2024年全国网民网络安全感满意度

遏制网络违法犯罪

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：郑州大学网络空间安全学院

2024年10月

本报告数据来源于2024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“网安联”公众号:

2024 网民网络安全感满意度

“遏制网络违法犯罪”专题调查报告

郑州大学网络空间安全学院

2024 年 10 月

课题组名誉组长：

胡传平　郑州大学网络空间安全学院　教授、院长

课题组组长：

李　妍　郑州大学网络空间安全学院　副教授

课题组副组长：

韩　颖　郑州大学网络空间安全学院　讲师

课题组成员：

刘浩然　郑州大学网络空间安全学院

司　创　郑州大学网络空间安全学院

于洋易　郑州大学网络空间安全学院

霍　可　郑州大学网络空间安全学院

付琦皓　郑州大学网络空间安全学院

黄海谭　郑州大学网络空间安全学院

白雨婷　郑州大学网络空间安全学院

蔡献宏　郑州大学网络空间安全学院

杨　涵　郑州大学网络空间安全学院

李佳鹏　郑州大学网络空间安全学院

目录

第一章 调查背景及成因

1.1 背景分析

现如今科技飞速发展，人类社会已经步入了一个全新的信息化时代。在这个时代里，计算机和互联网与我们的日常生活紧密相连，无论是在工作、学习还是娱乐方面，网络都发挥着不可或缺的作用。然而，正如一枚硬币有两面，网络在带来便利的同时，也滋生了一系列违法犯罪行为。

2024 年 1 月微软系统遭到俄罗斯黑客组织的攻击，攻击者通过“密码喷洒”策略访问了微软部分高级领导团队成员、网络安全和法律部门员工的电子邮件帐户。尽管微软表示没有证据表明威胁行为者可以访问客户环境、生产系统、源代码或人工智能系统，但这次攻击仍然暴露了企业网络安全防护的薄弱环节，引发了业界对网络安全防护措施的重新审视。

2024 年 9 月 25 日晚，英国多个主要火车站的公共无线网络系统遭遇了严重的网络攻击事件，这一事件迅速引起了广泛的社会关注。据英国铁路网公司及多家媒体报道，包括伦敦尤斯顿站、曼彻斯特皮卡迪利站、伯明翰新街站、爱丁堡韦弗利站以及格拉斯哥中央车站在内的多个交通枢纽均受到了影响。

近些年网络攻击事件频发，重大数据泄露和勒索软件攻击事件对全球企业和行业造成巨大损害。这些攻击涉及 VPN 漏洞、电子邮件系统入侵、医疗系统瘫痪等，促使各国加强网络安全防范，提高警惕性以应对日益严峻的网络威胁，这也让我们意识到遏制网络违法犯罪的重要性。

为了深入了解网络违法犯罪的成因和发展趋势，我们有必要对网络违法犯罪的背景进行深入分析。

网络技术是一把双刃剑：网络技术的飞速发展为网络违法犯罪提供了便利条件，犯罪分子可以利用各种技术手段隐藏身份、攻击系统、传播恶意软件等，使得网络违法犯罪行为更加隐蔽和难以追踪。

人工智能技术滥用的危害性：随着人工智能技术的发展，网络犯罪分子开始恶意使用这些技术来降低犯罪门槛、提高犯罪效率。例如，

利用 ChatGPT 等大型语言模型生成攻击性文本、进行社会工程攻击等

法律法规的相对滞后性：虽然我国已经出台了一系列针对网络犯罪的法律法规，如《中华人民共和国网络安全法》等，但随着网络犯罪的快速发展和演变，一些法律规定已经显得滞后，无法满足打击网络违法犯罪的现实需要。

网络犯罪的局部产业化、集团化：一些犯罪分子通过网络组织起来形成犯罪团伙或犯罪集团进行有组织的犯罪活动。这些犯罪集团具有严密的组织结构和分工明确的职责使得犯罪行为更加专业化和高效化。

1.2 问题成因

技术发展与漏洞利用：随着网络技术的飞速发展，新的技术不断涌现，但同时也带来了新的安全漏洞和弱点。黑客利用这些漏洞进行攻击，以获取非法利益或实现某种政治、宗教等目的。

网络安全意识薄弱：许多组织和个人对网络安全的认识不足，缺乏足够的防范意识和技能。这导致他们在面对网络攻击时，往往无法及时采取有效的防御措施，从而增加了被攻击的风险。

经济利益驱动：网络攻击往往与经济利益密切相关。黑客通过攻击企业、政府机构等目标，窃取敏感信息、勒索赎金或破坏系统正常运行，以获取经济利益。这种利益驱动使得网络攻击行为屡禁不止。

地缘政治冲突：地缘政治冲突也是导致网络攻击事件频发的一个重要原因。在某些情况下，网络攻击被用作政治斗争的工具，通过攻击对方的网络基础设施或窃取敏感信息来打击对方。

黑客组织与个人恶意行为：一些黑客组织或个人出于炫耀技术、报复社会或实现其他非法目的，会主动发起网络攻击。这些攻击往往具有高度的隐蔽性和破坏性，给受害者带来严重的损失。

网络基础设施的脆弱性：许多网络基础设施在设计、建设和运营过程中存在安全漏洞和弱点，这些漏洞和弱点容易被黑客利用进行攻击。例如，一些公共无线网络由于缺乏足够的加密和安全验证机制，容易被黑客入侵并控制。

第二章 调查意义与研究目的

网络犯罪行为的危害体现在多个层面，其严重程度足以对个人权益、社会秩序、经济发展乃至国家安全造成巨大威胁。2024 年 3 月 29 日，全国打击治理电信网络诈骗工作视频会议召开，中共中央书记处书记、国务委员王小洪强调要依法严打电信网络诈骗犯罪，强化预防措施，加强源头管控，综合治理，以应对当前电信网络诈骗犯罪的新变化新趋势。所以遏制惩处违法犯罪行为迫在眉睫。

此次发布会的调查意义主要有以下三点：

1、深入理解公众对于共建“清朗”网络空间的新期待和新要求，以此为基础提升网络安全保障水平。

2、通过调查，掌握网民对网络空间安全感的感知，全面了解网络违法犯罪的现状。

3、为未来网络违法犯罪防治研究提供坚实的基础和明确的研究方向。

基于这些调查意义，我们进一步明确了研究的主要目的，具体包括以下三个战略要点：

第一，通过线上问卷调查，深入了解网民对网络安全感的感知程度，以及对政府打击网络违法和跨境诈骗力度的满意度，分析影响满意度的因素，收集公众对加强网络犯罪打击的期望与建议。

第二， 对比 2023 年数据，评估 2024 年网络违法犯罪的趋势和现有措施的效果，优化政府及相关机构的工作策略，减少网络诈骗事件，净化网络空间。

第三，识别网络安全的主要威胁，了解用户在遭遇网络安全事件时的应对方式，优化应急响应机制，推动网络安全技术和产品的研发，提高整体防御能力，建立信任体系，并通过持续监测和改进网络环境，逐步建立公众对互联网的信任。

第三章 研究方法

鉴于网络违法犯罪行为的复杂性和多样性，本研究旨在通过以下方法来揭示其成因并提出相应的对策。

聚类分析 (Cluster Analysis)：用于将数据集分组，使得同一组内的数据更相似，不同组间差异较大。这有助于将用户或网络犯罪行为划分为不同类型，以识别规律或重点关注的对象。

聚类的目标是最小化以下目标函数：

$$J = \sum_{i=1}^{k} \sum_{j=1}^{n_i} \| x_j^{(i)} - \mu_i \|^2$$

其中，k是行为聚类数量， n_i是第i个行为聚类中的样本数量,μ_i是第i个行为聚类的中心，$x_j^{(i)}$是第i个行为聚类中的样本。

克隆巴赫系数（Cronbach's Alpha）：针对样本数据的信度分析，用于衡量问卷各题目的一致性，消除了个体打分差异的影响，反映出了一个人在各题目间打分的波动情况，数值越接近 1 表示信度越高。

$$\alpha = \frac{N \cdot \bar{c}}{\bar{v} + (N-1) \cdot \bar{c}}$$

其中，N是题目数量，$\bar{c}$是题目间的平均协方差， $\bar{v}$是每个题目的平均方差。

偏相关分析 (Partial Correlation)：测量在控制其他变量的情况下，两个变量间的关系。例如，在控制年龄的前提下，评估受访者的教育水平与预防犯罪安全意识的相关性。

$$r_{XY.Z} = \frac{r_{XY} - r_{XZ} \cdot r_{YZ}}{\sqrt{(1 - r_{XZ}^2)(1 - r_{YZ}^2)}}$$

交叉分析（Crosstab Analysis）：也称为交叉表分析，是一种用于探索两个或多个分类变量之间关系的统计技术。在 4.3 节中，对网

络违法犯罪行为的载体分析涉及到交叉分析，以了解不同类型网络违法犯罪行为（如违法有害信息、侵犯个人信息、网络诈骗）在不同载体（如短视频 APP、社交媒体平台）上的分布情况。

推理统计（Inferential Statistical Methods）：通过样本数据来推断总体特征的统计方法。其中，T 检验是一种用于比较两组数据均值是否存在显著差异的统计方法。它基于样本数据计算出 t 值，通过与临界值比较来判断差异的显著性。在本研究中，我们将 2023 年和 2024 年的犯罪行为数据视为两个独立样本，通过 T 检验来评估它们在均值上是否存在显著差异。

根据样本数据，运用以下公式计算 t 值：

$$t = \frac{\overline{X_1} - \overline{X_2}}{\sqrt{\frac{S_1^2}{n_1} + \frac{S_2^2}{n_2}}}$$

其中，$\overline{X_1}$ 和 $\overline{X_2}$ 分别为 2023 年和 2024 年犯罪行为数据的均值，S_1^2 和 S_2^2 为相应的方差，n_1 和 n_2 为样本量。

比较结果：2023 年与 2024 年流量绑架行为和侵犯个人信息犯罪行为存在显著差异。

第四章 调查结果与分析

4.1 调查对象群体分析

本次问卷的调查群体具有行业广泛、性别比例均衡、年龄和学历层次多样以及网民角色以普通消费者为主等特点。通过对这些调查对象的分析，我们能够从不同的职业领域获取关于遏制网络违法犯罪行为的丰富观点和经验。

调查对象包括党政机关、事业单位的领导干部和一般人员，企业的管理人员和一般人员，专业技术人员，农林牧渔水利业生产人员，学生，自由职业者，无业/失业/退休人员等

从问卷中可以看出参加本次问卷的受访者有以下特点：

从性别比例来看，男女比例基本持平，仅 3%左右的差别，我们可以较为均衡地了解不同性别的用户对遏制网络违法犯罪行为的看法和态度；从年龄构成来看，大都在 10-49 岁之间，尤其集中在 20－29 岁的青年人和 10－19 岁的青少年，这个年龄段的人群在社会生活中活跃度高，对违法犯罪问题的感受更为直接；从学历及职业构成来看，约 86%是初中及以上学历，学生，企业/公司一般人员占比较高。学生是互联网的活跃用户，学生群体的参与为我们提供了年轻一代的视角，他们对网络的依赖程度高，面临的网络风险也较为突出，企业 / 公司一般人员在工作和生活中可能面临各种潜在的违法犯罪风险，他们的意见对于制定针对性的遏制措施具有重要意义；从在互联网生活中主要担任的网民角色来看，77%以上的人只是普通消费者，不从事互联网行业相关工作，他们作为社会的大多数，其对违法犯罪问题的感受和需求反映了广大民众的普遍关切。

4.2 用户反馈纪实：问题与反馈、感受与期望

1.【调查问卷全局统览】

本次调查所采用的问卷分为主问卷和专题问卷。主问卷主要是针对网民基本用网信息的调查，从主问卷中可以了解到网民的个人信息，观测到网民的用网情况，掌握实时困扰网民的网络安全问题，更好地认识民众的安全意识，也能更深入的感知到网民对当前网络环境及治理措施的安全感、信任度、危机感等整体满意度以及未来期望。如图 4.2.1 所示：

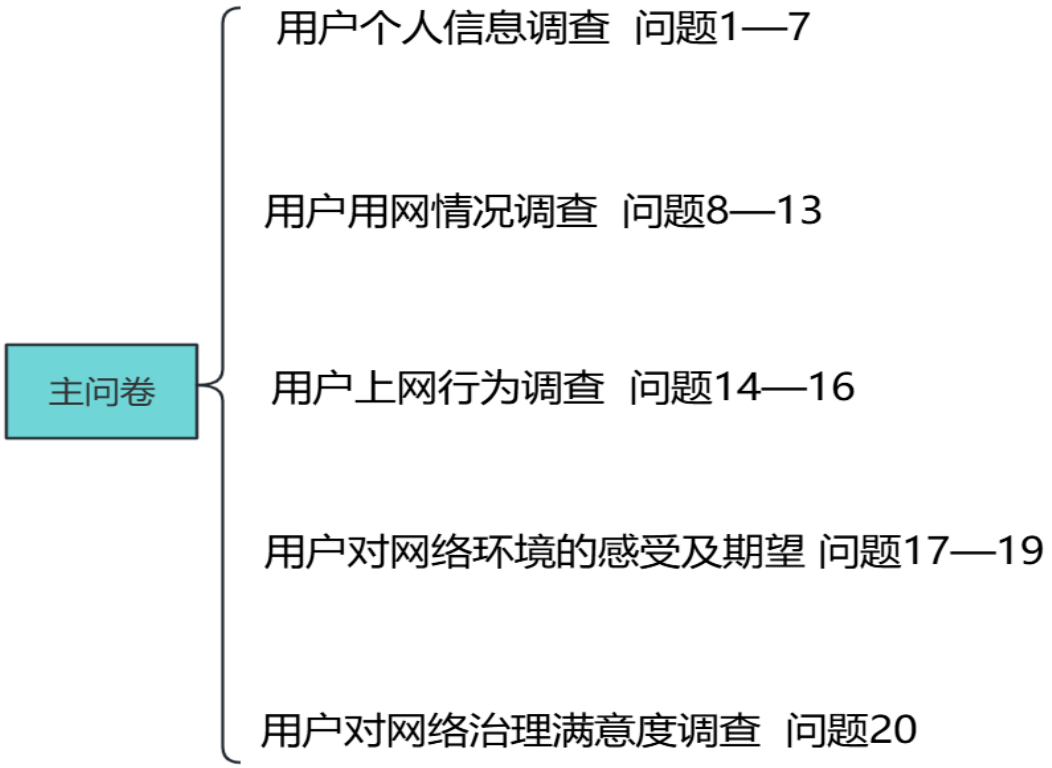


图 4.2.1

而在本次专题问卷调查中，除了对受访者个人情况的了解，主要聚焦于用户对侵犯个人信息、网络攻击、网络入侵、网络诈骗等违法行为的认知与感知。特别是，调查深入探讨了用户对网络诈骗的知识掌握程度及其采取的应对策略。同时，问卷还着重考察了用户对当前网络安全宣传的感知，以及他们对网络环境的整体满意度。此外，调查还特别关注了用户对于打击低俗违法信息和跨境诈骗等行为的治理成效的评价，以及对未来网络环境改善的期望。如图 4.2.2 所示：

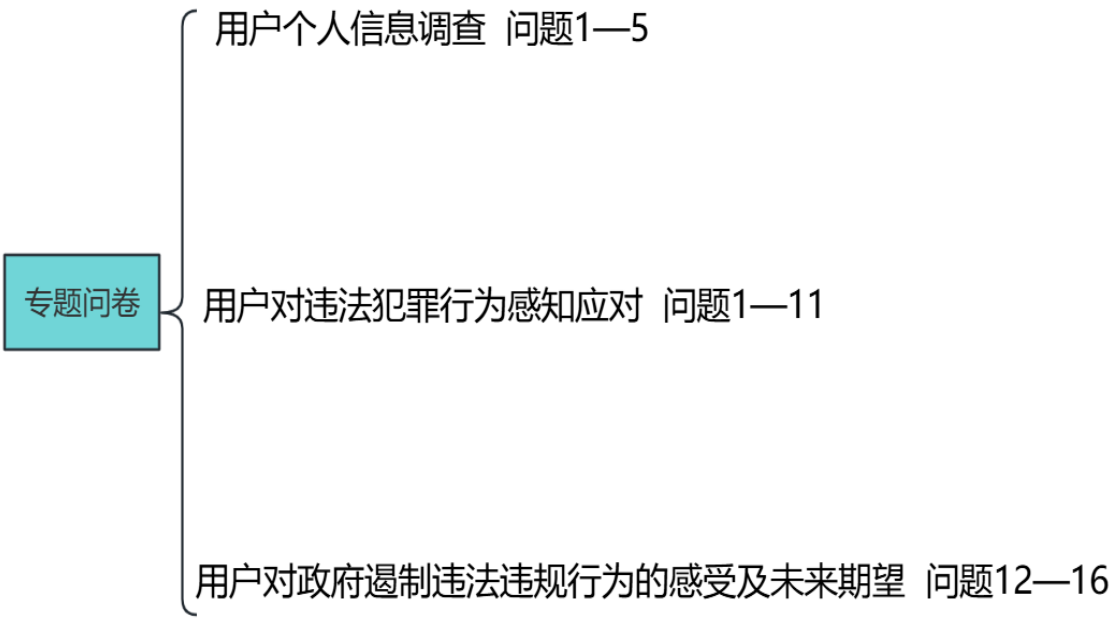


图 4.2.2

2.【网民用网行为分析】

如图 4.2.3 和 4.2.4 所示，通过细致分析所提供的数据，我们观察到 10 至 19 岁的青少年在社交应用的使用率达到了 8.95%，而进入 20 至 29 岁的年轻成年期，这一比例显著上升至 16.14%，凸显了年轻用户在互联网服务领域的领先地位。同样，这一年龄段在网络媒体（14.68%）、数字娱乐（12.90%）和电子商务（11.97%）等热门领域的活跃表现也颇为抢眼。随着年岁的增长，30 至 39 岁的成年人在电子商务（11.23%）和生活服务（10.49%）方面的参与度虽然有所降低，但仍维持在较高水平。相较之下，40 岁及以上的中老年群体在互联网活动中的活跃度明显下降，特别是 60 岁及以上的老年人群，他们在社交应用上的参与率降至 1.99%，在网络媒体上的参与率亦仅为 1.81%。这些数据明确地反映了一个社会趋势：随着年龄的增长，人们在网络空间的活动频率普遍降低，尤其在社交和娱乐等互动性较强

的领域。同时，这也揭示了不同年龄段用户在互联网服务需求上的偏好差异，年轻一代倾向于娱乐和社交活动，而中老年群体则可能更加关注健康医疗和生活便利服务。（交叉分析）

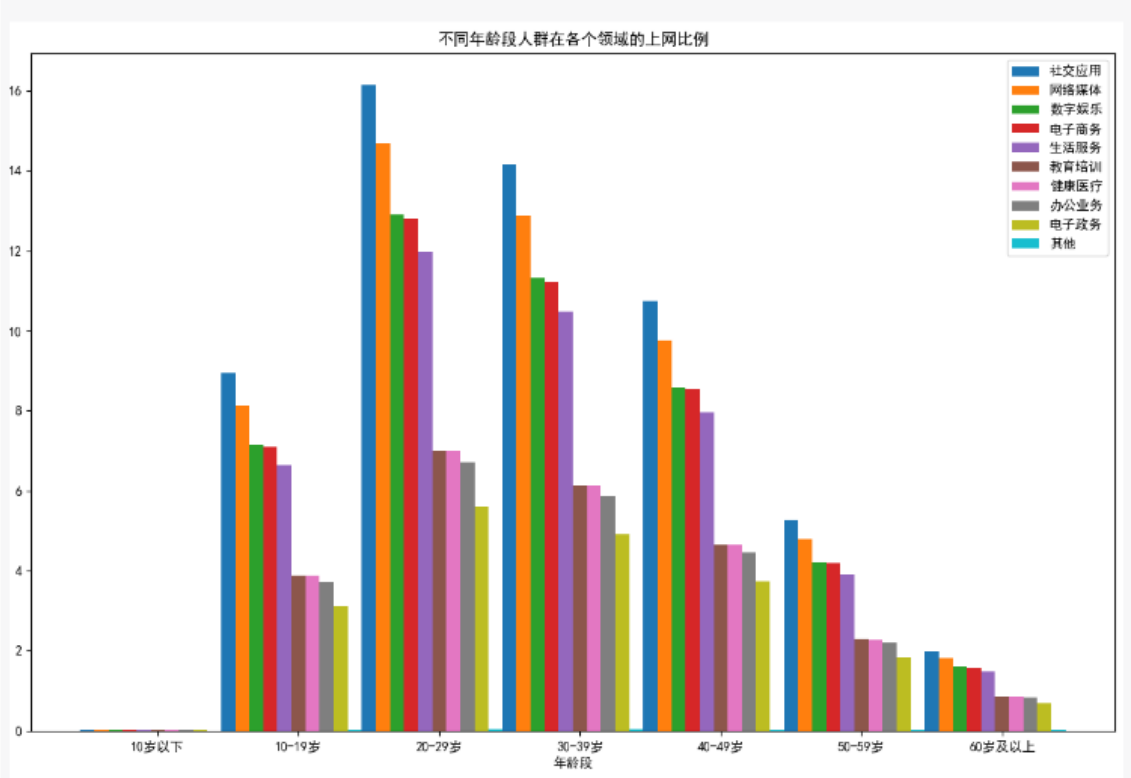


图 4.2.3

网络媒体	数字娱乐	电子商务	生活服务	教育培训	健康医疗	办公业务	电子政务	其他
0.03%	0.02%	0.02%	0.02%	0.01%	0.01%	0.01%	0.01%	0.00%
8.14%	7.15%	7.10%	6.63%	3.88%	3.87%	3.72%	3.11%	0.02%
14.68%	12.90%	12.81%	11.97%	7.01%	6.99%	6.71%	5.60%	0.04%
12.87%	11.31%	11.23%	10.49%	6.14%	6.13%	5.88%	4.91%	0.04%
9.77%	8.59%	8.53%	7.97%	4.66%	4.65%	4.46%	3.73%	0.03%
4.80%	4.22%	4.19%	3.91%	2.29%	2.28%	2.19%	1.83%	0.01%
1.81%	1.59%	1.58%	1.48%	0.87%	0.86%	0.83%	0.69%	0.01%

图 4.2.4

3.【反诈知识获取途径的多样化】

通过观察图 4.2.5，我们可以看到当聚类数为 3 时，惯性下降的

速度开始减缓，这表明 3 可能是最佳的聚类数。基于肘部图的分析结果，我们将使用 3 个聚类中心重新对数据进行聚类。（使用 KMeans 聚类方法）。

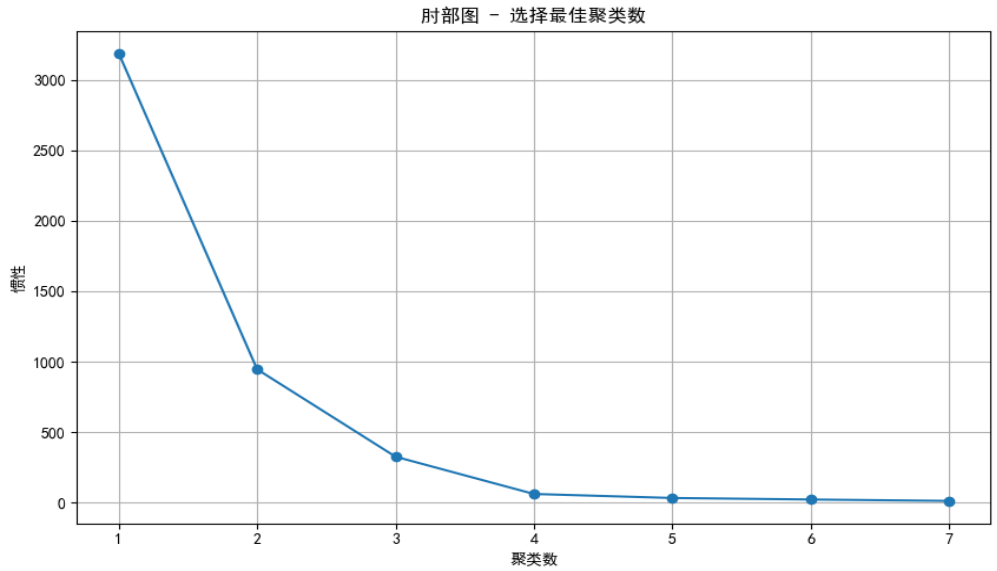


图 4.2.5

通过图 4.2.6 的分析，我们不仅观察到不同颜色的线条代表了不同的信息获取群体，还揭示了公众在防诈反诈知识获取上的偏好和行为模式。图中横轴展示了从新兴的数字媒体到传统宣传手段的多样化了解渠道，而纵轴映射了各渠道在全国范围内的普及程度，描绘了信息传播的全面图景。整体上，三条折线呈现出由左向右的递减趋势，表明在众多传播途径中存在明显的层级结构，一些途径被广泛接受和使用，而其他途径则相对边缘化，这反映了现代信息传播的快速变化及公众对不同信息来源的信任度和接受度差异。蓝色折线的高位显示警方短信提醒、社交平台和学校教育等现代化、互动性强的途径在信息传播中起到桥梁和纽带作用，普及率超过 35%。橙色折线所示的途径普及率较低，但仍有一部分人群通过社区讲座、专业研讨会等专业或小众方式获取信息。绿色折线揭示的现象最为引人注目，其最低的 1%普及率表明，通过公交、地铁广告、家长和教师指导、报纸、广播、电视等传统媒体及公安机关笔录了解防诈反诈知识的比例极低，暗示传统媒体作用减弱，公众信任度降低，特定群体接触机会有限。特别是绿色折线所代表的第三聚类中心的第二个样本，极低普及率可能指

向特殊或未广泛认知的渠道，如行业内部通讯或非常规信息发布平台，强调了未来宣传工作需关注信息传播多样性和受众差异化需求，以有效提升公众防诈意识和自我保护能力。

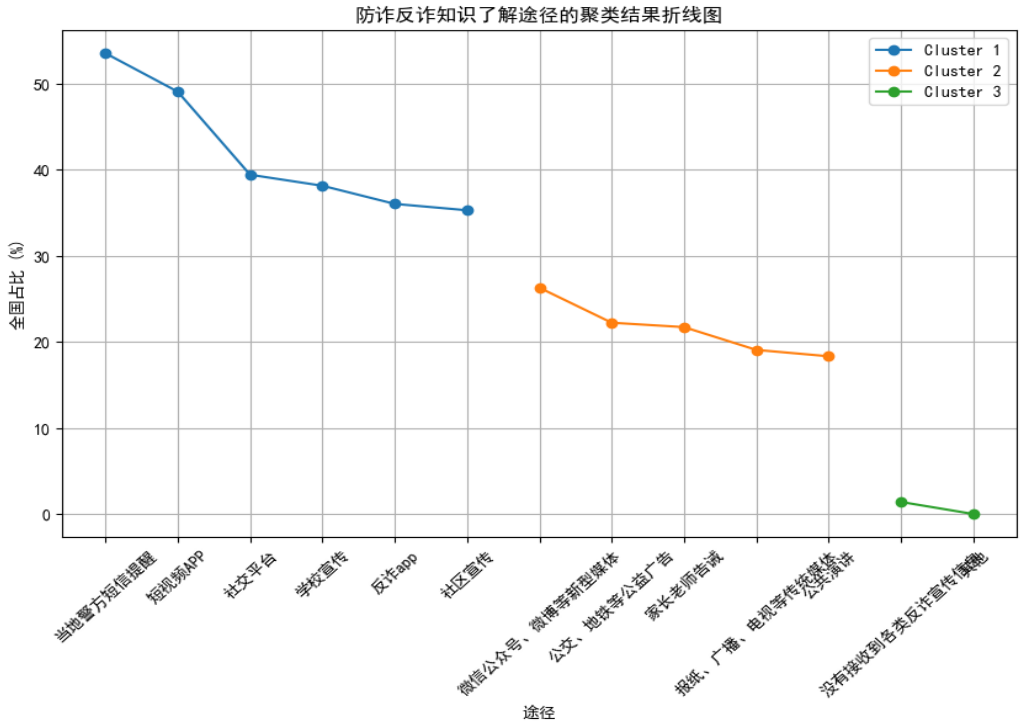


图 4.2.6

4.【网民对网络安全感知】

对于网民们的感受，首先，让我们聚焦网民对于网络空间整体安全的感知。根据我们的调查数据，从图 4.2.6 中清晰可见，高达 82.14%的网民对当前网络空间的整体感受给予了六分或以上的积极评价，较往年的 75.8%有了大幅的提升，这表明在大部分用户眼中，网络环境总体上是相对安全的，且高达 81.41%的用户对网络空间安全保障充满信心，也体现出近些年来政府对于网络的治理颇有成效，让网民信心大增。然而，当我们细化到网络实体与信息的信任度以及网络环境的不安定因素对意外风险的影响这两个层面，情况则稍显复杂。在这两方面，网民给出及格评价的比例分别下降至 78.15%和 73.52%，尽管较往年有所提升，但提升信息内容的可信度和网络环境的稳定性仍将是未来工作的重点方向。

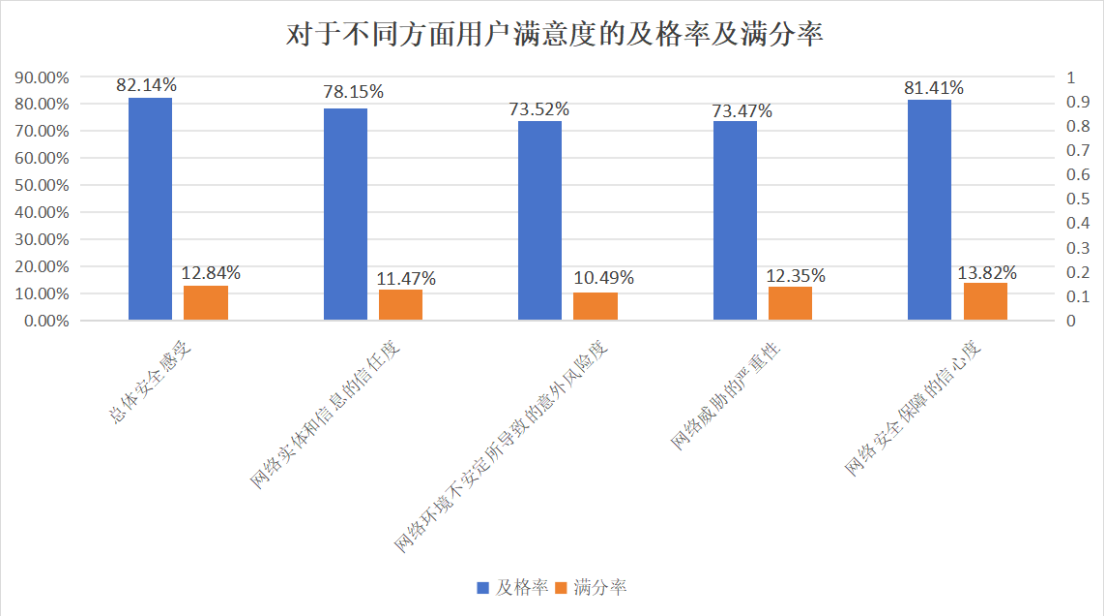


图 4.2.7

整体来看，虽然各个方面的及格率都在 70%以上，表明用户对这些方面的基本认可，但满意率普遍较低，说明用户在实际体验中可能存在不满或期望未能达到的情况。这提示相关机构需要进一步提升用户的满意度，改善用户体验。此外，对于网络威胁的严重性方面，网民的感受呈现两极分化的形势。一方面，对网络威胁严重性的满意度满分比例较高，反映出相当一部分网民在应对网络风险时具有较强的信心；另一方面，及格比例却相对较低，这暗示尽管遭遇网络威胁的网民群体比例较小，但一旦遭袭，其影响往往极为严重，损失程度不容忽视。

5.【专项监管行动成效分析】

接下来让我们聚焦于专项监管行动的效果。网信、公安等部门联合开展了“清朗”、“净网”等一系列专项行动，重点打击网络戾气及违法违规行为。根据下图，六成多网民对专项行动在遏制网络乱象方面的成效表示满意，仅有 9%的网民对工作成效不满意或不清楚。

通过对网民反馈的梳理，我们识别出当前网络治理面临的主要问题，包括治标不治本、网络违法行为频发、网络安全状况改善不足、行动效果短期化，以及黑灰产业链的持续存在、保护伞没有打掉等。

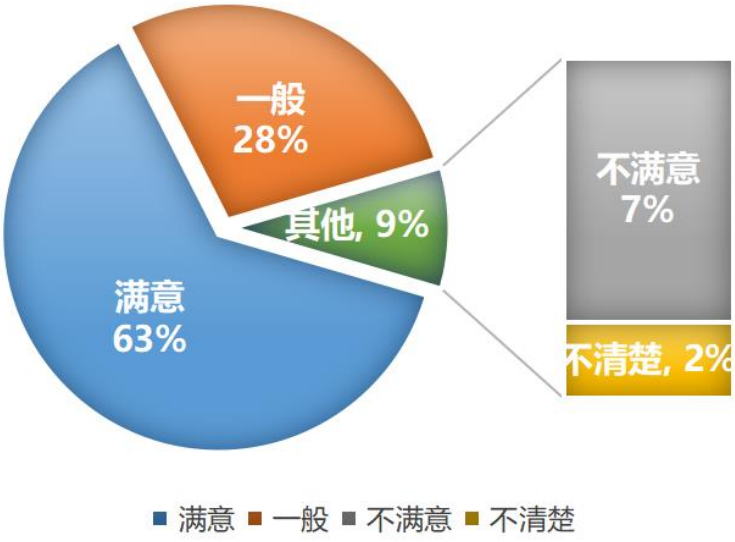


图 4.2.8

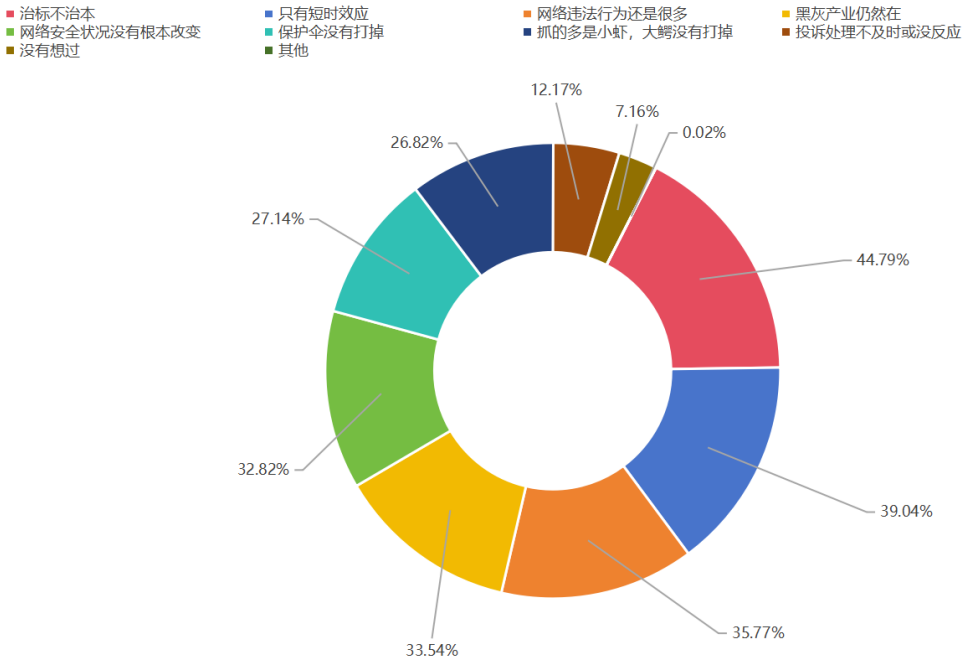


图 4.2.9

6.【问题反馈与未来展望】

随着网络技术的飞速进步，网络安全威胁也日益严峻。根据主问卷调查数据显示，63.92%的用户遭遇过网络暴力，而 35.58%的人个人信息安全受到侵犯。尽管如此，当面对这些问题时，只有 23.66%的用

户选择向公安部或网信办举报，显示出公众在应对网络安全事件时的犹豫与无力。

更令人担忧的是，31.87%的用户表示不再使用受影响的服务或采取任何措施，这反映出部分网民在面对网络安全问题时存在一定的放弃心态。与此同时，51.72%的用户在过去一年中没有改变其网络安全习惯，表明他们的安全意识并未得到显著提升。

值得注意的是，互联网服务提供商过度收集个人信息的做法仍然普遍且严重。超过四成的受访者报告收到过违法有害信息，近半数人经历过隐私泄露。这些数据揭示了当前网络监管和网络信息内容审核方面的不足，需要进一步加强和完善。

近年来，网络诈骗现象层出不穷，形式多样，甚至通过 APP、直播等新渠道进行传播，让人防不胜防。然而，48.31%的用户会在遭受诈骗时提醒家人同事，同时也有相当一部分人愿意向监管部门举报、向公安部门报警或向相关网站投诉，以阻止诈骗行为的蔓延和保护他人免受侵害。

综上所述，我国网络安全形势依然严峻，亟需加强网络监管和法律制度建设，提高公众的安全意识和自我保护能力，共同营造一个更加安全、健康的网络环境。

展望未来，我国网络安全形势的严峻性要求我们必须加强网络监管和法律制度建设，提升公众的安全意识和自我保护能力。我们期待通过全社会的共同努力，构建一个更加安全、健康的网络环境，以应对不断变化的网络安全挑战。

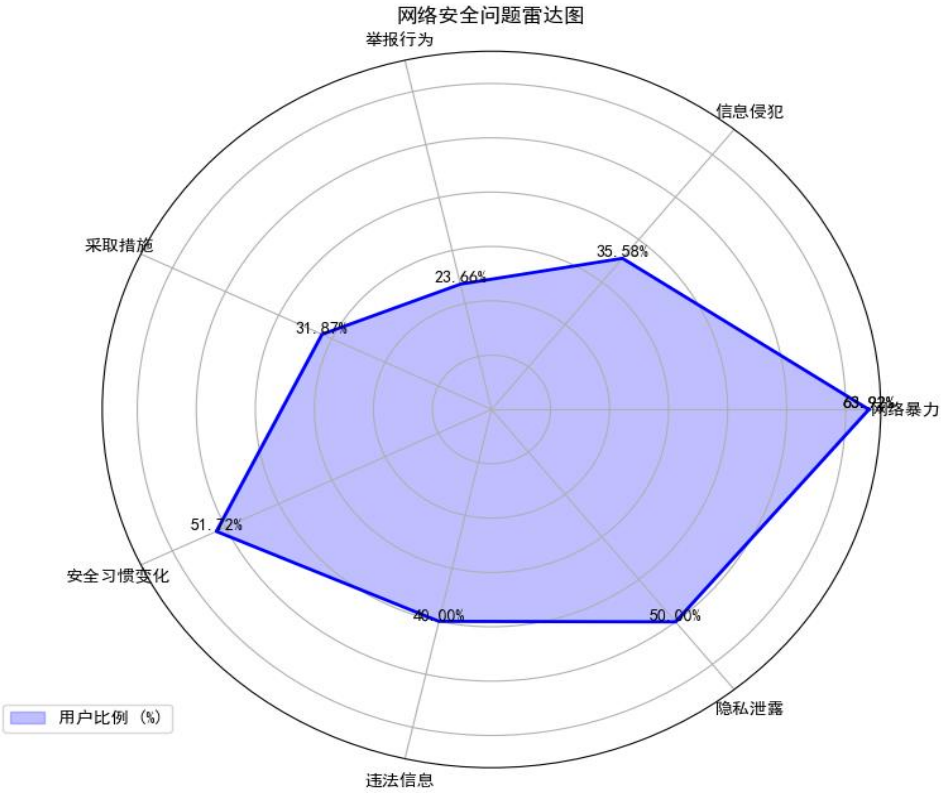


图 4.2.10

4.3 调查数据分析及对比

1.犯罪行为的波动分析

如图，在受访者使用网络时曾遇到过的违法犯罪情况中，违法有害信息占比 52.38%，位居第一，同样在 2023 年也是占比最多的，分别为 54.97%、54.69%。以浏览器绑架、流量窃取、软件捆绑下载等形式的流量绑架行为占比 33.19%，相较于 2023 降低约 3%。而网络诈骗犯罪和网络黑灰色产业的犯罪形式相较于 2023 升高。这表明网络犯罪形势复杂多变，既有上升的趋势，也有下降的趋势，需要持续关注并采取相应措施。

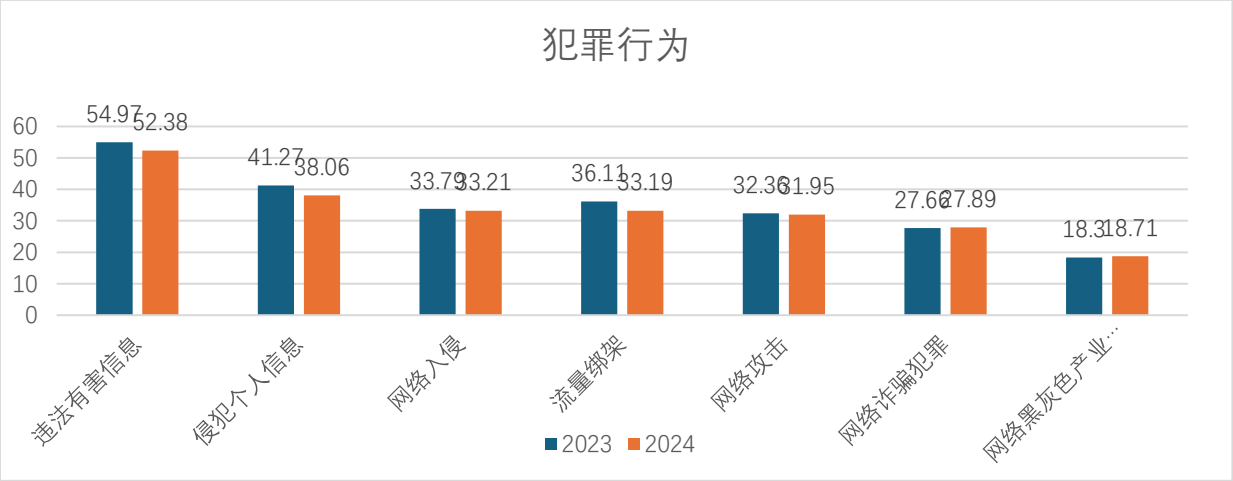


图 4.3.1 （1）

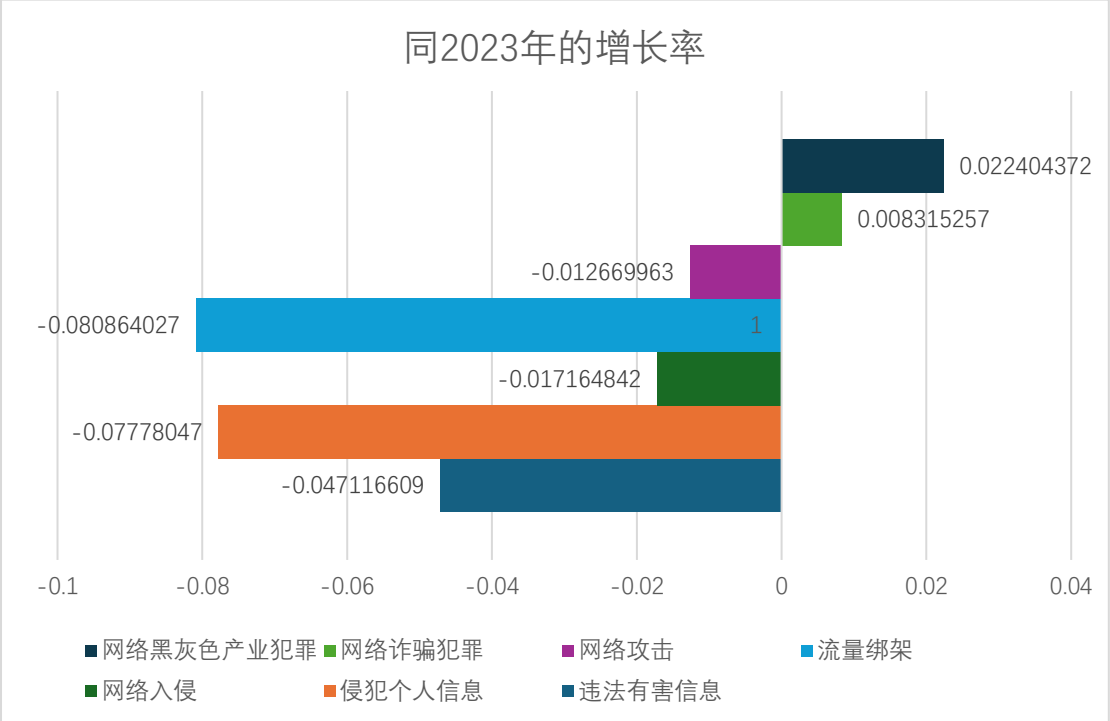


图 4.3.1 （2）

由此可见，网络违法犯罪行为与去年并无较大差异，但违法有害信息、侵犯个人信息及流量绑架等问题不容忽视，亟需社会各界共同努力，采取有效措施加以应对。

2.犯罪行为的载体分析

由问卷调查统计可知，无论是哪种形式网络违法犯罪，其载体均分布广泛。对网络违法犯罪行为的载体进行交叉分析，以了解不同类型网络违法犯罪行为（如违法有害信息、侵犯个人信息、网络诈骗）在不同载体（如短视频 APP、社交媒体平台）上的分布情况。

从图中可以看出，传播违法有害信息的网络违法犯罪行为，主要以短视频 APP、微信朋友圈或微信摇一摇、购物 APP 等为载体进行传播，其中短视频 APP 和微信朋友圈或微信摇一摇占比较高，分别为 45.91%、37.77%，可能是犯罪行为发生、传播或诱导的主要渠道。

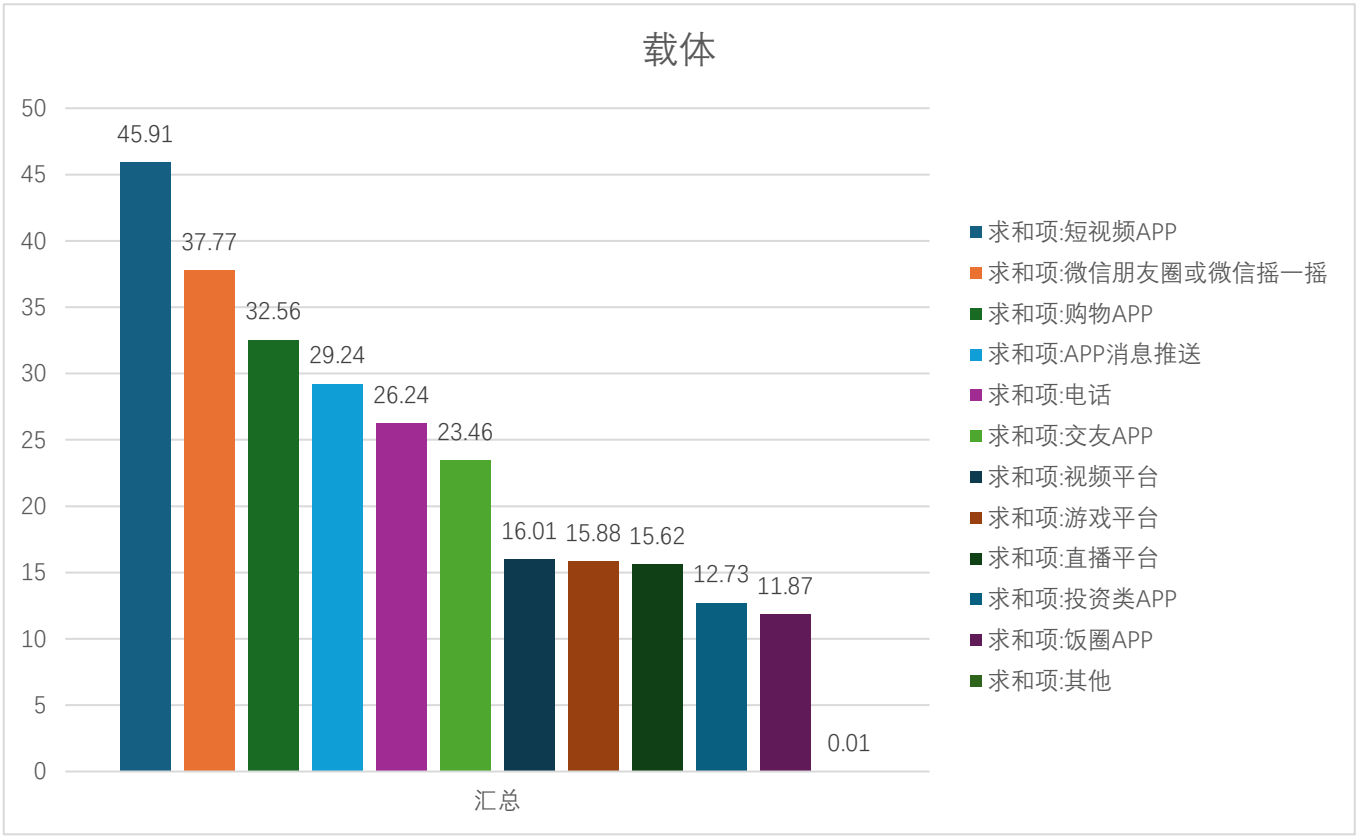


图 4.3.2

我们可以看到短视频 APP 和其他网络社交渠道成为网络犯罪的主要载体之一。随着互联网技术的发展和人们行为习惯的改变，我们应加强对主要载体的监管和打击力度，同时提高公众的网络安全意识。

3.犯罪行为的频率分析

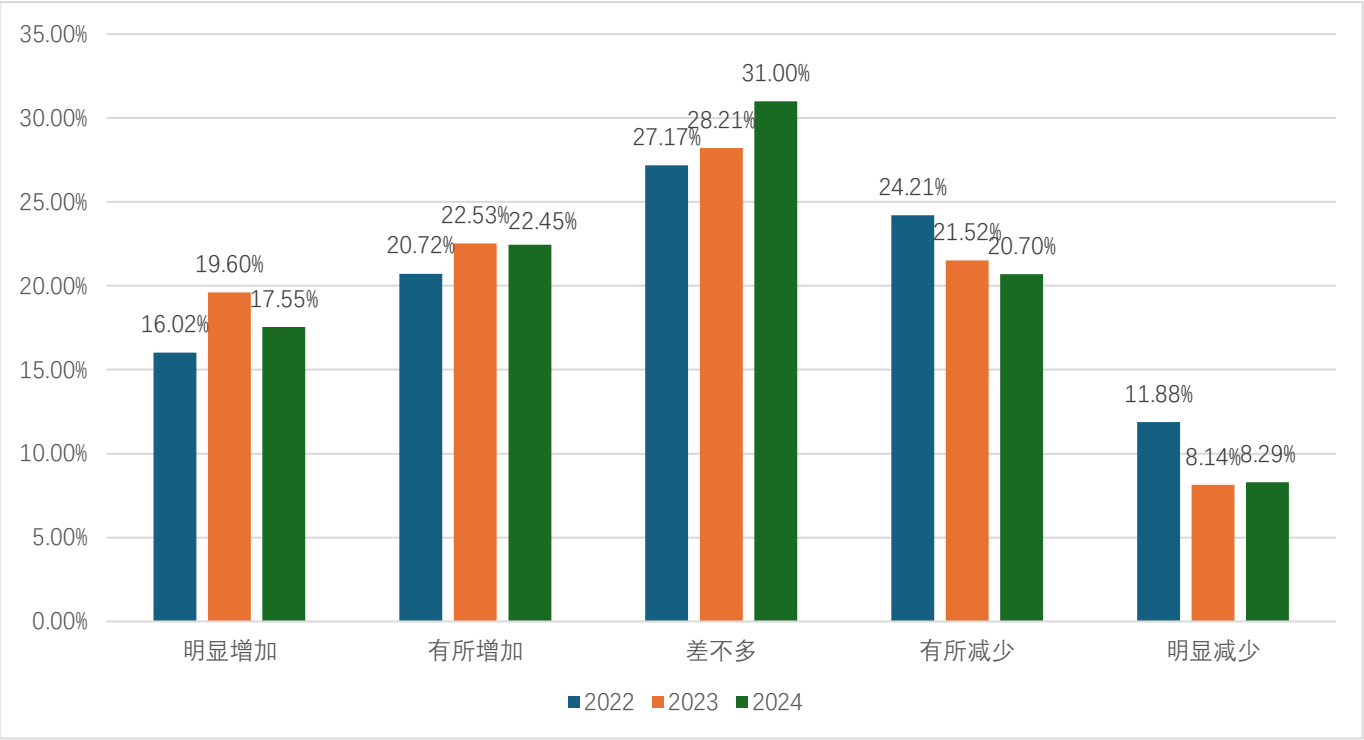


图 4.3.3

如图所示，三年的数据相差不大。这表明网络诈骗频率仍然较高，传统网络违法犯罪行为依旧猖獗，这与互联网技术的快速发展、网络空间的日益扩大以及网络犯罪分子的不断活跃有关。因此，网络诈骗的打击力度仍应加大，强化网络安全宣传教育，从而降低网络违法犯罪频率。

4. 预防为先的意识分析

在是否知晓官方的反诈服务渠道和平台的调查中，如图所示，知晓国家反诈中心 APP 的受访者占比由 2023 年的 33.94%增长至 2024 年的 68.1%，由三年数据可以看出，其他渠道和平台知晓程度相差不大。由此可见，我们在打击网络诈骗方面的宣传和教育取得了积极成效，对反诈的工作应继续坚持下去，让反诈意识深入人心。

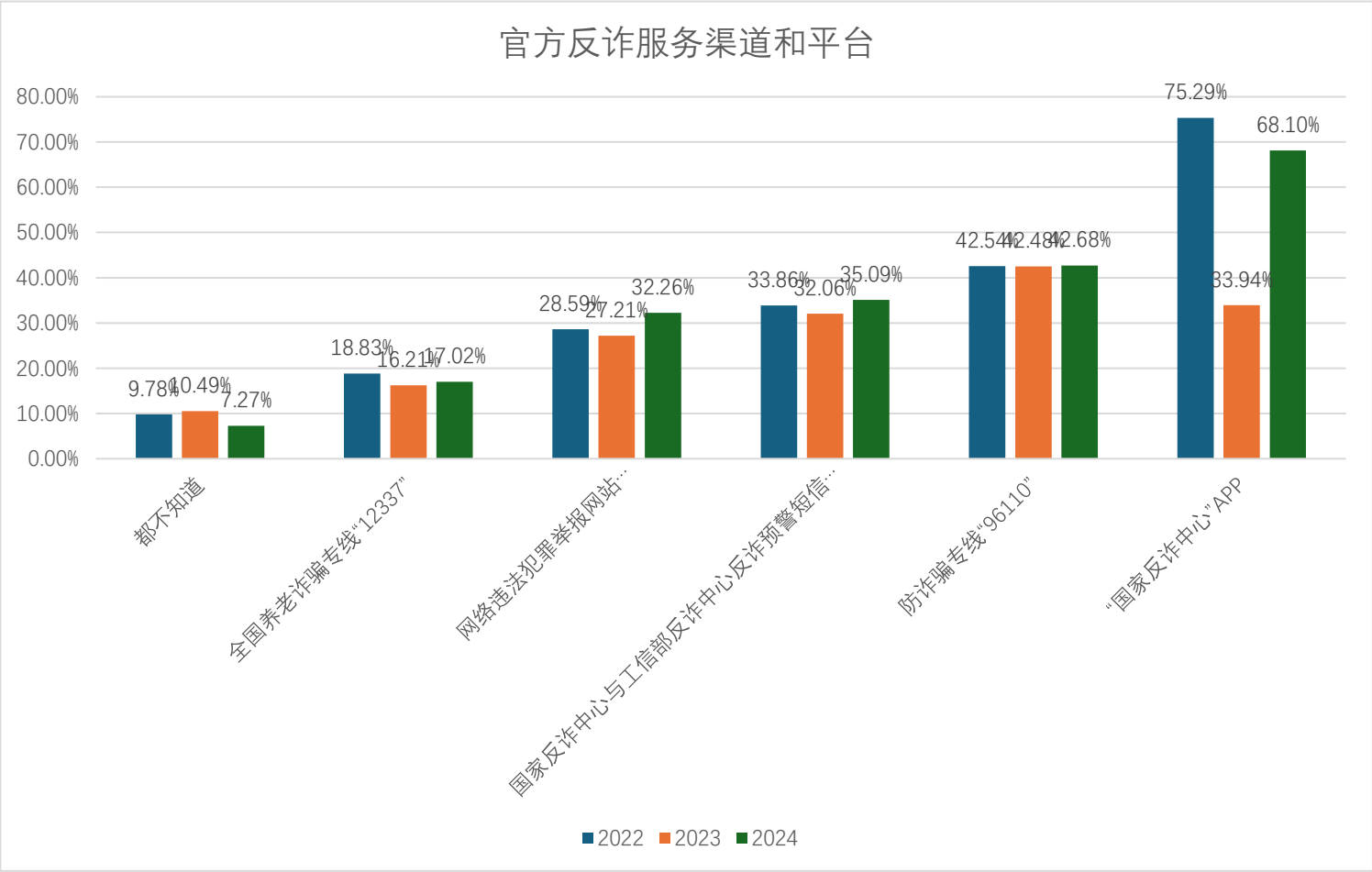
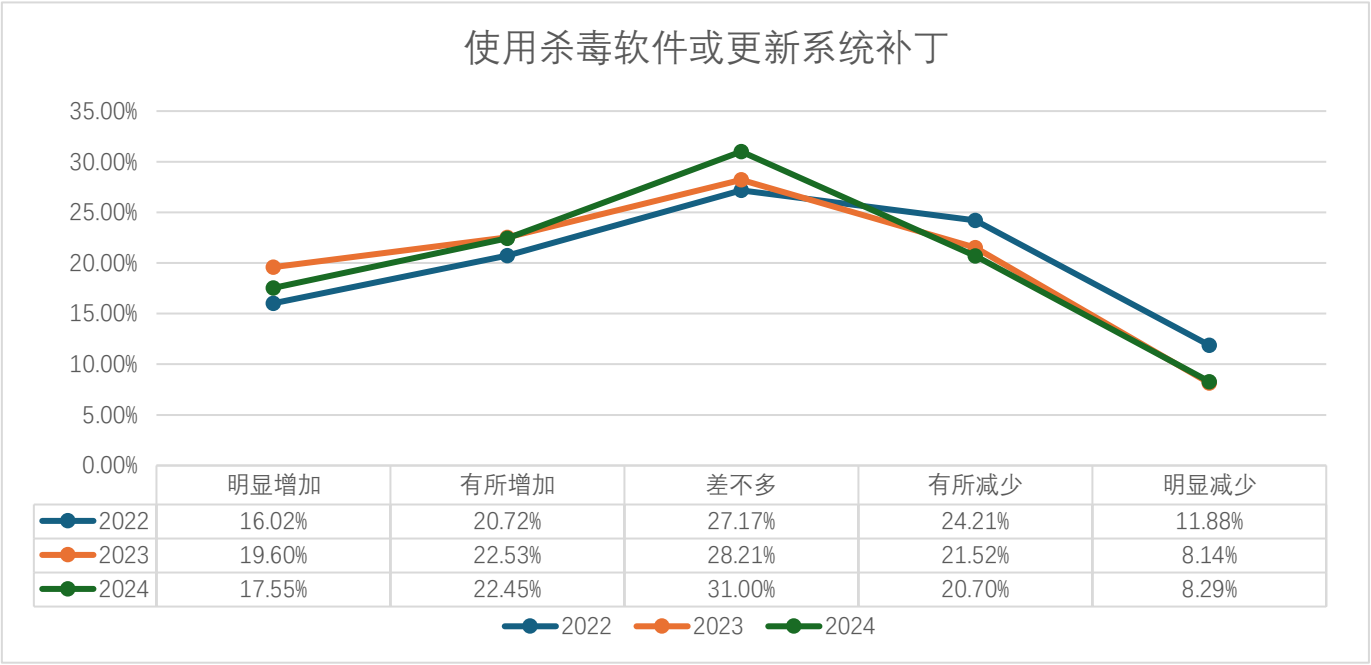


图 4.3.4

杀毒软件和系统补丁是保障用户计算机安全的一道重要屏障，如图所示，能定期使用正规杀毒软件或经常更新系统补丁的受访者，由 2023 年的 22.47%增至 24.71%，不定期（偶尔）占比最多为 31.53%。能定期和不定期使用杀毒软件或更新系统补丁的受访者相比于 2022 和 2023 年有所增加，可以看出公民防范意识有一定的提高，但仍有一部分人缺乏足够的预防意识，未能做到“居安思危，未雨绸缪”。



	明显增加	有所增加	差不多	有所减少	明显减少
2022	16.02%	20.72%	27.17%	24.21%	11.88%
2023	19.60%	22.53%	28.21%	21.52%	8.14%
2024	17.55%	22.45%	31.00%	20.70%	8.29%

图 4.3.5

5.地域数据的对比分析

如图所示，上海市，网络违法犯罪形式的比例均比全国占比低，其中 AI 诈骗、金融诈骗、电信诈骗等形式的网络诈骗犯罪占比 21.6%，比全国占比低约 6%。

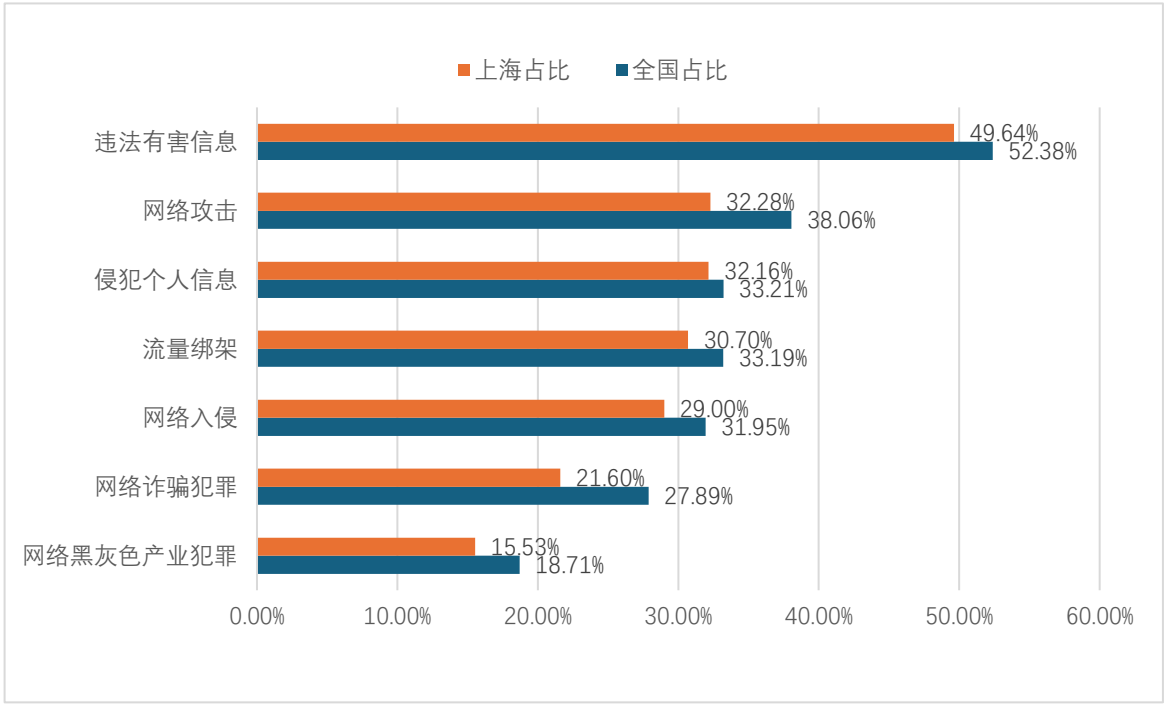


图 4.3.6

如图所示，云南省，民众遇到过各种形式的网络诈骗的比例均比全国占比高，其中以电话欠费、积分兑换、中奖诈骗的形式占比最高，为 46.42%。

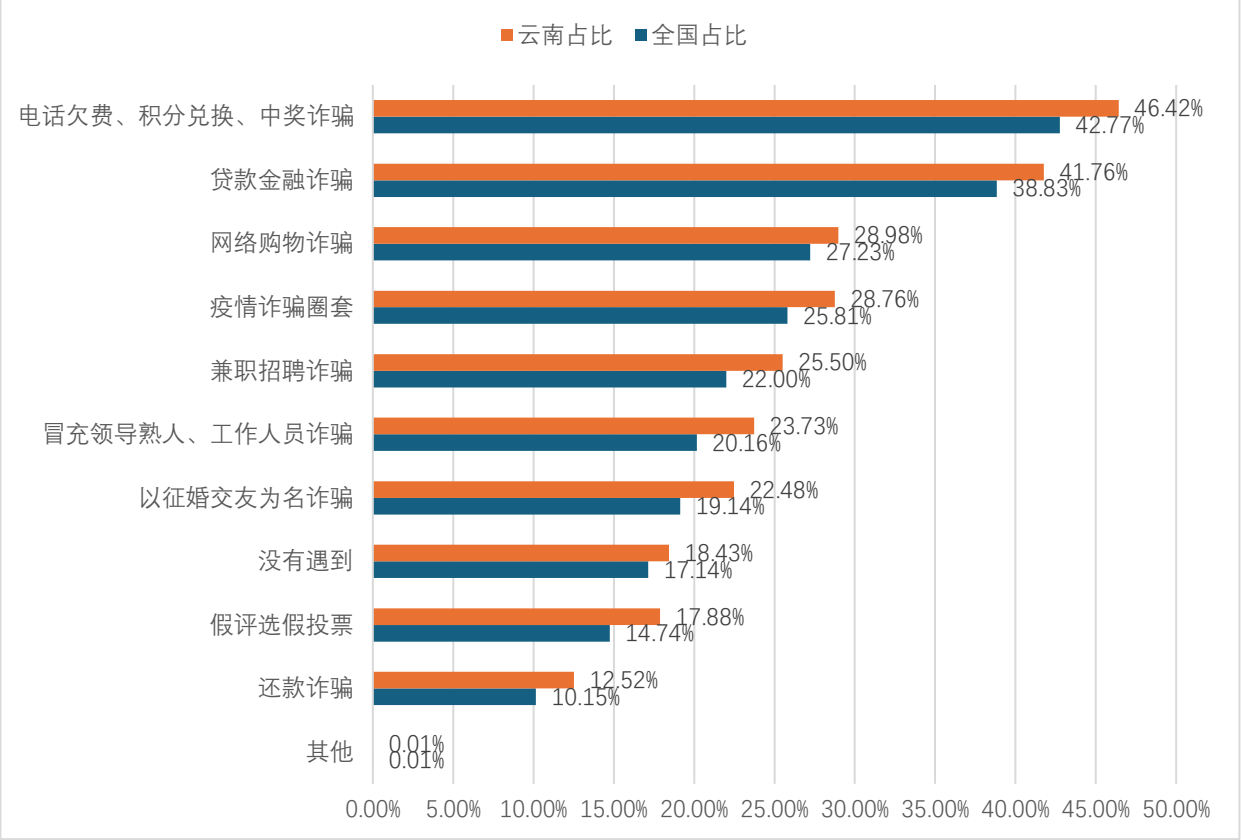


图 4.3.7

上海由于其经济发达、技术先进、执法严格以及网络环境规范等因素，使得其网络犯罪活动均比全国低。而云南则可能由于经济相对落后、执法难度较大以及地理和文化差异等因素，导致网络犯罪活动均比全国高。由此可以看出，地域差异以及发展不平衡是导致地区关于网络违法犯罪问题不同方面占比不同的重要原因。发展相对比较好的地区社会资源较为充足，包括反诈活动、法律援助、教育资源等等，能够有效地预防和打击网络违法犯罪行为。而有一些地区由于地域差异以及资源不平衡，整治力度不够，网络违法犯罪形式多样，民众防范意识不足。因此，因地制宜，合理高效地针对地区特点进行网络犯罪的预防和打击是尤为重要的。

第五章 社会影响

5.1 研究结果的社会影响

本次调查活动通过广泛的问卷调查和深入的数据分析，积累了大量关于网络违法犯罪的信息。这些数据不仅具备重要的学术研究价值，也在多个层面上体现了显著的社会价值。

首先，调查数据全面反映了当前网络违法犯罪的状况、成因及其影响，为政府部门制定更为精准有效的政策措施提供了坚实的基础。例如，自 2024 年以来，按照公安部“净网 2024”专项行动统一部署，全国公安机关持续开展了打击整治网络暴力违法犯罪专项行动，重拳打击通过网络实施侮辱谩骂、造谣诽谤、侵犯隐私等网络暴力违法犯罪活动，取得了显著成效。据统计，上半年全国公安机关共侦办网络暴力案件 3500 余起，依法采取刑事强制措施 800 余人，行政处罚 3400 余人。这一系列举措不仅有效地净化了网络环境，也为经济活动提供了一个更加安全可靠的平台。

其次，调查活动还激发了高校与企业在网络空间安全领域的合作。比如，“绿盟公益基金-教育奖助学金”的成立，旨在资助网络安全专业的贫困学生，促进该领域的教育与人才培养。再如，华中科技大学与天融信等企业共建校企实习基地；上海交通大学与奇安信科技集团股份有限公司合作建立了信息系统安全联合实验室；奇安信与郑州大学共建了“郑州大学智能数据安全产业院”，并通过设立“奇安信奖助学基金”支持该校网络安全学院的学生。此外，奇安信集团还与嵩山实验室签订了战略合作协议，双方将在网络安全前沿技术等方面展开深入合作，推动科研成果转化为实际生产力。

图 5.1“绿盟公益基金-教育奖助学金”成立仪式现场

图 5.2 天融信与华中科技大学共建“教学实习基地”

图 5.3 奇安信奖助学金捐赠暨发放仪式在郑州大学北校区举行

图 5.4 奇安信集团与嵩山实验室战略签约仪式

本次调查不仅为政策制定、公众教育、企业管理、技术研发等领域提供了宝贵的信息资源，而且促进了校企之间更紧密的合作，有助于提升全社会的网络安全意识和技术水平，进而促进社会和谐稳定与

经济健康发展。

5.2 研究结果对经济发展的意义

信息技术的快速发展使得互联网成为了推动经济增长的关键动力。然而，伴随而来的是信息安全威胁逐渐成为阻碍经济发展的重要因素。本次调查活动通过详尽的数据分析，揭示了网络违法犯罪行为对经济发展的多方面负面影响，其目的在于鼓励更多企业积极参与我国网络空间安全建设。

例如，北京奇安信科技集团股份有限公司在发布会上发布了《政务大模型安全治理框架》研究报告。报告指出，政务大模型正驱动政府数字化转型，提升服务效率，优化营商环境，简化审批流程，降低企业成本，吸引投资，促进产业信息化和智能化升级，增强区域竞争力。它还通过大数据分析，助力政府制定精准政策，推动经济高质量发展。政务大模型提供的个性化公共服务，如在线医疗和教育，提高了民众生活质量，刺激消费市场活力。然而，政务大模型的应用也面临安全的挑战，如数据泄露、内容违规和模型篡改等风险，可能对社会经济造成严重影响。研究报告深入探讨了这些问题，并提出安全治理框架。该框架通过多层次防护措施，确保政务大模型在数据处理、模型训练和应用过程中的安全性，有效避免经济损失，保障其在推动社会经济发展中的积极作用。通过建立这一安全治理框架，政务大模型将更稳健地支持数字政府建设，为经济的持续健康发展提供坚实支撑。

图 5.5 《政务大模型安全治理框架》封面

另一个例子是绿盟科技，该公司在调查期间定期发布《绿盟科技威胁周报》，及时通报最新信息系统漏洞并提供专业安全建议，帮助企业有效预防数据泄露和恶意攻击，从而减少了由网络安全威胁导致的直接经济损失，保护了企业的经济利益，同时也维护了整个社会经济环境的稳定。

图 5.4 绿盟科技威胁周报

本次调查活动不仅揭示了网络安全挑战，更强调了加强网络安全措施对经济健康发展的积极作用。希望更多企业和组织能从中认识到网络安全的重要性，积极参与到我国网络安全建设中，共同促进国家经济的稳定与持续发展。

第六章 调查报告总结与展望

6.1 调查报告总结

本次调查报告通过对网络违法犯罪的现状进行全面而深入的分析，揭示了当前网络空间存在的主要问题及其成因，并提出了切实可行的对策建议，为政府、企业和社会各界提供了重要参考。报告采用了多种先进的研究方法，确保了调查结果的科学性和准确性。特别是在利用互联网技术手段方面，报告通过线上问卷调查的方式，广泛收集了来自不同背景网民的意见和建议，实现了大范围的数据覆盖和高效的信息收集，展现了现代信息技术在社会科学研究中的巨大潜力。

调查结果表明，网络违法犯罪对社会的影响深远，涉及社会职能监管、网民自我保护意识、网络产品多样化、法律政策优化及网络安全技术提升等多个方面。同时，调查还揭示了网络违法犯罪对经济发展的负面影响，包括对企业竞争力、营商环境、技术创新、数字经济以及国际竞争力的影响。通过本次调查，我们不仅获得了大量的数据支持，也为未来的网络安全工作指明了方向。

6.2 可持续性展望与建议

未来，网络空间的安全挑战将持续演变，对网络违法犯罪的打击和预防工作也将面临新的任务和要求。为此，提出以下创新性和可持续性展望：

技术应用：探索和应用前沿科技，如区块链、大数据分析、人工智能等，提高网络安全防护水平。区块链技术用于数据存储和传输过程中的加密保护，确保数据的完整性和不可篡改性；大数据分析帮助识别网络犯罪的趋势和模式，为制定针对性的预防措施提供依据；人工智能则可以在网络攻击检测、风险评估等方面发挥重要作用，实现智能化的网络安全管理。

国际合作：建立更加紧密的国际合作机制，通过共享情报、联合执法等方式，形成全球性的网络犯罪打击网络。各国应积极参与国际规则的制定，推动形成公平合理的国际网络空间治理框架，为全球网络安全贡献力量。

普及教育：持续推动网络安全意识的普及教育，构建全民参与的

网络安全文化。通过开展形式多样的网络安全宣传活动，提高公众对网络安全的认识和自我保护能力，特别是加强对青少年的网络安全教育，从小培养他们的网络安全意识，为未来的网络环境打下坚实的基础。

长期跟踪研究：建立长期跟踪研究机制，定期发布网络安全状况报告，及时反映网络空间的新变化、新问题。这不仅有助于社会各界及时了解网络安全形势，也有利于政府部门和相关机构调整和完善政策措施。鼓励学术界和产业界加强合作，共同推动网络安全理论研究和技术应用的创新，为网络空间的长远发展提供智力支持和技术保障。

本次调查报告不仅为当前网络空间的安全治理提供了重要参考，也为未来网络空间的健康发展指明了方向。通过持续的努力和创新，网络空间必将变得更加安全、健康、和谐。

网安联微信公众号

网安联微信小程序

"网络安全共建网"官网

网安联秘书处

官网：www.iscn.org.cn

电话：020-8380 3843/13911345288

邮箱：cinsabj@163.com