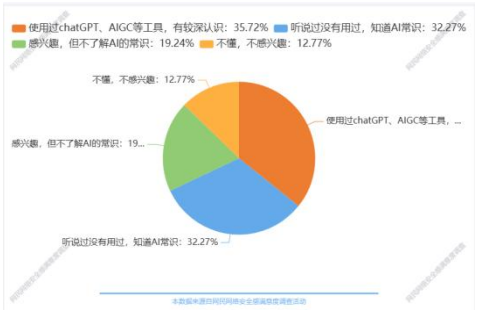


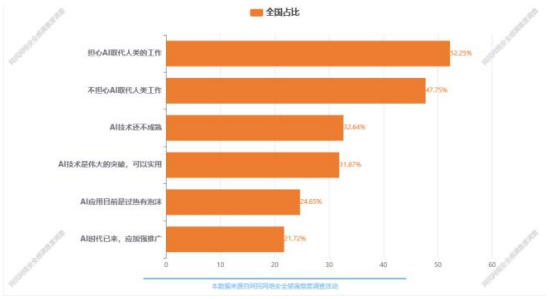


2.3. 人工智能（AI）新技术与网络安全

2.3.1.人工智能（AI）发展现状

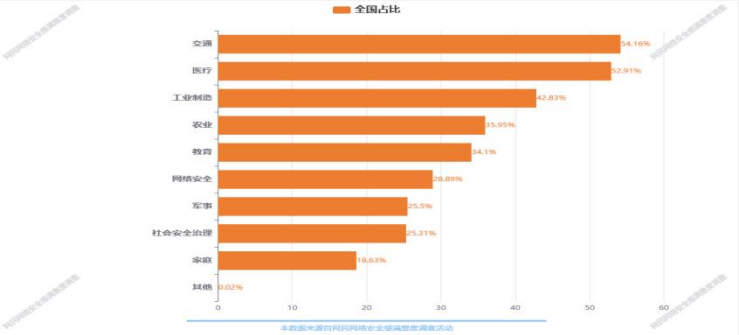
随着科技的飞速发展，人工智能（AI）已经成为了当今社会的热门话题，从自动驾驶汽车到智能家居，从虚拟助手到机器人，人工智能（AI）的发展现状呈现出蓬勃发展的态势。2022年ChatGPT的横空出世，在人工智能领域掀起了重要变革，这一智能工具因其解放人类生产力的潜力，从使用者到投资者，引起了各界的广泛关注，再次将人工智能（AI）推向大众视野。在本次受访人员中，87.23%的人员听过人工智能并对此感兴趣。35.72%的人员使用过ChatGPT、AIGC等工具，这说明人工智能已经渗透到了我们生活的方方面面。部分受访者在调研时也表示担心担心人工智能（AI）会是取代人类工作，但是整体上来看，对其的认可度还是较高，31.87%的人员认为AI技术是伟大的突破，可以使用，还有21.72%认为AI时代已来，应加强推广。





人工智能（AI）的应用现状非常广泛，涵盖了包括制造业、医疗保健、金融、农业众多行业和领域。对于期待人工智能（AI）在哪些领域发挥优势，主要还是集中在交通、医疗、工业制造和农业等，未来这些相关行业及产业或将会是人工

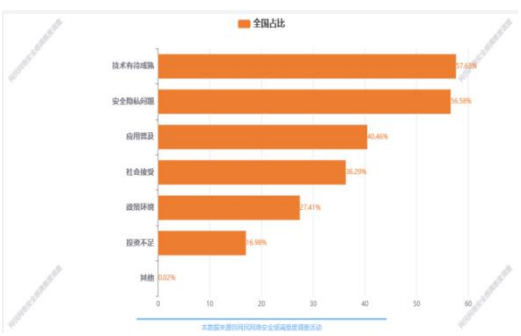
智能（AI）发展的下一风口。其中值得留意的是，还有 28.89%对人工智能（AI）在网络安全行业领域发展比较关注，人工智能（AI）有望为网络安全行业带来革命性的变革。总结来看，人工智能（AI）的普及和应用不仅提高了生产效率，还促进了各行业的数字化转型和创新发展。

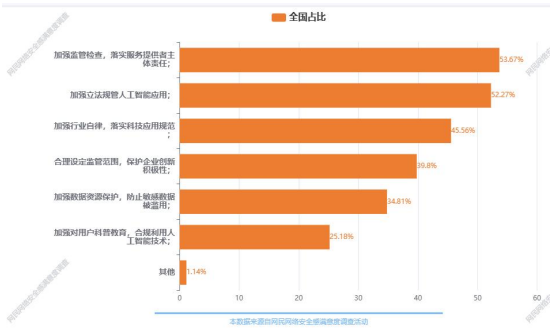


2.3.2. 人工智能（AI）网络安全影响

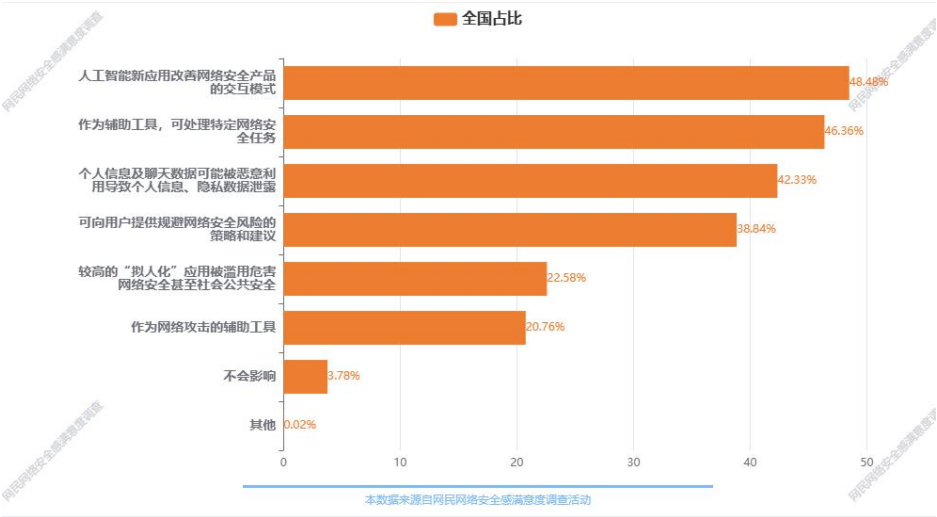
作为信息社会的革命性技术，人工智能（AI）可谓智能化信息社会的核心技术，具有广泛的应用前景。在带来诸多便利的同时，也伴随着一系列发展障碍和安全隐患。57.63%的人员认为目前人工智能应用的发展面临的主要障碍是技术有待成熟，57.58%的认为人工智能带来的安全隐私问题。这是由于人工智能（AI）依赖于大量数据进行训练和学习，如果数据的数量不足或质量不高，可能无法准确反映现实世界的真实情况，加上算法具有复杂的计算过程和内部逻辑，学习模型出现失误，将导致 AI 的决策和判断出现偏差。同时，人工智能在采集、使用和分析海量数据的过程中，可能涉及个人隐私信息的泄露、数据篡改等风险。特别是当这些数据包含国家秘密、个人敏感信息等时，一旦被黑客窃取或系统遭受攻击，将对数据安全构成严重威胁，影响个人利益，严重还可能对整个社会造成严重影响。

综上所述，在推进人工智能行业领域应用的同时，应对其发展当中可能存在的安全问题予以高度重视，在确保技术的安全性和有效性，提升人工智能的安全性和可靠性的同时，加快制定和完善人工智能（AI）相关法律法规，加强监管，明确 AI 技术的使用范围、权限和责任归属，为 AI 技术的发展提供法治保障。加大对 AI 技术滥用行为的打击力度，维护社会稳定和个人权益。

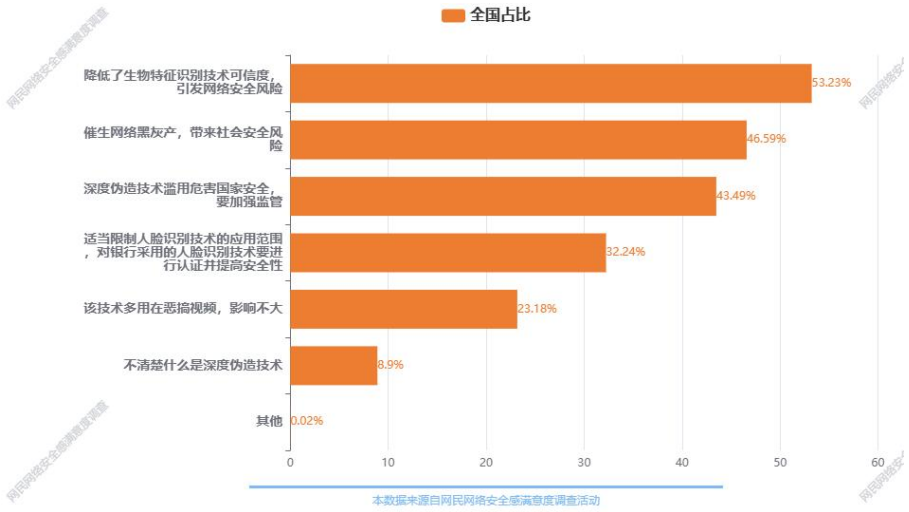




聊天机器人程序是人工智能的典型应用。爆火的聊天工具如 ChatGPT 更是一种革命性的人工智能语言模型。对于其对网络安全带来的影响，48.48%的人员认为人工智能应用改善网络安全产品交互模式，46.36%的人员认为作为辅助工具，可处理特定网络安全任务。人工智能（AI）具备强大的数据分析能力，能够分析海量网络流量数据，识别异常模式并迅速响应，如基于机器学习的入侵检测系统可以自动识别未知威胁，并在其造成损害之前采取应对措施。这种自动化响应不仅提高了防御效率，还减少了对人工干预的依赖。人工智能（AI）系统还能够对网络活动进行实时监控，识别潜在威胁并预测其发展趋势。通过分析历史数据和当前态势，AI 可以提前洞察潜在攻击，实施预防措施。通过不断学习和优化模型，人工智能将在网络安全产品和网络安全建设工作中起到重要作用。人工智能具有强大的文本生成能力的同时，这意味着它也可以被用于生成恶意软件、暗网站点和其他网络攻击工具。故在使用 ChatGPT 等人工智能聊天工具时，应采用加密技术、访问控制等安全措施来保护敏感数据不被泄露或滥用，保证用户数据的安全性和隐私性。政府层面应加强对人工智能技术的监管力度，制定相关法律法规和标准来规范其使用和发展。



近两年出现了 AIGC 和“AI 换脸”应用，对于这种以“深度伪造”为代表的新技术新应用，本次受访人员也提出了自己的观点。AIGC 即人工智能生成内容，是利用人工智能技术来创作生成文字、图片、音频、视频等内容的方式。而“AI 换脸”则是深度伪造技术在图像和视频领域的一种应用，它利用深度学习、虚拟现实等生成合成类算法对图像进行分析和处理，从而实现对人脸的替换和伪造。52.32%的人员认为这种新技术降低了生物特征识别技术可信度，46.59%的人员认为可能引发网络安全风险，催生网络黑灰产，带来社会安全风险，还有 43.49%人员认为深度伪造技术滥用危害国家安全，要加强监管。由此可见，大部分人员对“深度伪造”技术带来安全风险问题比较慎重和关注。未来，应加大深度伪造检测技术的研发力度，提高检测的准确度和稳定性。同时其核心相关的在数据安全、身份安全等网络安全技术也需要同步进行发展，用更安全和可靠的生物特征识别技术，将身份、行为、数据和业务深度关联，形成安全防御体系。

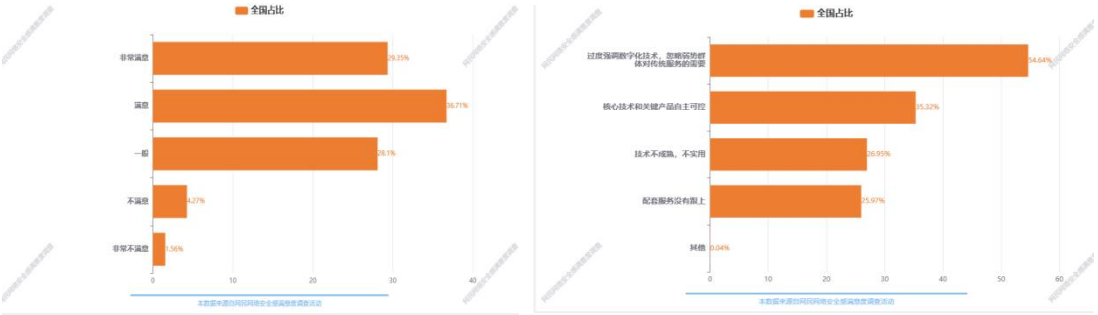


2.4. 数字政府与智慧城市安全

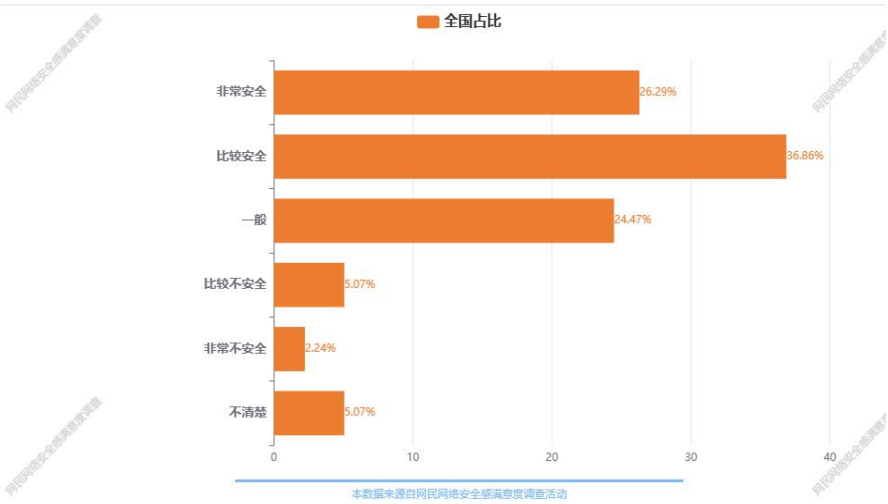
我国数字政府和智慧城市均处于快速发展阶段，数字政府和智慧城市中新技术的应用包括大数据技术、5G 技术、区块链技术、人工智能技术、物联网技术、云计算计算等。关于数字政府和智慧城市中新技术的应用效果评价，本次调研 36.71%人员认为满意，还有 29.35%的人员认为非常满意。但是数字政府和智慧城市新技术应用还是存在具体的问题。如 54.64%的人员认为数字政府和智慧城市新技术应用过度强调数字化技术，忽略弱势群体对传统服务的需要。弱势群体通常指老年人、低收入者、失业者、残疾人等在社会经济中处于不利地位的人群，

他们可能因经济、教育、身体等原因无法适应或接入数字化服务，可能存在进错失政府提供的福利和机会的情况。

未来，数字政府在推进过程中应充分考虑弱势群体的需求，平衡数字化与传统服务的关系。通过加强数字基础设施建设、优化数字政府服务、建立多方参与的支持体系、加强数字素养教育和完善法律法规等措施，确保弱势群体能够平等地享受政府提供的各项服务。

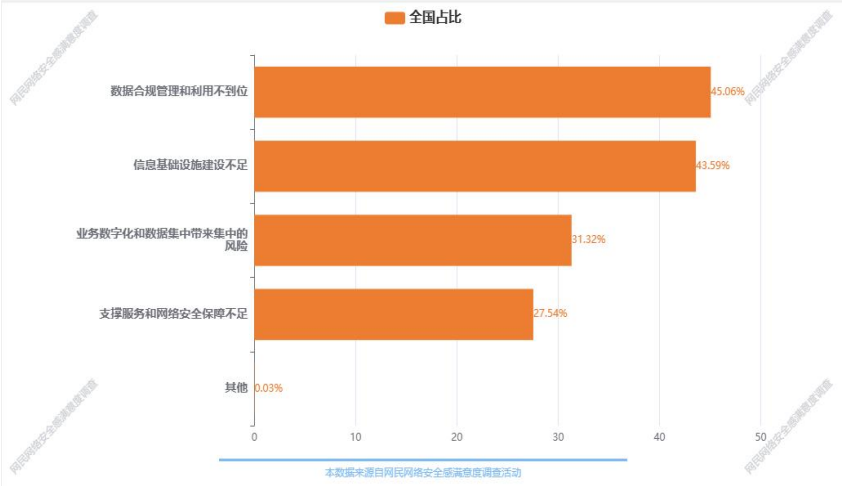


得益于近年来我国对网络安全建设的重视与积极推动，数字政府及智慧城市在新技术建设应用推广的过程当中，安全建设也基本保持同步建设水平，例如以《网络安全法》为基础的网络安全法规体系不断完善，为数字政府和智慧城市的安全提供了法律保障。以国产 CPU、国产操作系统、国产数据库为代表的自主可控的信创底座不断成熟，为数字政府和智慧城市的安全筑牢了基础。安全厂商百花齐放，各类安全产品也愈发成熟，为数字政府和智慧城市的安全提供了技术支撑。



尽管我国数字政府和智慧城市的安全状况总体较好，但仍存在一些问题和挑战。45.06%的人员认为数字政府和智慧城市不安全的地方主要在于数据合规管理

和利用不到位。43.59%的认为是由于信息基础设施建设不足。在数字政府和智慧城市中，数据的权属问题一直是一个难点，政府、企业、个人等各方在数据产生、使用和共享过程中的权益和责任不清晰，容易导致数据滥用和侵权问题。尽管我国已经出台了一系列关于网络安全和数据保护的法律法规，但是在数据收集、存储、处理和共享等方面尚不完善，缺乏明确的法律指导和规范。要推动数字政府和智慧城市的高质量发展，需持续加强法律法规完善、监管机制建设，同时加大在数据分析和挖掘方面的投入，提高数据分析和挖掘能力。



三、调查总结及未来展望

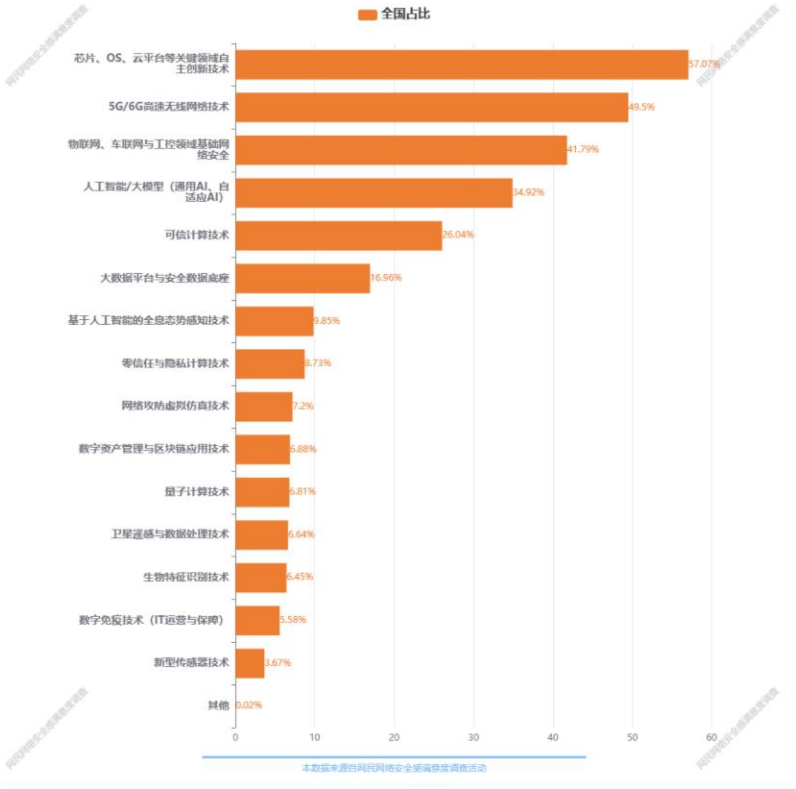
3.1 调查总结

通过本次调研可以发现，新技术在网络安全领域的应用趋势和发展方向是多元化的。主要原因是随着人们对网络的依赖程度越来越高，网络安全问题也变得更加复杂多样化。网络安全的防护工作将不再局限于传统的防火墙和杀毒软件等手段，而是会采用多种手段和技术来保障网络的安全，尤其网络安全与大数据技术、5G 技术、区块链技术、人工智能技术、物联网技术、云计算计算等新一代信息技术的融合创新，有助于更好地应对各种网络攻击和威胁，提高整体安全防护能力水平。

如人工智能构建智能防御新时代，它们可以自动化地分析大量数据、识别异常行为并预测潜在威胁。通过智能分析网络流量、用户行为以及安全事件等数据，帮助企业实现精准的安全防护和快速响应，进一步不断优化和完善安全防护策略，提高整体安全防护水平。区块链技术帮助构建可信数字生态，区块链技术以其去中心化、不可篡改的特性在网络安全领域展现出巨大潜力，为数字资产提供可靠

的存储和传输机制，保障数据的安全性和完整性。此外，还可以用于构建可信的身份认证和访问控制机制，防止身份冒用和未授权访问等安全威胁。零信任打破传统基于边界的安全防护思路，重塑网络边界，将安全控制点细化到每一个访问请求上。通过身份验证、访问授权、持续监控等手段，确保只有经过授权的应用程序才能访问企业资源，有效缩小了远程访问的攻击面。

结合本次调研也发现，57.07%人员认为芯片、OS（操作系统）、云平台等关键领域的自主创新也是网络安全未来发展的热点和重点。自主可控是确保网络安全的必要条件。目前，我国在网信领域（如芯片和基础软件等方面）仍存在一些短板。芯片方面，其短板在于制造工艺、装备、材料、设计工具等方面。以 AI 芯片为例，我国起步晚，在算法方面缺乏原始创新，目前仍依赖进口。基础软件方面，操作系统大部分依赖 Windows，国产操作系统很少。大型工业基础软件，如集成电路涉及软件基本上是进口，自主研发的较少。我国亟需“扬长处，补短板”，努力突破“卡脖子”问题，加强核心技术自主创新，研发具有自主知识产权的产品，实现关键自主可控，是提升网络安全的关键。



3.2 未来展望

我国当下处于数字经济快速发展的重要阶段，应多措并举加强新技术应用的

网络安全建设工作。

一是加强技术创新，加快自主核心技术研发。实现网络安全关键技术自主可控，是筑牢数字中国安全屏障的底气所在。同时结合人工智能、区块链等新一代信息技术，研发更先进的网络安全产品，进行应用转化和价值闭环，保证相关技术创新的持续推进，不断提升国产网络安全产品质量，从而提高社会和企业的整体安全防护能力水平。

二是完善法律法规，建立健全的网络安全法律保障体系。当下我国已经形成以《网络安全法》、《数据安全法》和《个人信息安全保护法》为核心的中国网络安全法律体系框架，应在此基础上，强化数据分类分级保护、数据安全审查、数据出境管理等制度措施，提高网络数据监测预警和应急处置能力，维护网络空间秩序。同时加强网络安全监管，实现权责明确的多部门联动结合监管和合作协调，提高跨部门的网络安全响应能力。加大对网络犯罪的打击力度，注重保护个人隐私，明确网络空间的行为规范和责任追究机制。

三是加强专业人才培养和团队建设，提升人员就业技能。当前，我国网络安全领域人才不足，已成为阻碍我国产业发展的主要因素，特别是实战型人才培养方面，存在显著的需求缺口。应制定网络安全人才专项，加强网络安全人才培养支撑力度。通过明确培养目标、优化培养方式，有计划、有目的地推进和实施网络安全人才培养工作。高校是网络安全人才培养的主阵地，企业是岗位实践的最终平台，应加强校企产业融合合作，促进专业领域人才培养，培养行业发展需要的复合型创新型人才，以“硬实力”打造一支具有全球竞争力的网络安全团队。