互联网行业：2020 年网络安全威胁信息研究报告(2021 年)

2021 年 3 月 12 日，《中华人民共和国国民经济和社会发展第十四个五年规划和 2035 年远景目标纲要》正式发布，明确提出将“加强网络安全基础设施建设，强化跨领域网络安全信息共享和工作协同，提升网络安全威胁发现、监测预警、应急指挥、攻击溯源能力”

作为发展规划之一，对国家网络空间安全提出了更高的发展要求。

网络安全威胁信息作为发现网络威胁、抵御网络攻击的重要依托，助力信息安全防御手段向主动化、自动化、精准化转型，对于维护国家网络空间安全、建设数字中国具有重要意义。

2020 年新冠肺炎疫情爆发后，线上办公的广泛普及加剧了信息传递对网络的依赖，催生了愈加频繁的网络攻击行为。网络攻击的产业化发展趋势使得攻击工具和手法变得愈加复杂多样，传统的防火墙、入侵检测技术、恶意代码扫描、网络监控等被动防御手段显得捉襟见肘疲于应付。面对日益严峻的网络空间安全威胁，研究网络安全威胁信息有助于企业更好“知己”“知彼”，了解自身的网络安全脆弱点，掌握已知、未知的网络安全风险点，不断提升自身在实战中的检测与响应能力，筑牢网络安全防御城墙。

本报告从定义内涵、应用价值、标准化进展、政策和产业支撑等多个方面阐述了网络安全威胁信息的概念和发展现状。结合 2020 年全球网络安全威胁信息，从网络环境安全现状、常见网络攻击手法、受攻击行业和地域分布、国内较严重网络威胁及攻击事件等多维度系统性分析了 2020

年国内外网络安全形势。阶段性梳理了网络安全威胁信息在国内重点行业的典型应用案例。最后，围绕发展中存在的标准化落地不足、共享机制缺失、产业成熟度较低等诸多问题进行了探索性思考，结合产业现状提出了针对性的意见和建议。

对于本报告中的局限与不足，恳请各方同仁批评指正。

关键词：新冠肺炎 疫情 网络安全