

大数据时代的网络空间安全风险与防御

周剑勇

云南金质信息技术服务有限公司, 云南 昆明 650000

DOI: 10.61369/TACS.2025060011

摘 要 : 当前, 我们已然步入了大数据时代。大数据、互联网等技术在为人们生活各个领域提供便利的同时, 也带来了一定的网络空间安全问题。在此背景下, 立足新的时代背景并积极探索大数据时代下网络空间安全风险与防御对策势在必行, 正当其时。本文在分析大数据时代的网络空间安全防护的重要性的同时, 就大数据时代的网络空间安全的风险与防御对策进行了探讨, 以期能够给相关人士提供一些参考借鉴。

关 键 词 : 大数据; 网络空间; 安全风险; 防御对策

Cybersecurity Risks and Defense in the Era of Big Data

Zhou Jianyong

Yunnan Hi-Q Information Technology Service Co.,Ltd, Kunming, Yunnan 650000

Abstract : At present, we have already entered the era of big data. While technologies such as big data and the Internet provide convenience to various fields of people's lives, they also bring certain cybersecurity issues in cyberspace. In this context, it is imperative and timely to base ourselves on the new era background and actively explore cybersecurity risks and defense countermeasures in cyberspace in the era of big data. This paper analyzes the importance of cybersecurity defense in cyberspace in the era of big data, and discusses the cybersecurity risks and defense countermeasures in cyberspace in the era of big data, in order to provide some reference for relevant personnel.

Keywords : big data; cyberspace; security risks; defense countermeasures

随着数字技术的飞速迭代, 大数据时代已全面来临。大数据技术被广泛应用到了社会各个领域之中, 成为推动经济与社会发展的重要动力。但是, 大数据技术有着明显的开放性、双面性特点, 这也对网络空间安全环境带来了巨大冲击, 尤其是会带来数据泄露、网络攻击、数据安全以及隐私保护等诸多风险问题^[1]。在此背景下, 深入分析大数据时代的网络空间安全防护的重要性, 探索大数据时代的网络空间安全风险与防御的有效对策有着重要的现实意义。

一、大数据时代的网络空间安全防护的重要性

(一) 保障个人信息权益的核心防线

在大数据时代下, 网络空间安全防护对于个人的信息权益保障和隐私防护有着重要价值。当前, 大数据已经融入到人们生活各个领域, 个人的吃穿住行等各种活动中都可以看到大数据的身影。同时, 在人们生活过程中也会产生个人信息、位置信息以及消费信息等各种敏感数据。而这些数据一旦泄露将会对个人的日常生活以及隐私安全带来巨大冲击^[2]。例如, 当个人在某电商平台的消费数据泄露之后, 很可能受到网络诈骗的威胁, 进而冲击着他们的财产安全。又如, 当个人的隐私信息, 如照片、视频等泄露之后, 很可能会导致其出现名誉危机进而影响其正常生活。所以, 在大数据时代下, 积极构建网络空间安全防护体系能够有效保障个人信息权益, 避免其受到相应的风险侵害。

(二) 维护企业稳定运营的关键支撑

对于企业来说, 在大数据背景下, 他们对于大数据、互联网

等新兴科技的依赖度也是比较高的, 如在产品研发、客户开发、销售推广、售后服务等各个环节都需要大数据技术来支持。而这些数据当中往往包含着客户信息、商业机密、产品专利等关键信息, 如果这些信息出现泄露的话, 不但会影响到企业自身的品牌名誉, 而且也会直接影响到他们的正常运行^[3]。例如, 在金融企业中, 如果客户信息被泄露的话, 往往会导致企业出现信任危机, 或面临巨大的经济赔偿与损失风险。此外, 在大数据背景下企业网络空间安全事故的出现也会进一步冲击着他们的市场影响力和竞争力, 从而使其难以稳定地运行与发展。所以, 大数据时代下的网络空间安全防护能够为企业的稳定运营带来关键性的保障和支撑。

(三) 保障国家网络空间主权的重要基石

当前, 大数据在国家各个领域都有着深入的应用。但是, 可以看到, 一些关键领域的的数据信息依然面临着较大的安全风险, 如果这些领域出现网络安全问题时, 极可能影响到整个社会秩序。例如, 税务领域出现网络空间问题时, 往往意味着其关键信

息被泄露，而这也直接威胁国家的信息安全。所以，网络空间安全防御体系的构建是新时期推进“安全中国”建设的重要一环，对于国家网络空间主导权的维护以及整体安全的保障有着重要意义。

二、大数据时代的网络空间安全的风险探讨

（一）数据泄露风险：海量数据存储与传输中的隐患

在大数据时代下，数据泄露是主要的网络空间安全风险类别。通常来说，其主要潜藏在数据储存以及传输等环节之中。首先，在数据储存环节中，一些单位或企业主体往往借助服务器集群等方式来进行数据存储，但这些集群平台也有着一定的安全漏洞，加上一些企业并没有建立相应的网络空间安全防护机制，直接加大了其网络信息泄露的风险^[4]。例如，一些中小型企业因为资金成本方面的压力，并没有选择优质的存储服务器系统，这也使得他们无法很好地保障敏感信息安全，面临着巨大的数据泄露风险。其次，当前一些单位或企业相关人员在网络空间安全意识和能力方面存在不足，这也使得他们在工作中可能出现疏忽等情况，导致敏感信息泄露，进而影响到其正常运行与发展。

（二）网络攻击升级风险：针对大数据系统的新型攻击手段

网络攻击是常见的网络空间安全问题，其有着较强的突发性与复杂性特点。以往的网络攻击大多是通过简单的手段来对单一的目标进行攻击，但是随着大数据时代的来临，网络攻击依托大数据技术能够实现精准化、多点化的攻击^[5]。例如，一些黑客借助大数据技术来找到企业的系统弱点、网络安全体系薄弱之处进行精准攻击，这也直接影响了企业的信息安全。同时，当前一些网络攻击也运用了分布式拒绝服务（DDoS）技术，这种类型的网络攻击不管是规模还是破坏力都比较大，会直接导致被攻击目标的服务器出现瘫痪情况。此外，随着人工智能技术的发展，基于 AI 技术的网络攻击手段开始出现，他们有着较强的智能性特点，会给大数据系统的安全带来巨大威胁

（三）数据质量安全风险：虚假数据与数据污染的影响

数据质量安全风险也对网络空间安全构成重要影响，主要表现为虚假数据与数据污染带来的危害。通常来说，大数据有着用户自主上传、社交平台等多种来源渠道，其具体的内容与质量也有着较大的差异，一些信息本身就属于错误或者是虚假的信息，如果没有进行有效的验证和筛选就直接使用的话，会带来巨大的负面问题^[6]。例如，个别企业在对市场进行调研时，如果贸然采用虚假市场客户反馈信息的话，很可能会影响到其自身的决策，冲击他们的生存与发展。所以，在大数据时代下，如何有效应对数据质量安全风险，排除虚假信息与信息污染的冲击也是网络空间安全防御体系构建的重要内容。

（四）隐私保护风险：数据过度采集与滥用的挑战

隐私保护风险在大数据时代愈发凸显，主要源于数据的过度采集与滥用。可以看到，当前一些企业主体为了追求更高的利益，就不顾消费者个人信息与数据隐私，选择过度采集用户信息。例如，一些手机 APP 软件在安装时强制要求获取用户的个人

通讯率、位置信息、相册信息等数据，而如果用户不同意的话，则他们无法使用这些 APP。又如，一些 APP 在用户注册时，要求用户填写家庭住址、电话等详细信息，这些信息如果被泄露的话，都会给个体财产、安全等带来巨大威胁。

三、大数据时代的网络空间安全风险的防御对策

（一）强化技术防护：构建多层次数据安全防护体系

技术防护是抵御网络空间安全风险的核心屏障，需覆盖数据从产生到销毁的全生命周期，形成多层次、立体化的防护网络^[7]。首先，在数据采集环节可以引入“数据脱敏”技术，以此来对相关数据进行“去标识化”处理，更好地提高其安全防护等级，减少泄露风险。其次，在数据储存过程中，应当引入较强的数据加密技术，如可以采取 AES-256 算法来对相关数据进行加密，或者通过多节点备份等方式来防止数据丢失。在此基础上，还可以基于云存储方面的安全防护需求推进云平台自动检测技术和扫描系统的融入，以此来更好地检测可能存在的信息安全漏洞，及时消除信息安全问题。再者，在数据传输过程中，可以引入 SSL/TLS 安全传输协议，从而更好地保障数据的安全传输，减少可能存在的泄露以及窃取等风险。而对于企业来说，应当提高对网络空间安全的重视度，加大相关资金与技术投入，同时引入传输白名单等机制，限制异常 IP 访问，以此来更好地保障信息数据安全性。

（二）完善法规制度：健全网络空间安全法律保障体系

法规制度是网络空间安全防御的“硬约束”，需通过完善法律框架、细化监管标准，为安全防御提供明确依据。对此，相关部门应当立足于大数据时代背景，加快制定和完善关于网络空间安全方面的法律条例，如针对 AI 技术的不断发展与运用，对《中华人民共和国个人信息保护法》等进行完善，明确网络空间安全风险方面的责任与处罚措施。在此基础上，要推进公安部、网信部、工信部以及市场监管部等多个部门与领域的协同配合，打造跨部门、协同化的网络安全监管体系，及时发现和处理风险异常问题，更好地保障网络信息与数据安全^[8]。再者，应当鼓励广大企业或行业协会加快制定大数据安全技术规范或者开发相应的网络空间安全标准，以此来全面提高企业的网络空间安全等级。

（三）提升管理水平：优化大数据安全管理机制

管理水平如何直接影响着网络空间安全防御质量。对此，企业与机构等相关主体一方面要加快成立关于网络信息安全的防护、监管机构，配备专业的人员来维护自身网络空间与信息安全；另一方面要积极推进数据访问权限管理制度、安全审计制度、应急响应预案等机制的建立，以此来更好地维护自身的网络空间安全^[9]。此外，还应定期展开专业化的安全风险评估工作，对自身的网络空间安全情况进行评估排查，如可以和专业机构进行合作，全面检测自身网络空间存在的安全隐患与漏洞，及时制定方案进行优化处理，从而全面提升自身的网络空间安全等级。

（四）加强人才培养：打造高素质网络空间安全人才队伍

人才是网络空间安全防御的“核心资源”。在大数据背景下，面对网络空间安全风险与问题，必须要强化专业化人才培养。首

先,对于企业而言,为了更好地应对大数据时代的网络信息安全问题,应当积极开展安全培训工作,不断提高内部人员对于网络信息安全的重视度与认知。例如,可以定期邀请相关专家来展开网络空间安全、信息安全、常见防范措施等方面的专业培训,不断强化人员的网络信息安全意识,提升他们的风险防范和安全防护能力。同时,企业方面也要积极引入一些专业人员担当网络空间安全防护者的角色,维护自身的信息与数据安全。其次,对于高校而言,应当发挥好自身高素质人才培养的重任,不断优化网络空间安全相关专业课程设置,增加大数据安全、AI 安全防护、隐私计算等前沿内容,同时和企业等主体之间进行密切合作,为学生提供良好的实践机会,提升他们的专业能力^[10]。再者,相关

部门也应积极开展一些网络安全方面的技能大赛、知识竞赛,以此来营造良好的网络空间安全氛围,激发高校、企业在高素质网络空间安全人才建设方面的积极性,为网络空间安全防御体系的构建奠定坚实的人才基础。

总之,在大数据背景下,积极构建网络空间安全防御体系有着重要的现实意义。对此,我们有必要在把握大数据时代的网络空间安全风险类别的同时,积极探索有效的对策和路径,尤其是通过强化技术防护、完善法规制度、提升管理水平、加强人才培养等方式来有效构建现代化、安全化的网络空间安全防御体系,从而更好地发挥大数据的价值,推动社会经济健康可持续发展,保障个人、企业和国家的网络安全。

参考文献

-
- [1] 孙玉琴. 大数据时代公民信息安全面临的问题及解决建议 [J]. 办公室业务, 2024, (22): 40-42.
- [2] 赵一畅. 大数据时代的网络空间安全风险与防御 [J]. 数字通信世界, 2024, (10): 75-77+80.
- [3] 甘加燕. 大数据时代网络空间安全态势感知技术思考——评《网络空间安全防御与态势感知》[J]. 安全与环境学报, 2024, 24(06): 2472.
- [4] 杨亚. 大数据时代网络意识形态安全建设探赜 [J]. 领导科学论坛, 2024, (02): 84-87.
- [5] 匡一帆. 大数据时代加强网络信息安全建设的现实困境与突围路径 [J]. 科技传播, 2022, 14(09): 125-128.
- [6] 于湛璇. 大数据时代人工智能技术在网络空间安全中的应用研究 [J]. 无线互联科技, 2021, 18(24): 110-111.
- [7] 宋瑞娟. 大数据时代我国网络安全治理: 特征、挑战及应对 [J]. 中州学刊, 2021, (11): 162-167.
- [8] 丁爱萍. 大数据时代网络信息安全及对应策略研究 [J]. 电子技术与软件工程, 2021, (16): 253-254.
- [9] 高增荣. 大数据时代人工智能在计算机网络技术中的应用 [J]. 中国新通信, 2021, 23(12): 116-118.
- [10] 刘雪婷. 大数据时代高校网络信息安全法制教育研究与实践 [J]. 邵阳学院学报 (社会科学版), 2021, 20(02): 94-98.