



# 2021年全国网民网络安全感 满意度调查专题报告

## 新技术应用与网络安全专题

广东新兴国家网络安全和信息化发展研究院  
复旦大学网络空间国际治理研究基地

2021年12月

本报告数据来源于 2021 网民网络安全感满意度调查活动，任何组织和个人引用本报告中的数据和内容须注明来源出处。

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](http://www.iscn.org.cn) “网安联” 公众号：



**2021 网民网络安全感满意度调查  
“新技术应用与网络安全” 专题报告**

**广东新兴国家网络安全和信息化发展研究院  
复旦大学网络空间国际治理研究基地**

**2021 年 12 月**

# 目录

一、前言.....	1
二、主要发现.....	3
2.1新技术应用前景向好，网络安全问题需重点关注.....	3
2.2 5G网络建设需加强，5G安全问题应加快解决.....	3
2.3数字政府与智慧城市应用新技术收获好评，部分问题值得关注.....	4
2.4网络安全新技术发展百花齐放，体系建设应齐头并进.....	4
三、从业人员基本情况.....	5
3.1从业人员基本情况.....	5
四、专题分析.....	9
4.1新技术应用前景与制约因素.....	9
五、结论.....	22

## 一、前言

为充分发挥网络安全社会组织在网络空间建设中的桥梁作用，全面提升社会组织服务国家及地方政府网络安全建设的能力和水平，促进全国网络安全事业的发展，由全国各级网信、公安、工信、市场监管等政府部门的指导和大力支持、全国 135 家网络社会组织共同发起，以“网络安全为人民、网络安全靠人民”为主题的 2021 网民网络安全感满意度调查活动于 2021 年 8 月 3 日启动。本活动持续 10 天，共收回问卷 284.5235 万份，经数据清洗消除无效数据后，有效问卷 264.7339 万份。

此次发布的调查问卷分为公众版和从业人员版。公众版从大众化的角度，设置八个专题二级问卷，分别是网络安全法治社会建设、遏制惩处网络违法犯罪、个人信息保护和数据安全、网络购物权益保护、未成年人网络权益保护、互联网平台监管与企业自律、数字政府服务与治理能力提升、数字鸿沟消除与乡村振兴；从业人员版从网络从业人员的技术专业化角度，设置四个专题二级问卷，分别是等级保护实施与企业合规、行业发展与生态建设、新技术应用与网络安全、科技创新与人才培养。其中“新技术应用与网络安全”作为二级问卷之一，围绕我国新技术应用与网络安全设置十七个问题。

为全面分析我国新技术应用与网络安全情况，基于发起单位调查所得的数据，由广东新兴国家网络安全和信息化发展研究院主办、复旦大学网络空间国际治理研究基地承办，围绕本专题及聚焦行业趋势，结合分析得出两项调查结论，汇总形成本报告。

2021年12月6日至10日，2021年全国网民网络安全感满意度调查报告发布周在北京面向全社会举办。《2021年网民网络安全感满意度调查“新技术应用与网络安全”专题报告》作为发布周的重要组成部分，不仅反映了现阶段新技术应用与网络安全在数据要素化、可视化方向的具体实践，也为网络安全行业发展提供决策思考和可行路径，进而为网络空间建设提供有益参考。

## 二、主要发现

经过对调查数据统计、分析后，有以下主要发现：

### 2.1 新技术应用前景向好，网络安全问题需重点关注

(1) 通过本次调查发现，5G、人工智能、区块链、大数据和物联网等新技术在各个领域应用广泛，从业人员均看好新技术的应用和发展前景。具体来说，从业人员最看好人工智能技术应用的场景排前3的是：交通（70.48%）、医疗（69.98%）和教育（50.99%）；参与调查的从业人员中有48.41%的人认为区块链未来会广泛应用于各个行业领域；有54.97%的从业人员表示其所在单位已经运用了大数据技术；物联网在智能家居（73.14%）、智能交通（50.75%）、智能物流（47.92%）、智能医疗（41.85%）的渗透率超过40%。

(2) 各新技术在应用场景下出现的网络安全问题受到从业人员的高度关注。在工控领域的网络安全问题方面，核心技术自主可控不高（61.56%）、安全建设水平偏低（61.51%）和安全监管力度不足（53.29%）等三个方面认可度均超过50%；在人工智能的“AI换脸”应用的安全方面，降低生物特征识别技术可信度（74.85%）、催生网络黑灰产（71.26%）和深度伪造技术滥用危害国家安全（59.35%）三个方面同样超过50%；从业人员同样认为区块链应用存在的问题中，网络安全问题同样值得关注，如监管制度不完善为56.56%，缺少数据共享政策规划为52.97%；在物联网安全风险方面，几大网络安全问题关注度同样超50%，信息安全风险高为76.84%、物联网设备不安全为66.86%、未建立完善的安全管理机制为52.84%。

### 2.2 5G网络建设需加强，5G安全问题应加快解决

(3) 在参与调查的从业人员中，有64.04%的人认为目前5G服务收费比4G高的情况可能阻碍5G的发展，有58.46%的人认为目前5G网络覆盖面较小，有45.9%的人认为5G技术不成熟，出现网络错误/卡顿。这些数据说明，5G网络的建设水平还需进一步加强，包括利用规模经济实现降本增效以降低5G资费，加强5G基站建设扩大网络覆盖面，以及持续不断的优化改进5G技术降低网络错误和卡顿情况的出现。

(4) 在调查从业人员对新技术新应用的网络安全顾虑时，关注过5G移动网络安全问题的从业人员占73.73%，占比排名第1，数据显示目前5G的网络安全问题受到行业的重点关注，说明5G存在网络安全问题是比较多的，应投入更多的资源重点关注，加快解决5G网络的网络安全问题。

### **2.3数字政府与智慧城市应用新技术收获好评，部分问题值得关注**

(5) 数据显示超过一半的从业人员认为数字政府和智慧城市中新技术的应用效果是令人满意的，但应用新技术过程中存在以下问题应加以改善：过度强调数字化技术，忽略弱势群体对传统服务的需要；技术不成熟，不实用；配套服务没有跟上。

### **2.4网络安全新技术发展百花齐放，体系建设应齐头并进**

(6) 在以下几个选项中至少有44%的从业人员认为会是未来的发展热点：芯片、OS、云平台等关键领域自主创新技术；5G/6G高速无线网络技术；物联网、车联网与工控领域基础网络安全；大数据平台与安全数据底座。

(7) 在调查从业人员对于加强新技术应用于网络安全保障方面的建议时，几乎所有针对性选项均获得了较高的认可，在以下几个方面的认可度超过60%：加强自主创新，加快技术研发；完善法律法规，制定伦理道德规范；健全行业监管，加大执法与惩戒力度；培养专业人才，提升人员就业技能。

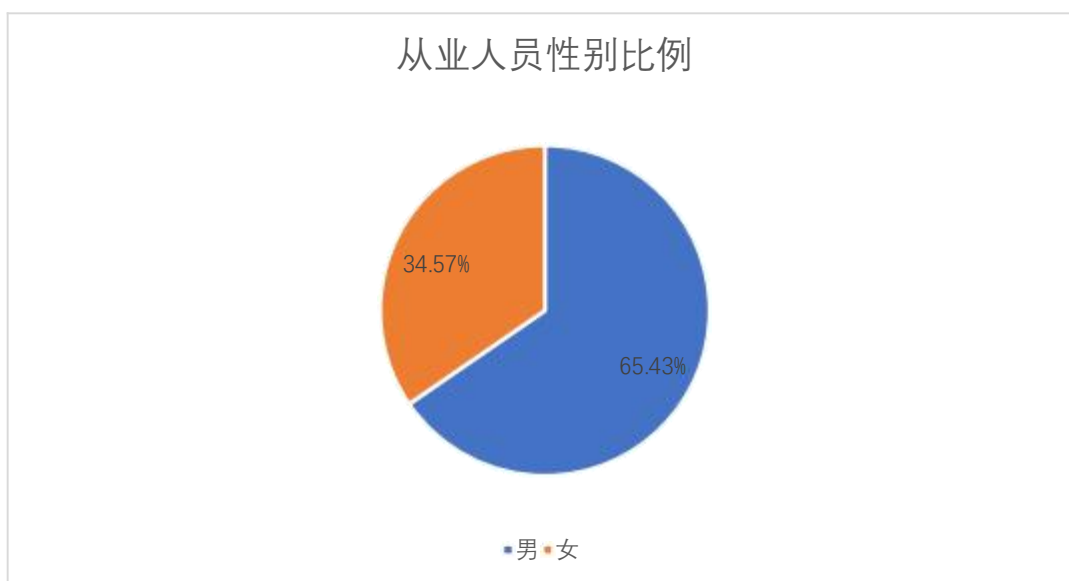


### 三、从业人员基本情况

#### 3.1 从业人员基本情况

##### (1) 性别分布

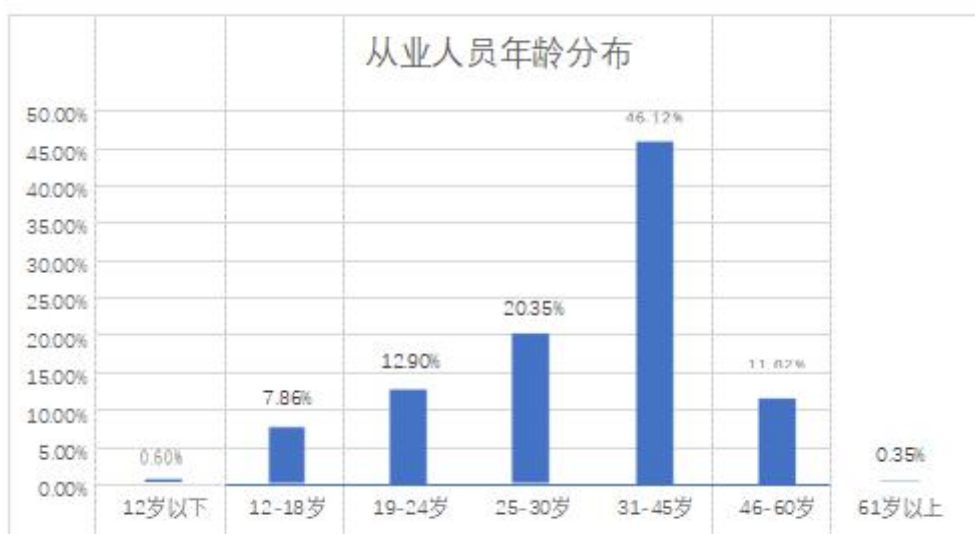
参与本次调查的从业人员中男性占65.43%，女性网民占34.57%，从数据上看男性比例较多，远超出我国男女性别比例与IT行业从业者的男女性别比例。



图表3.1-1：从业人员性别比例

##### (2) 年龄分布

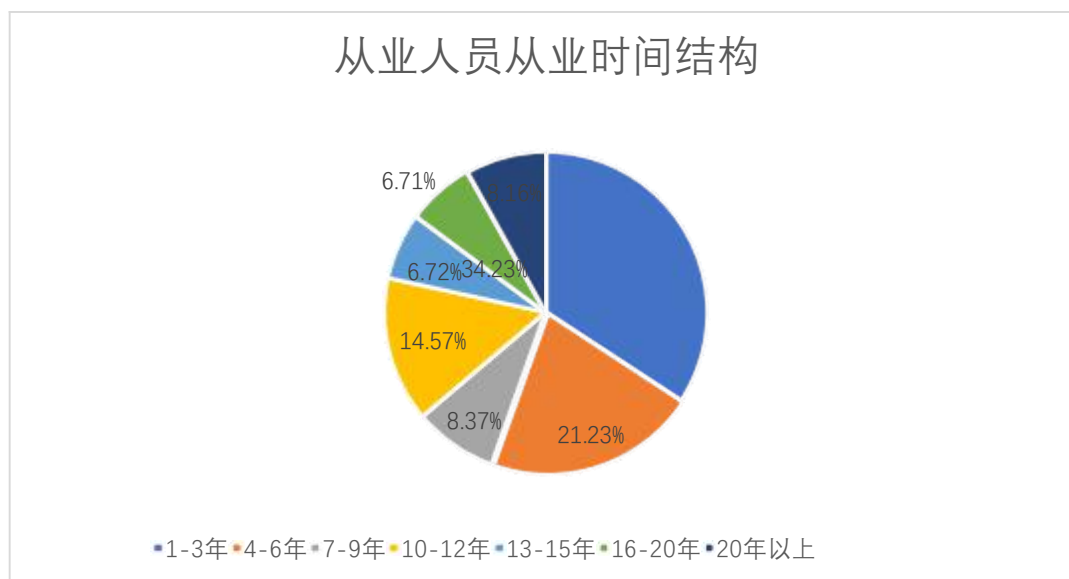
参与调查的从业人员中青年人占大多数。其中，12岁到18岁占7.86%，19岁到24岁占12.9%，25岁到30岁占20.35%，31岁到45岁占46.12%，即30岁以下年轻人占约41.11%。45岁以下占87.23%，从业人员年龄以中青年为主，占比接近一半。



图表3.1-2: 从业人员年龄分布

### (3) 从业时间结构

参与调查的从业人员在网络行业的从业时间较短。其中，从业时间1-3年的占比为34.23%，从业时间4-6年的占比为21.23%。数据显示超过一半的从业人员在网络行业的从业时间不足7年。

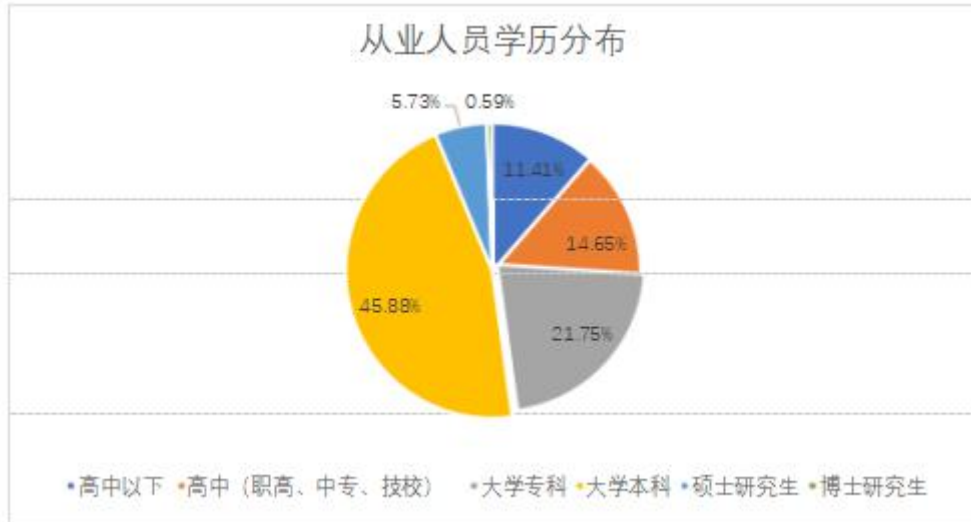


图表3.1-3: 从业人员从业时间结构

### (4) 学历分布

参与调查的从业人员中本科的人数最多，占45.88%，其次是大专学历，占21.75%，大专以上学历为73.94%，在普通网民群体中受教育的程度相对不低，

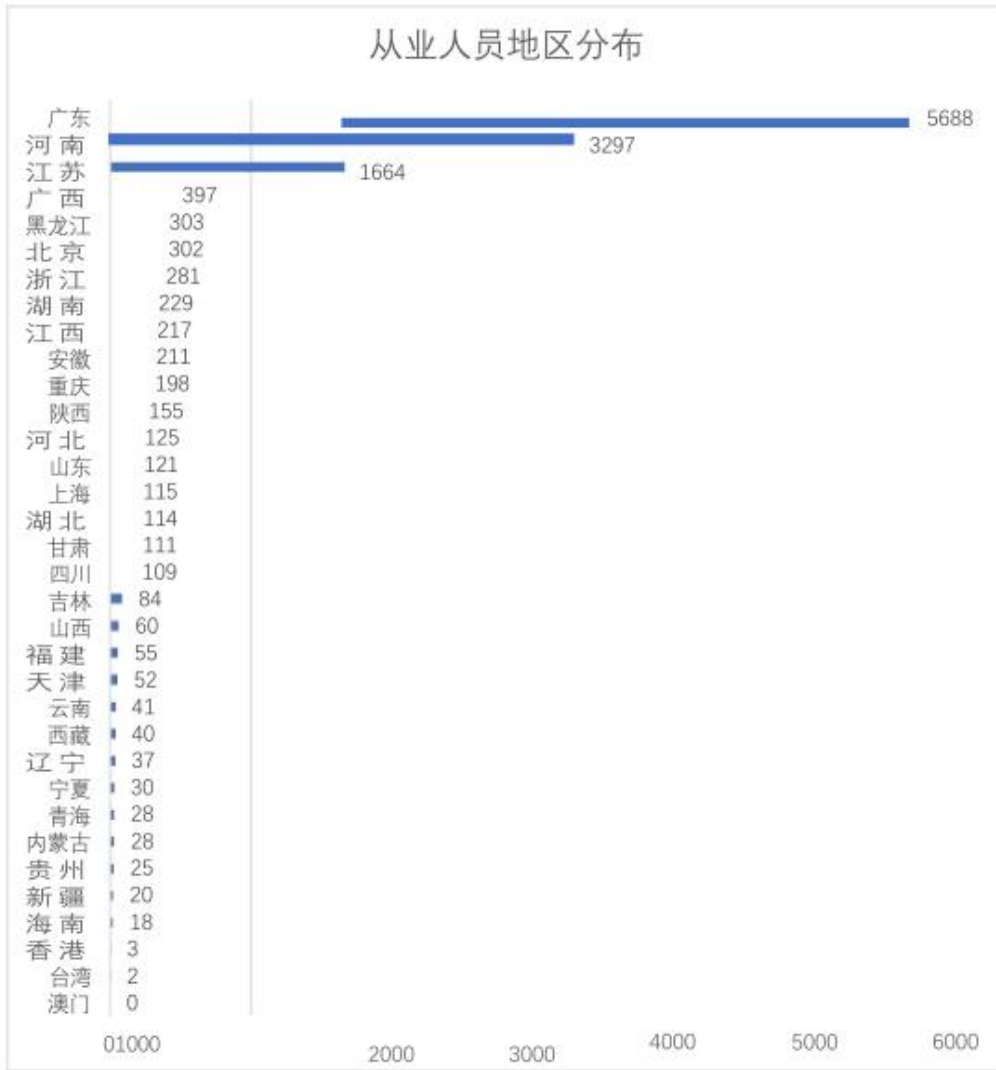
远高于我国网民中大专及以上学历比例，数据显示我国网络行业从业人员的受教育水平相对较高。



图表3.1-4从业人员学历分布

#### (5) 地区分布

参与调查的从业人员来自全国各省、直辖市、自治区和港澳台地区等，其中广东、河南、江苏、广西、黑龙江、北京、浙江、湖南、江西、安徽的有效答卷数量排列前10位。各地区分布情况如下图：



图表3.1-4从业人员地区分布

## 四、专题分析

### 4.1 新技术应用前景与制约因素

参与本专题答题的从业人员人数为14160。

在数字时代，新技术与新应用形态的不断创新变革，使得网络生活的形态得到极大地丰富，基于5G、人工智能、大数据、物联网的各种生产和消费应用场景不断推陈出新，同时也带来不断升级的网络安全问题挑战。

本专题就5G、人工智能、区块链、大数据、物联网、数字政府和智能城市发展、网络安全等方面的问题开展调查，了解从业人员对于新技术和新应用的发展与网络安全应用的评价，发现差距和问题。

#### （1）对新技术新应用的网络安全问题的关注度

从业人员对新技术新应用的网络安全问题的关注度排列前5位为：5G移动网络（73.73%）、大数据（64.24%）、人工智能（53.68%）、物联网（41.36%）、云计算（39.87%）。数据显示从业人员对新技术新应用的网络安全问题是比较关注的。



图表4.1-1：对新技术新应用的网络安全问题的关注度

（图表数据来源：从业人员版新技术应用与网络安全专题第1题：您关注过以下哪项新技术新应用的网络安全问题？）

## (2) 对5G技术的顾虑

参与调查的从业人员对5G技术的顾虑排名前4的有：1比4G服务收费更高（64.04%），2网络覆盖面小（58.46%），3技术不成熟出现网络错误或卡顿（45.90%），4网络不安全（33.35%）。数据显示，从业人员对5G技术最关注的是费用较高和网络信息覆盖仍然不足的问题。

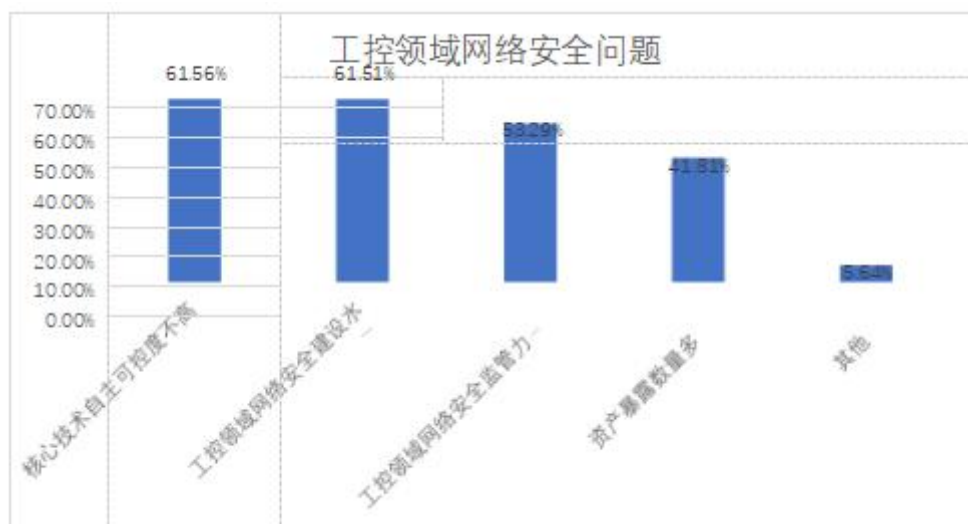


图表4.1-2: 对5G技术的顾虑

（图表数据来源：从业人员版新技术应用与网络安全专题第2题：您对5G技术存在哪些顾虑？）

## (3) 工控领域网络安全问题

参与调查的从业人员认为工控领域网络安全建设不容忽视，各方面的问题关注度都不低，在列出的5个选项中，4个明细选项的关注度均超过40%，分别为：1核心技术自主可控度不高（61.56%）、2工控领域网络安全建设水平偏低（61.51%）、3工控领域网络安全监管力度不够（53.29%）、4资产暴露数量多（41.81%）。

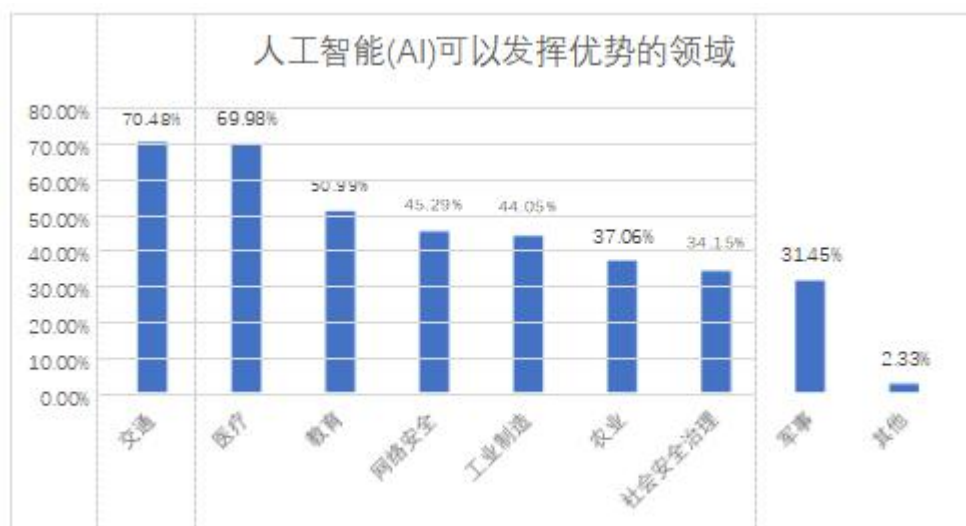


图表4.1-3: 工控领域网络安全问题

(图表数据来源: 从业人员版新技术应用与网络安全专题第3题: 您认为工控领域网络安全存在哪些问题?)

#### (4) 人工智能(AI)可以发挥优势的领域

参与调查的从业人员认为人工智能(AI)可以发挥优势的领域排名前5的为: 1交通(70.48%)、2医疗(69.98%)、3教育(50.99%)、4网络安全(45.29%)、5工业制造(44.05%)。数据显示, 从业人员认为人工智能可以应用的领域非常广泛, 有比较好的应用前景。

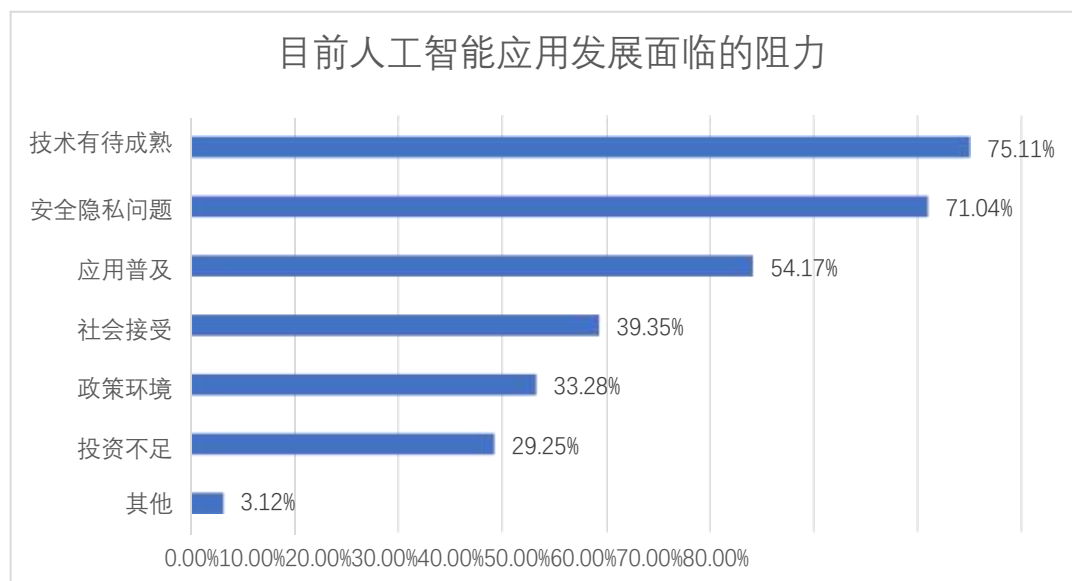


图表4.1-4: 人工智能(AI)可以发挥优势的领域

（图表数据来源：从业人员版新技术应用与网络安全专题第4题：您最期待人工智能(AI)在哪些领域发挥优势？）

#### （5）目前人工智能应用发展面临的阻力

参与调查的从业人员对目前人工智能应用发展面临的阻力排前3位为：1技术有待成熟（75.11%），2安全隐私问题（71.04%），3应用普及（54.17%），数据显示技术成熟度、安全隐私保护问题等是从业人员关注的重点。



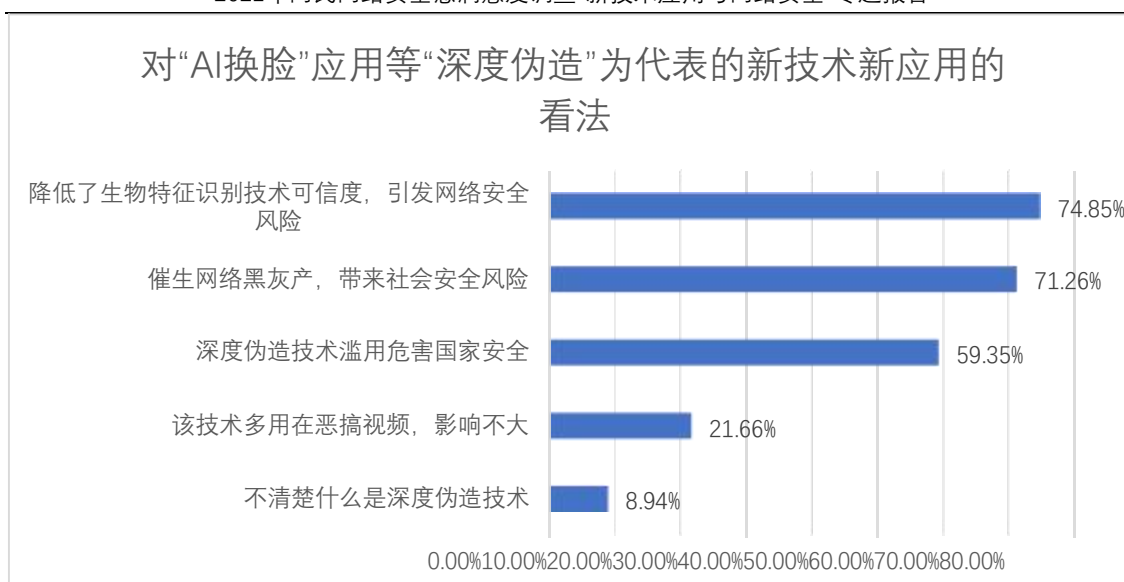
图表4.1-5：目前人工智能应用发展面临的阻力

（图表数据来源：从业人员版新技术应用与网络安全专题第5题：您认为目前人工智能应用的发展面临的最大阻力是？）

#### （6）对“AI换脸”应用等“深度伪造”为代表的新技术新应用的想法

参与调查的从业人员对“AI换脸”应用等“深度伪造”为代表的新技术新应用的想法排前3位为：1减低了生物识别技术可信度（74.85%）、2催生网络黑灰产业（71.26%）、3深度伪造技术滥用危害国家安全（59.35%）。数据显示从业人员对深度伪造技术是比较担心的。

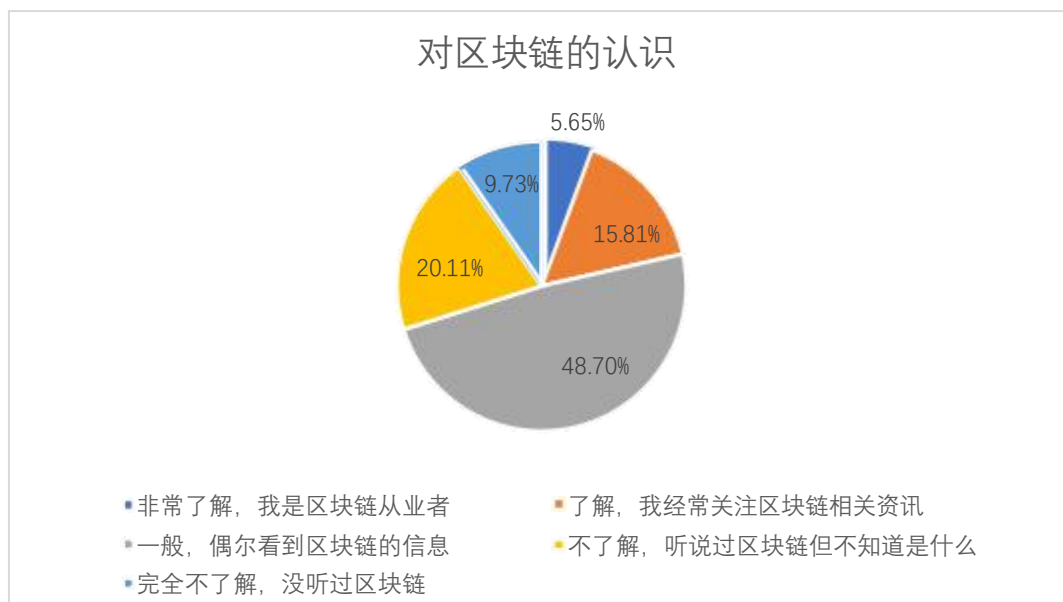




图表4.1-6：对“AI换脸”应用等“深度伪造”为代表的新技术新应用的想法（图表数据来源：从业人员版新技术应用与网络安全专题第6题：近两年出现了“AI换脸”应用，您怎么看这种以“深度伪造”为代表的新技术新应用？）

#### （7）对区块链的认识

参与调查的从业人员对区块链的认识看法为：48.7%从业人员认为一般，偶尔看到区块链的信息；20.11%从业人员对区块链不了解，听说过；也有9.73%完全不了解。数据显示从业人员对区块链了解程度一般或不高。

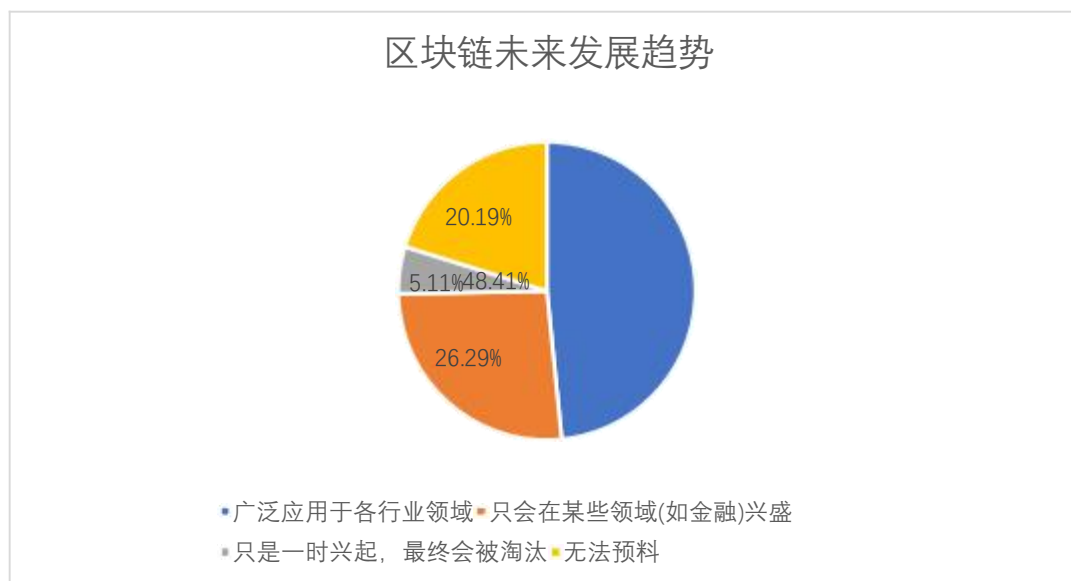


图表4.1-7：对区块链的认识

（图表数据来源：从业人员版新技术应用与网络安全专题第7题：对区块链，您了解多少？）

### （8）区块链未来发展趋势

参与调查的从业人员对区块链未来发展趋势的看法：认为会广泛应用于各行业领域最多，占48.41%，认为只会在某些领域（金融）兴盛的占26.29%和认为无法预料的占20.19%，认为只是一时兴起，最终会被淘汰的5.11%。看好区块链发展的比例不低。



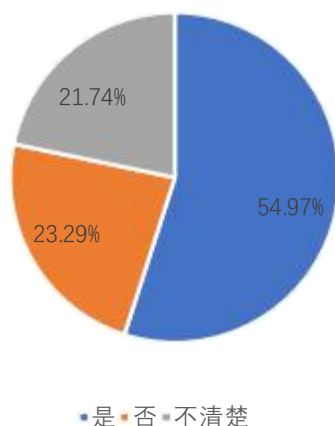
图表4.1-8：区块链未来发展趋势

（图表数据来源：从业人员版新技术应用与网络安全专题第8题：您觉得区块链未来发展会如何？）

### （9）所在单位对大数据技术应用情况

参与调查的从业人员所在单位对大数据技术的应用情况方面，54.97%的从业人员所在单位有应用了大数据技术；23.29%的从业人员所在单位没有应用大数据技术，21.74%表示不清楚。数据显示大数据开始在从业人员单位得到较广泛的应用。

### 所在单位对大数据技术应用情况



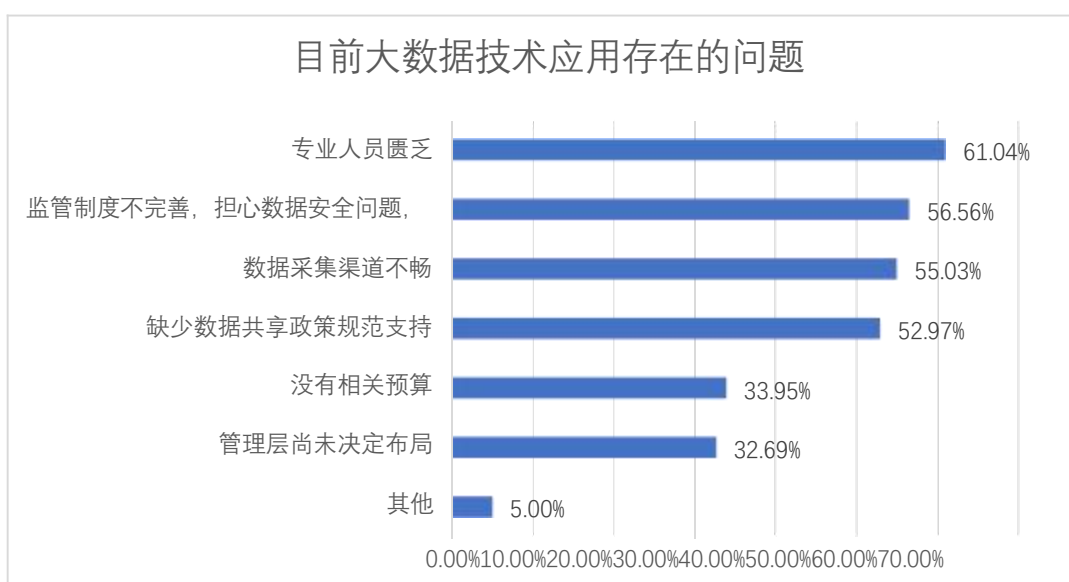
图表4.1-9：所在单位对大数据技术应用情况

（图表数据来源：从业人员版新技术应用与网络安全专题第9题：您现所在单位是否应用了大数据技术？）

#### （10）目前大数据技术应用存在的问题

根据对从业人员的调查，目前大数据技术应用存在的问题排前5位是：1专业人员匮乏（61.04%），2监管制度不完善（56.56%），3数据采集渠道不畅（55.03%），4缺少数据共享政策规范支持（52.97%）。数据显示人才、制度、渠道、规范等问题是大家比较关注的。

### 目前大数据技术应用存在的问题

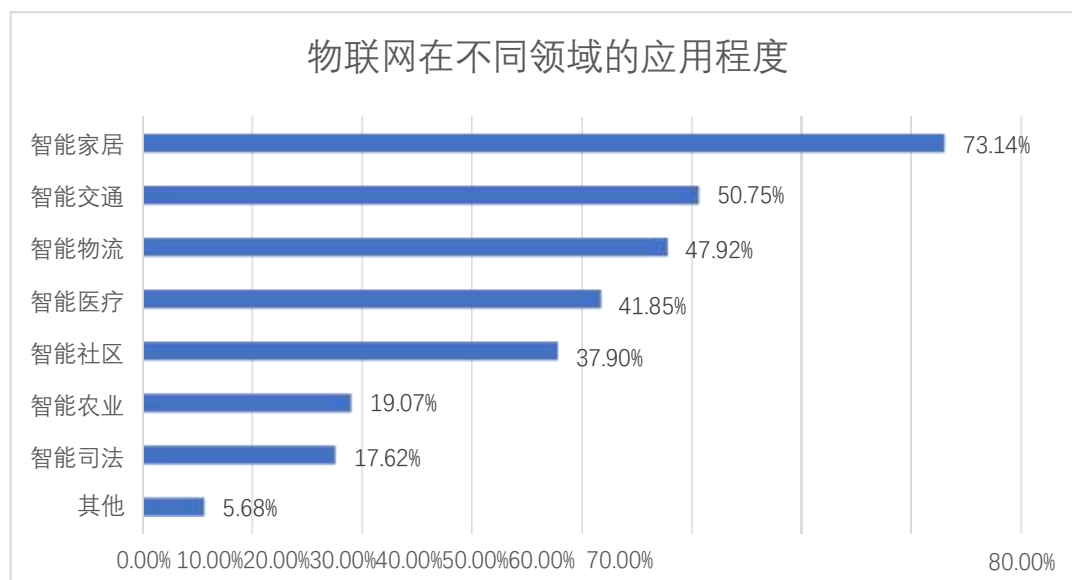


图表4.1-10：目前大数据技术应用存在的问题

（图表数据来源：从业人员版新技术应用与网络安全专题第10题：您认为目前大数据技术应用上存在哪些问题？）

## (11) 物联网在不同领域的应用程度

参与调查的从业人员使用过的物联网应用，排前3位是：1智能家居领域（73.14%）2智能交通（50.75%），3智能物流（47.92%）。显示在智能家居、交通、物流等领域物联网技术应用比较广泛。

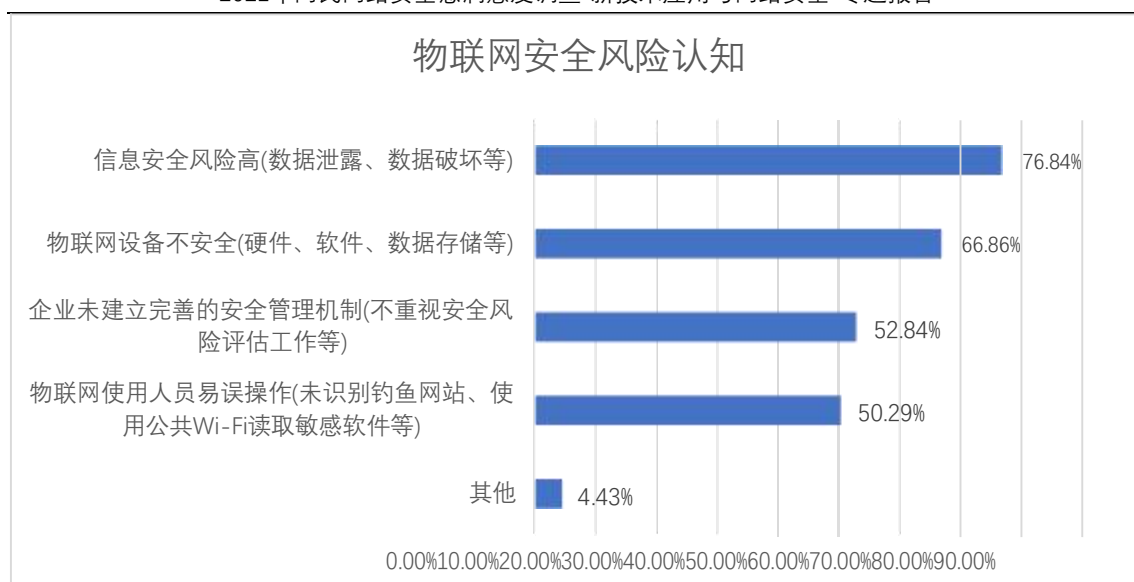


图表4.1-11：物联网在不同领域的应用程度

（图表数据来源：从业人员版新技术应用与网络安全专题第11题：您在哪些领域体验过物联网的应用？）

## (12) 物联网安全风险认知

参与调查的从业人员对当下的物联网安全风险看法为：76.84%认为信息安全风险高，66.86%认为物联网设备不安全，52.84%认为企业未进阿里完善的安全管理机制，50.29%从业人员认为物联网使用人员易误操作。数据显示从业人员对物联网的安全风险是比较担心的。

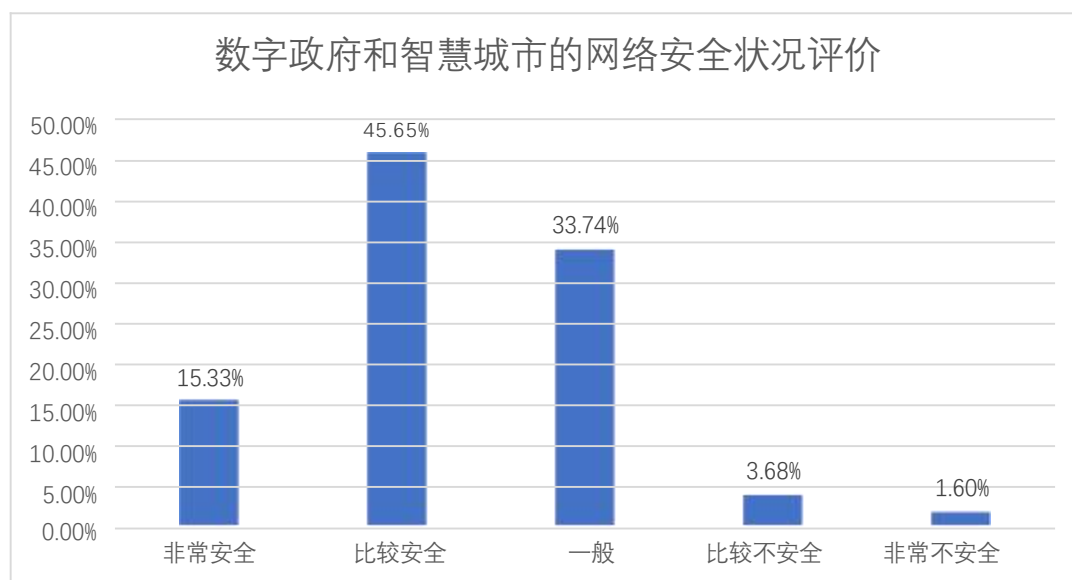


图表4.1-12：物联网安全风险认知

（图表数据来源：从业人员版新技术应用与网络安全专题第12题：您认为当下的物联网安全风险主要存在哪些方面？）

### （13）数字政府和智慧城市的网络安全状况评价

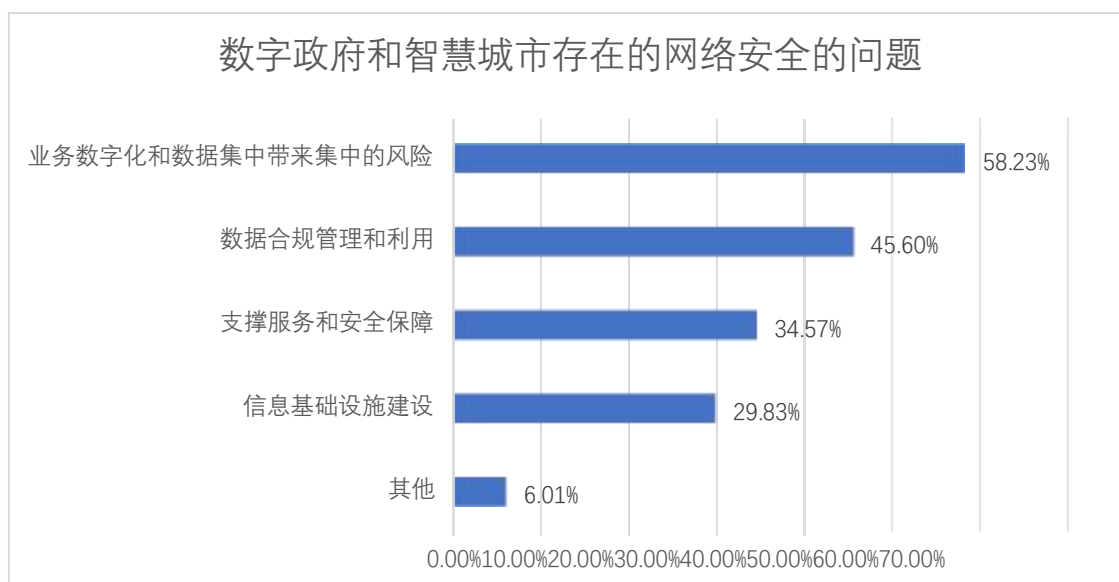
参与调查的从业人员对数字政府和智慧城市的网络安全状况评价：15.33%从业人员认为非常安全，45.65%认为比较安全，33.74%认为一般。数据显示超过一半的从业人员认为数字政府和智慧城市的网络安全状况是比较安全的。



图表4.1-13：数字政府和智慧城市的网络安全状况评价

（图表数据来源：从业人员版新技术应用与网络安全专题第13题：您对数字政府和智慧城市的网络安全状况评价？）

在进一步调查从业人员认为数字政府和智慧城市的网络安全存在哪些方面时发现，业务数字化和数据集中带来集中的风险和数据合规管理和利用两个问题受到的关注度比较高，分别是58.23%和45.6%。数据显示，在数字政府和智慧城市的网络安全方面的问题主要是跟数据使用有关。



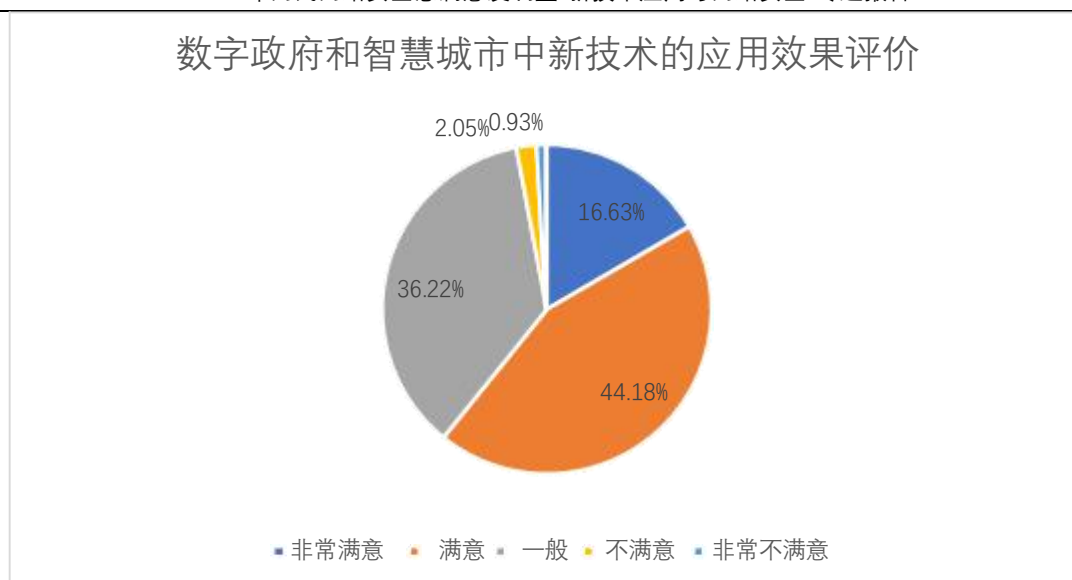
图表4.1-13.1：数字政府和智慧城市存在的网络安全的问题

（图表数据来源：从业人员版新技术应用与网络安全专题第13.1题：你认为数字政府和智慧城市不安全的方面主要是什么？）

#### （14）数字政府和智慧城市中新技术的应用效果评价

从业人员对数字政府和智慧城市中新技术的应用效果评价：16.63%从业人员认为非常满意，44.18%认为满意，36.22%认为一般。数据显示超过一半的从业人员认为数字政府和智慧城市中新技术的应用效果是令人满意的。

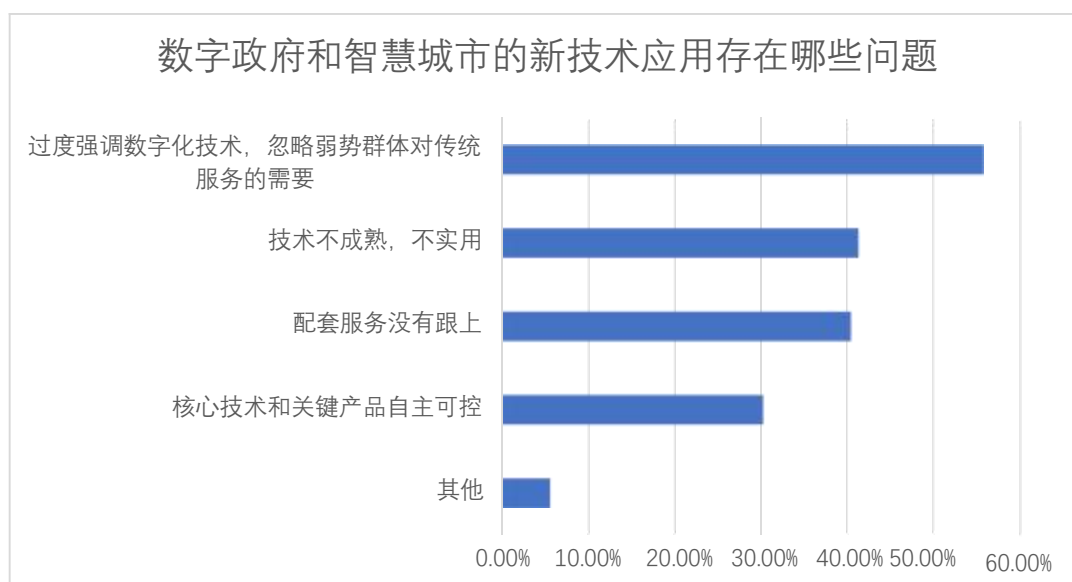
### 数字政府和智慧城市中新技术的应用效果评价



图表4.1-14：数字政府和智慧城市中新技术的应用效果评价

（图表数据来源：从业人员版新技术应用与网络安全专题第14题：您对数字政府和智慧城市中新技术的应用效果评价？）

在调查数字政府和智慧城市的新技术应用存在哪些问题时，排名前3的为：1过度强调数字化技术，忽略弱势群体对传统服务的需要（55.81%）、2技术不成熟，不实用（41.3%）、3配套服务没有跟上（40.43%）。

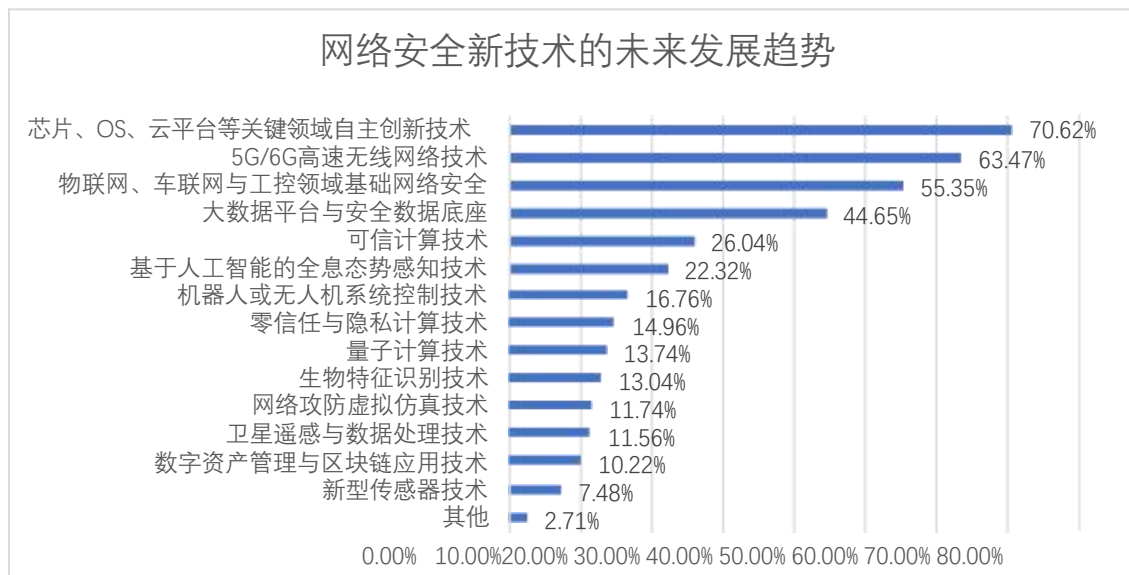


图表4.1-14.1：数字政府和智慧城市的新技术应用存在哪些问题

（图表数据来源：从业人员版新技术应用与网络安全专题第14.1题：你认为数字政府和智慧城市新技术应用存在的问题主要是什么？）

#### （15）网络安全新技术的未来发展趋势

在调查从业人员关注的网络安全新技术未来的发展趋势时，最受到关注的排前3的热点为：1芯片、OS、云平台等关键领域自主创新技术（70.62%）；25G/6G高速无线网络技术（63.47%）、3物联网、车联网与工控领域基础网络安全（55.35%）。



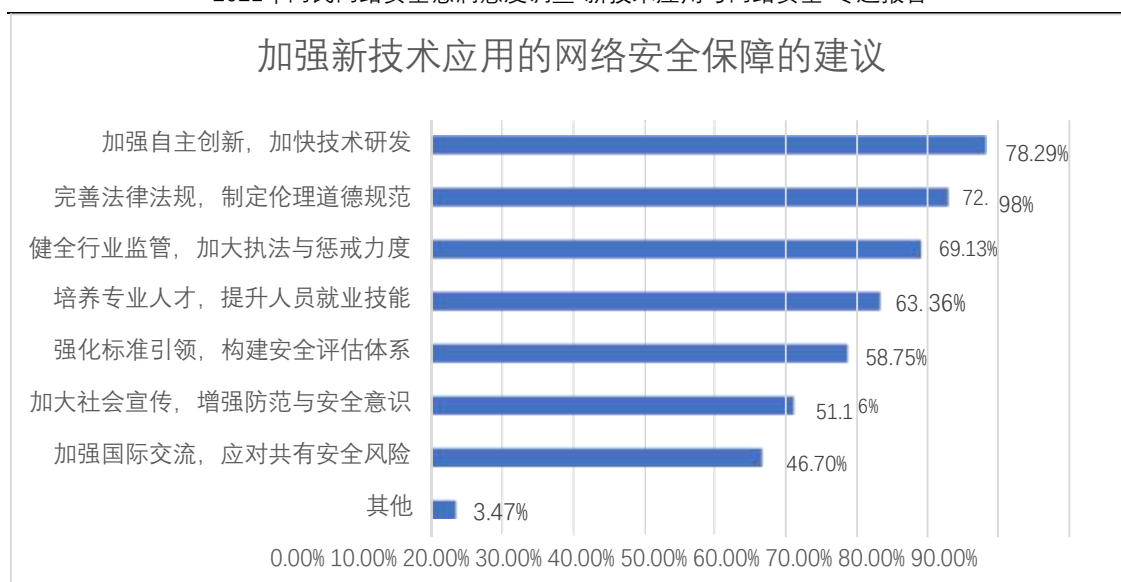
图表4.1-15：网络安全新技术的未来发展趋势

（图表数据来源：从业人员版新技术应用与网络安全专题第15题：您认为哪些网络安全相关技术是未来发展的热点？）

#### （16）加强新技术应用的网络安全保障的建议

参与调查的从业人员对加强新技术应用的网络安全保障的建议排前3位的位置：1加强自主创新加快技术研发（78.29%）、2完善法律法规（72.98%）、3健全行业监管加大执法与惩戒力度（69.13%）。数据显示从业人员对加快自主创新、完善法规、坚强监管等方面比较关注。





图表4.1-16：加强新技术应用的网络安全保障的建议

（图表数据来源：从业人员版新技术应用与网络安全专题第16题：您对加强新技术应用的网络安全保障有哪些建议？）

## 五、结论

本次网民网络安全感满意度调查是在总结去年满意度调查成功经验的基础上进行的，在许多方面包括问卷设计、组织发动、活动支持、数据服务等都有新的突破。在公安等有关主管部门大力支持下，在各组织单位共同努力下，调查活动取得良好效果，活动收回的问卷数量比去年有跨越式的增长，说明网络安全感满意度调查活动受到了网民和从业者。从统计结果来看，本次问卷调查数据提供了丰富的信息，反映了广大从业人员对当前网络安全状况和治理效果的满意程度的评价，包括从业人员对热点问题的关注、对整体网络安全态势的感受、以及对政府监管、企业自律、行业发展、新技术应用等方面的评价。另外，从业人员还提出了许多意见和建议，这些意见对政府有关部门加强网络空间治理，打造一个安全、清朗的网络空间有增添的调查的成果是丰富的。

概括起来，本次调查成果有以下主要结论：

### **(1) 网络安全新技术应用效果良好，发展趋势令人期待**

绝大多数参与调查的从业人员对当前网络安全新技术新应用的效果表示肯定，同时均对未来新技术进行一步广泛应用于各行各业予以较高的期待，对于阻碍各个新技术推广应用的阻力及问题许多从业人员也多加关注，显示出从业人员对于新技术新应用改善我国网络安全水平充满信心。

在过去一年里，各级政府部门在党中央的统一部署下，围绕网络空间治理的各种问题，突出重点，积极谋划，精准施策，先后推出一系列有针对性的法律、规范、措施和行动，从多个层面和领域出发，打出了一套套组合拳，取得了显著的成果，给人民交出了一份漂亮的答卷。其行动之迅速，力度之大，成果之丰富，令人印象深刻，体现出我国政府成熟、自信、眼光和气魄，更标志着我国政府在网络空间治理能力方面有了长足的进步。

随着数据安全保护法、个人信息保护法、关键信息基础设施保护条例等重要法律的推出和实施，网络安全治理的“四梁八柱”框架建设取得重要成果，加上一系列的配套措施的落实，打开了网络安全治理的新局面，也标志着我国网络安全治理上了一个新台阶。调查结果也显示过去一年里我国网络安全治理在多个方面的工作取得了显著成效，网民的评价的大幅提升也充分证明了这一点，网络空

### **(2) 数字政府和智慧城市新技术应用获好评，新技术网络安全问题需重视。**

参与调查的从业人员超过一半认可新技术在数字政府和智慧城市中的应用。但是，在深入调查5G、人工智能、大数据、物联网等细分技术应用情况时，显示网络安全问题依旧是从业人员的关注重点，说明在将新技术应用到各行各业时，还需格外关注网络安全的问题并加以解决。同时，对于加强新技术应用于网络安全保障，从业人员也从数据合规利用、出台法律法规、自主可控核心技术研发和人才、标准体系建设等多个方面给出建议。

今年以来抗击疫情的斗争进入常态化阶段，在党、政府和人民的共同努力下，我国国民经济加快恢复和发展。疫情的发生和发展，给人们工作和生活方式带来了很大的变化。隔离、封锁等变化一方面给人们生活造成不便，但另一方面也给数字经济的发展提供了一个特殊的契机。远程办公、网络协同、线上服务等需求的爆发，极大地推动了各行各业向业务数字化转变。有了网络和信息技术的加持，传统经济迎来了升级换代加速发展的新阶段。在应对变局的过程中，出现了许多基于网络信息技术的新技术、新应用，也让人看到了数字经济的巨大活力和发展潜力。碳中和、绿色经济等新发展目标 and 理念的提出引领各个行业进入新一轮转型、升级和发展阶段。数字化是未来发展的方向，数字技术和网络技术已经成为关键技术，网络和信息化基础设施成为不可或缺的基础条件，网络安全将起重要的保障作用。习近平总书记对网络安全的重要性作出了重要论断：“没有网络安全就没有国家安全，没有信息化就没有现代化”。

习总书记还深刻阐述了网络安全和信息化发展的辩证关系，指出“网络安全和信息化是一体之两翼，驱动之双轮，必须统一谋划，统一部署，统一推进，统一实施。”。“十四五”规划对数字中国建设进行了统一部署，强调协同推进数字经济、数字生活和数字政府建设。在这个背景下，公安、网信、工信等部门加强了对网络空间的监管和对违法犯罪活动的打击，重点整治了网络诈骗、谣言传播等问题，有力地保障了网络空间的安全，调查数据也显示网民对政府采取的应对措施的效果评价是比较满意的。政府近年来加强智慧城市、智慧交通、平安城市等信息化建设大大地改善了信息化基础设施，为提升政府现代化治理能力，改善数字政府公共服务打下坚实的基础。我国在网络安全领域加强治理，成效显著，为数字经济的发展奠定了良好的基础。



网安联微信公众号



网络安全共建网官网

## 网安联秘书处

官网:[www.iscn.org.cn](http://www.iscn.org.cn)

电话:020-8380 3843 / 139 1134 5288

邮箱:[cinsabj@163.com](mailto:cinsabj@163.com)