大数据背景下计算机信息技术在网络安全中的应用路径分析

贺小芳，周绍勤
浙江丰汇恒信息科技有限公司，浙江 杭州 311199
DOI: 10.61369/TACS.2025070023

摘　　要： 互联网的出现与普及，带领我们迈入大数据时代。以计算机信息技术革新，应用于网络安全领域，一方面提升处理效率、防护能力，但也在另一方面无形加重了网络安全负担，数据泄露风险增加、人员制度管理难度增加。从某种程度上来说，互联网、大数据等都是一把双刃剑，如何在网络安全领域发挥积极防御能力，还需要加强相应积极效用，削弱负面影响。因此，本文探讨大数据与计算机信息技术内涵，并就当前计算机信息技术在网络安全领域的应用提出更多发展路径，希望能够为相关从业者提供更多借鉴与参考。
关 键 词： 大数据；计算机信息技术；网络安全；应用

Analysis on the Application Paths of Computer Information Technology in Cybersecurity under the Background of Big Data

He Xiaofang, Zhou Shaoqin
Zhejiang Fenghuiheng Information Technology Co., Ltd., Hangzhou, Zhejiang 311199

Abstract: The emergence and popularization of the Internet have led us into the era of big data. The innovation of computer information technology and its application in the field of cybersecurity, on one hand, improve processing efficiency and protection capabilities; on the other hand, it invisibly increases the burden of cybersecurity, with higher risks of data leakage and greater difficulties in personnel system management. To a certain extent, the Internet, big data and other technologies are double-edged swords. To give full play to their positive defensive capabilities in the field of cybersecurity, it is necessary to strengthen their positive effects and reduce negative impacts. Therefore, this paper discusses the connotations of big data and computer information technology, and puts forward more development paths for the current application of computer information technology in the field of cybersecurity, hoping to provide more references for relevant practitioners.
Keywords: big data; computer information technology; cybersecurity; application

引言

时下，大数据技术在各领域的应用都十分火热，档案信息管理、财务数据管理等过程中都以先进的设备系统支持，在方方面面提升工作效率。网络安全领域也是如此，通过大数据的应用能够合理规避风险，如果能够做到安全防御、人力与物力的多重管理，先进性、现代性是俱佳的。网络信息安全防护所涉及的领域各式各样，恰所需的约束与制度更是应当综合统筹、尽善尽美。相关技术人员也只有掌握了网络安全需求动态，才能够从多个方面进行安全防护，真正将大数据技术的积极作用展示出来。因此，关于大数据背景下计算机信息技术在网络安全中的应用路径分析具有深远意义。

一、大数据与计算机信息技术内涵

大数据技术对海量、多元、高速产生的信息资源进行深度挖掘与价值转化，可见并非简单指代数据规模的庞大，更强调数据类型的多样性、处理速度的实时性以及潜在价值的低密度性。从其应用本质来看，大数据通过对数据的采集、清洗、存储、分析与可视化，将原本分散、无序的信息转化为可指导决策的知识，广泛服务于商业预测、公共管理、科研创新等领域，成为驱动数字经济发展的核心生产要素之一[1-3]。

计算机信息技术是支撑信息采集、处理、传输、存储与应用的技术体系总和，是连接物理世界与数字世界的关键桥梁。在硬件层面，其中包括了 CPU、内存、硬盘等核心部件，还有通信设备、终端设备几种，构成了信息处理与传输的物理基础。从软件层面来看，计算机内含操作系统、数据库管理系统、应用软件及

算法模型等，负责实现对硬件资源进行调度和管理[4]。当前，计算机信息技术不断融合人工智能、云计算、物联网等新兴技术，从单一的计算工具逐渐发展为赋能各行各业数字化转型的综合性技术平台，深刻改变了人类生产生活的组织方式。

二、威胁计算机网络安全的几大方向

（一）系统安全漏洞

计算机在系统编程阶段，有时程序员的失误会导致计算机系统在运行期间出现漏洞，这些漏洞被隐藏在计算机系统之中，当用户需要使用到相关功能时，会出现系统的崩溃现象，进而会导致资料的破损。需要注意的是，漏洞是普遍存在的，造成用户损失的并不是漏洞本身，而是不法分子根据漏洞盗取客户的信息，进而直接攻击计算机，导致计算机无法实现有效运转，这样也会给用户造成了不可避免的损失。

（二）计算机病毒

计算机病毒不似生物病毒，一般代指计算机程序。如果不当操作或恶意种植，都会导致触发病毒程序，损害计算机性能，进而对网络安全造成威胁。计算机病毒能够通过文件传输、运行程序等传播，硬盘、软盘和网络都可能导致病毒[5-8]。当然，不同的病毒作用于不同位置，所造成的危害也不同。极端情况下可能出现系统崩盘，是必须引起重视和加强防御的，是当前计算机信息技术应用网络安全领域要解决的大问题。

（三）黑客攻击

黑客攻击作为计算机网络安全面临的最大威胁，黑客指的是熟悉计算机操作，并且精通计算机网络技术的人，他们为了达到自己的目的，大多数处于不良用途，会针对计算机漏洞进行攻击，进而导致网络系统的停止运行。这类共计主要包括两类：一是影响网络运行，破坏信息有效性与完整性；二是在不影响网络运行的情况下，窃取重要的机密信息。这种恶意攻击会给计算机网络系统带来重创，会导致用户丢失数据，严重的情况下会导致系统的崩溃，进而给企业带来更加严重的损失。

（四）网络安全监管不足

网络是一种开放性平台，因此面临各种各样的安全隐患。目前许多个人、企业不注重网络安全维护，甚至网络安全的认知观念落后，没有充分认识到网络安全与自己的生活与学习、工作息息相关。当遇到网络制度管理漏洞，极易被网络病毒和垃圾侵袭，而造成不同程度的损失。值得一提的是，当前我国网络法制并不健全，也增加了上述威胁和风险的可能性，导致网络病毒、系统漏洞等弥散。

三、大数据背景下计算机信息技术在网络安全中的应用

（一）网络风险动态预警

大数据技术支撑下，计算机信息技术可通过构建多维度数据采集与分析体系，实现网络风险的动态预警。首先依托分布式数据采集技术，实时汇聚网络流量数据、设备日志数据、用户行为数据及威胁情报数据，涵盖 TCP/IP 数据包特征、端口访问频率、异常登录位置、恶意代码特征码等关键信息，形成 PB 级甚至 EB 级的网络安全数据集。随后，借助机器学习算法对数据集进行深度挖掘，通过建立正常行为基线模型，识别偏离基线的异常行为模式。例如，当某终端设备短时间内发起大量非授权端口扫描请求，或某账号在不同地域同时进行高权限操作时，系统可快速捕捉此类异常特征[9-10]。同时，结合实时流计算框架，实现数据处理与风险判定的毫秒级响应，将潜在威胁转化为可视化预警信息，推送至安全管理平台。这种动态预警模式打破了传统静态防御的滞后性，使网络安全防护从“事后补救”转向“事前预判”，如金融机构可通过该路径提前识别针对核心交易系统的异常流量，避免资金安全风险，企业则能及时阻断针对内部 OA 系统的钓鱼攻击尝试，保障数据资产安全。

（二）网络攻击精准追踪

当网络安全事件发生后，计算机信息技术可借助大数据溯源技术，构建完整的攻击链追踪路径，为事件处置与责任认定提供依据。核心在于利用大数据的全量数据存储与关联分析能力，突破传统日志分析的碎片化局限。首先，通过分布式存储架构留存网络全流量数据包与设备操作日志，确保攻击过程中的每一个数据节点都可追溯。其次，运用图计算技术构建攻击行为关联图谱，将分散的日志数据转化为具有逻辑关联的攻击链路。例如，某恶意 IP 先通过漏洞扫描工具探测目标服务器端口，再利用 SQL 注入漏洞获取数据库权限，最后通过远程控制工具上传恶意程序，这一系列行为可通过关联图谱清晰呈现。此外，结合大数据的时空分析能力，可追踪攻击源的地理位置、网络运营商及历史攻击记录，为溯源工作提供多维度线索[11-13]。在实际应用中，该路径已成为打击网络犯罪的关键技术支撑，如在勒索病毒攻击事件中，安全团队可通过溯源技术定位病毒传播源头，协助执法部门抓获犯罪嫌疑人，在数据泄露事件中，可通过追踪数据传输路径，及时阻断数据外泄渠道，降低损失范围。

（三）网络安全防护体系

传统网络防护体系多采用固定规则策略，难以应对大数据时代复杂多变的网络威胁，而基于大数据驱动的自适应防护体系，可通过实时分析网络态势，动态调整防护策略，实现“主动防御”[14]。首先，通过部署广泛的感知节点，采集全网的流量数据、威胁数据、设备状态数据等，形成全面的网络安全数据资源池；其次，利用大数据分析平台对数据资源池进行深度处理，结合威胁情报库构建网络安全态势评估模型，实时评估当前网络面临的威胁等级、脆弱点分布及潜在风险；随后，基于态势评估结果，通过自动化决策引擎动态调整防护策略。例如，当发现某类新型恶意代码攻击时，系统可自动更新入侵检测系统与入侵防御系统的规则库，阻断同类攻击，当某区域网络流量异常激增时，可自动启动流量清洗机制，过滤恶意流量。最后，通过联动防火墙、终端防护软件、云安全服务等防护设备，将调整后的策略落地执行，形成全方位的防护屏障[15]。它的优势在于具备高度的灵活性与适应性，能够随着网络环境与威胁形势的变化持续优化防护能

力，如在云计算场景中，自适应防护体系可根据虚拟机的动态迁移情况，实时调整安全策略，确保每一台虚拟机都处于有效防护范围内，在工业控制系统中，可通过分析生产网络的正常通信规律，精准识别针对 PLC 设备的异常指令，避免工业生产事故，为关键信息基础设施安全提供有力保障。

四、结束语

当今时代不断发展进步，数据信息化成为社会发展的潮流趋势，计算机信息技术在网络安全中的应用也迎难而上。无论对个人还是企业，都应当加强网络安全观念，纷纷投入到网络安全维护当中。依托大数据技术，操作计算机信息技术进行网络安全预警，真实遭遇攻击也可进行溯源技术的精准追踪，一步步构建大数据驱动的自适应网络防护体系，将网络安全风险降到最低。这样的技术还在完善和革新中，也有赖计算机信息技术的支持共同维护网络环境。

参考文献

[1] 金涛，庄会富 . 计算机信息管理技术在科研院所网络安全中的运用研究 [J]. 网络安全技术与应用 ,2024,(01):161-163.

[2] 辛以威 . 新一代防火墙技术在计算机网络安全中的应用分析与验证 [J]. 网络安全和信息化 ,2024,(01):151-153.

[3] 鲁秀明 . 大数据时代下医院计算机网络信息安全技术应用实践探析 [J]. 电子元器件与信息技术 ,2023,7(12):136-139.

[4] 王思成，高飞雪，冷炜镧 . 在用户隐私数据安全保护中 NewSQL 数据库技术的应用策略 [J]. 信息系统工程 ,2023,(12):79-82.

[5] 刘娜，崔志武 . 计算机网络安全防护技术在冶金工业控制系统中的应用——评《有色轻金属冶炼过程优化与控制系统》[J]. 中国有色冶金 ,2023,52(05):161.

[6] 苏虞磊，薛方，曲蕴慧 . 计算机网络安全技术在网络安全维护中实际应用探讨 [J]. 公关世界 ,2023,(19):93-95.

[7] 马鑫越 . 大数据背景下医院计算机网络信息安全技术的应用实践研究 [J]. 科技资讯 ,2023,21(20):30-33.

[8] 徐楚原 . 大数据及人工智能技术的计算机网络安全防御系统设计分析 [J]. 数字技术与应用 ,2023,41(07):216-218.

[9] 邹莉萍，陈富汉 . 基于大数据分析技术的互联网安全风险分析以及预警研究 [J]. 九江学院学报 (自然科学版),2023,38(02):77-81+123.

[10] 刘晓荣，顾润龙 . 计算机安全技术智能化发展趋势思考——评《计算机网络安全原理》[J]. 中国安全科学学报 ,2023,33(06):234.

[11] 王磊 . 计算机网络技术视域下的网络信息安全防护体系建设研究 [J]. 中国宽带 ,2023,19(04):34-36.

[12] 孙善志 . 基于网络安全视角的医院信息管理计算机数据库技术应用分析 [J]. 数字通信世界 ,2023,(04):113-115.

[13] 汤荻 . 基于应用视角的计算机网络安全技术创新与应用 [J]. 网络安全技术与应用 ,2023,(03):15-17.

[14] 王和龙，宋静鹏，李聪 . 人工智能技术在工业互联网信息服务安全评估中的应用 [J]. 电声技术 ,2022,46(11):70-73.

[15] 万晓燕，安述照 . 基于大数据技术的信息安全专业校企合作人才推荐方法 [J]. 信息与电脑 (理论版),2022,34(20):158-160.

