大数据背景下网络空间安全防御的研究应用

薛树辉
中国人民解放军32016部队　甘肃　兰州　730020

摘　要：随着大数据时代的到来，网络空间安全面临前所未有的挑战。本文从大数据背景下网络空间安全新要求、网络空间面临的安全挑战及风险分析以及提升网络空间安全的主要措施及优化途径三个方面进行了深入探讨。在这一背景下，网络空间安全已成为我国发展的当务之急。

关键词：大数据背景；网络空间；安全防御

引言：我国已经进入新经济发展时期，这一阶段充满了多元化发展趋势和产业信息技术创新的机遇与挑战。随着大数据的应用和范围不断扩大，使得网络空间安全和数据稳定性成为了当务之急。本文旨在探讨大数据背景下网络空间安全的新要求和当前面临的安全挑战，以及提升网络空间安全的主要措施及优化途径，以期为制定和完善相应的安全优化措施提供参考和指导。

1 大数据背景下网络空间安全新要求

随着网络威胁和风险隐患的不断增加，数据安全需求日益凸显，主要包括数据的保密性、完整性、可用性和可控性。因此，全面提升网络空间安全等级变得至关重要。我们需要采取措施来保护数据的机密性，确保数据在传输和存储过程中不被未经授权的人访问。此外，数据的完整性也同样重要，以防止数据在传输或存储中被篡改或损坏。在新时代的网络安全防范中，要更加侧重技术和管理的结合应用。网络空间安全需要向技术管控层面转变，以便后续的工作实施和网络空间安全的全程优化。技术的不断进步和创新将为网络空间安全提供更多的解决方案，同时有效的管理也是确保网络安全的关键因素之一。通过技术和管理的紧密结合，我们将能够更好地应对网络威胁和风险，确保网络空间的安全性和稳定性。

2 网络空间面临的安全挑战及风险分析

2.1 网络程序负面影响

自网络诞生以来，其主要功能是运行各种网络程序。在大数据背景下，网络程序的利用和作用变得更加频繁和关键。然而，随着大量网络程序的运行和使用，恶意编程的机会也随之增多，对网络空间中的数据安全造成严重影响。在这些安全威胁中，恶意程序是造成网络程序瘫痪的主要原因。这些恶意程序或病毒会对数据信息进行篡改或破坏，并通过病毒传播，感染网络空间中的大量数据。

这些危害是非常严重的，而病毒程序的编程设计是这些问题的根本原因。不法分子通过恶意编程不仅可以窃取客户信息和数据，还可以通过网络传播病毒或程序进行远程控制操作，极大地增加了安全威胁。

2.2 网络安检漏洞影响

在网络安全保障领域，安全监测的重要性不容忽视。鉴于网络空间数据的重要性，现有网络安全技术的预防和监测系统亟需进一步优化。目前，虽然存在一些高科技、高水平的网络空间安全防御系统，但它们并不普遍，这给保护网络空间数据的安全带来了挑战。在大数据的背景下，这种局面对网络空间安全的巩固和促进产生了不利影响，增加了网络风险和潜在隐患。其中，网络安全监测的漏洞尤为明显，这使得网络后门、网络篡改以及网页仿冒等隐患成为当前网络安全中的严重问题。网络篡改隐患涉及通过非法技术手段对网页内容进行任意改动和破坏。网络后门隐患则指的是非法连接网络系统，植入恶意代码以盗取或破坏客户信息。

2.3 网络产品及平台风险影响

我国正处于信息化的高速发展时代，各类网络平台与信息业务模式层出不穷。在大数据背景下，系统与平台的应用率显著提高，大量应用程序（App）与网络应用应运而生。这些网络应用极大程度地影响了人们的日常生活与工作方式。然而，此发展趋势也给安全带来了挑战。部分程序开发商与技术人员在设计和开发过程中，缺乏必要的安全意识，过分追求经济效益和个人利益，忽略了安全问题。若这种情况长期存在，容易导致用户资料丢失或被篡改，给个人和社会带来严重的后果。

2.4 网络信息系统安全威胁

在信息时代，网络威胁如网络攻击、恶意软件和数据泄露持续演变，对信息系统构成了严重威胁。网络攻击包括了故意破坏、干扰或入侵信息系统的行为，例如拒绝服务攻击（DDoS攻击）和企业网络入侵，它们瞄

准着获取未授权的访问或窃取敏感数据。恶意软件则专门设计用于危害信息系统，包括病毒、蠕虫和特洛伊木马，它们的目标是破坏系统的完整性、可用性和机密性。数据泄露问题也日益严重，涉及敏感、保护或机密数据的非法或未授权传输、复制、窃取或其他形式的泄露。这可能导致个人隐私侵犯、商业机密泄露以及法规合规性问题。因此，维护信息系统安全至关重要，需要制定有效的安全策略和采取适当的安全措施来应对这些威胁，不仅关乎个人和企业的利益，也涉及社会整体的信息安全。

2.5 网络维护威胁

在当今数字化社会中，我们不可避免地面临多种网络安全威胁，这些威胁不断演化，对我们的网络空间安全和稳定构成了严重挑战。首先，安全漏洞存在于网络产品设计或实现中，这些漏洞可能被恶意个体利用以获取未授权的访问或进行其他有害活动，因此，定期的漏洞扫描和修复是至关重要的。黑客和病毒攻击是有意图的破坏活动，可能导致服务中断、数据损坏或隐私泄露。黑客可以利用各种手段侵入系统，而恶意软件如病毒和蠕虫可以自主传播，对系统造成严重损害，因此，实施强大的防火墙、反病毒软件和定期的安全培训可以有助于防范这些威胁。最后，安全管理的滞后问题是传统的管理模式可能不适应现代网络威胁的快速发展，导致防御措施落后于新型攻击手段的演进，为了维护网络安全，需要建立灵活的、专业化的安全管理体系，能够适应不断变化的威胁情景。因此，全面的网络安全策略应包括定期的漏洞管理、强大的防御措施、专业化的安全管理，以确保我们的数字世界不受威胁的侵害。

3 大数据背景下提升网络空间安全主要措施及优化途径

3.1 加强法治巩固提升安全战略意识

网络空间安全的优化与巩固是一个复杂且系统化的过程，特别是在大数据时代背景下，全面提升网络空间的安全效能和法治规范变得尤为关键。网络空间安全是信息时代的核心课题之一，对于国家安全、经济发展以及社会稳定具有重大影响。面对海量数据和复杂网络结构的双重挑战，我们需要以系统化的视角来审视网络空间安全问题，加强法治规范和战略意识的双重提升，以实现网络空间安全的全面优化与巩固。

在国家层面上，必须结合时代发展，制定并颁布网络空间安全相关的法律法规。这些法规应将网络空间视为核心对象，通过法律条款进行有效的监督、管理和推动实施。这不仅包括数据保护、隐私权、网络犯罪等领域的法律，还应包括促进网络技术创新和网络经济健康发展的法律。这样的做法可以形成一个全面的网络空间安全法律体系，为复杂多变的网络环境营造一个更安全、更清洁的空间。其次，各个部门和机构需要加强对网络空间安全的全程监测。根据不同行业的网络架构和服务对象，实施针对性的法规，并进行实时的问题跟踪和监督。这种方法不仅可以帮助及时发现和解决网络安全问题，还可以促进相关行业的网络安全意识和能力的提升。另外，从大数据应用的角度出发，提升网络空间安全的战略意识至关重要。这涉及到对网络空间安全的整体布局与规划，包括对大数据技术的安全应用、数据治理、网络基础设施的安全加固等方面。

3.2 加强网络空间监管与安全技术创新

在大数据时代，网络信息安全体系的建设远不仅仅依赖于计算机网络技术的进步。国家在政治体制和法律制度方面的保障同样至关重要。当前，大数据时代下的网络信息安全监管正处于不断发展和深入探索的阶段。国家必须敏锐地把握市场的发展趋势，从宏观战略的角度来认识网络信息安全对我国经济社会发展的重要性。因此，网络信息安全的提升必须从多个层面入手。在网络技术方面，国家需要进行宏观调控，不断推动网络技术的发展，以满足大数据时代的安全需求。其次，在政治策略上，国家必须充分认识到大数据信息安全体系建设的重要性，以及大数据安全对我国的深远影响。这意味着需要制定相应的政策和法律法规，以确保网络信息安全得到充分保障。

除此之外，在大数据时代背景下，网络空间安全优化的关键是明确数据的应用和效能，并通过开展大数据应用的调查和统计来加强安全监管。这种方法不仅有助于识别和解决现有的安全问题，还能预防未来的风险。面对各种木马程序和病毒的影响，必须在各个网络关口实施全面检测。这包括重新设置访问权限，提升访问权限等级，确保只有通过特定密钥认证的访问者才能获取相应的权限。同时，根据不同的安全等级，对用户的权限进行合理设置，从而减少未授权访问和潜在的安全威胁。

网络空间安全监测中应该充分利用人工智能的信息化优势。人工智能技术在网络安全领域的应用可以实现快速发现和定期巡检网络漏洞与风险隐患，并能自动执行应急处理。这种技术不仅提高了监测和响应的效率，还可以减轻人工监测的负担，使网络安全管理更加智能化和高效。

3.3 规范网络产品安全设计及稳定运行

在设计过程中，应该重点考虑应用程序（App）和系

统平台的安全标准及等级。不仅要确保新开发的产品符合安全标准，还需要对现有的、不符合安全标准的App和系统平台进行综合治理。这包括更新安全漏洞、强化数据保护措施和增强用户隐私保护。同时，根据国家相关法规，应清理和净化网络市场，强化对网络市场的综合监管与安全监测。这包括对网络产品进行定期审查，确保它们符合国家法律和行业标准，并及时处理不符合标准的产品。此外，市场监管部门应对存在安全漏洞的网络产品的违规者进行严格惩罚，以此作为维护网络环境安全稳定的重要手段。此外，提升公众对网络产品安全的意识也同样重要。通过教育和宣传，提高用户对网络安全的认识，使他们能够识别和防范潜在的网络威胁。

3.4 根据环境要求开展网络空间安全优化

在网络空间安全管理中，考虑市场环境的变化对强化网络安全管理的实效性与保障性至关重要。需要明确安全风险及隐患防范的重点，并采取相应措施来弱化风险入侵的影响。这包括识别和评估可能的安全威胁，如网络攻击、恶意软件和数据泄露等，并制定有效的应对策略。例如，加强防火墙和入侵检测系统的使用，以及使用加密技术来保护数据传输和存储。

在网络空间安全管理中，定时分析和定期检测是关键的策略。所以需要对网络产品的设计和开放的安全性能进行全面检查，以便及时发现并解决潜在的安全漏洞。这种持续的监控和评估可以帮助及时识别和防止小问题演变成大问题，从而最大程度地提高网络系统在大数据背景下的安全监测功能。此外，还应加强网络安全人才的培养和团队建设。通过提供专业的培训和教育，可以增强团队成员对最新网络安全威胁的认识和应对能力。同时，鼓励安全团队与行业内的其他专家和机构进行合作交流，共享安全信息和最佳实践。另外，还要注重网络安全法规的制定和执行。政府部门和行业监管机构应该制定适应时代发展的网络安全法规，对网络空间进行有效管理，确保网络产品和服务的合规性。总之，在网络空间安全管理中，结合市场环境的变化，强化安全管理实效性与保障性，以及计算机安全管控的应用结合，对保护客户信息和数据的安全至关重要。通过定时分析、定期检测、人才培养和法规制定等多方面措施，可以有效提升网络系统在大数据背景下的安全监测功能。

3.5 针对黑客病毒实时专业安全管控

在网络空间安全管理中，首先必须预测黑客和病毒攻击的可能性，并明确所处网络环境的安全等级，这是制定有效安全管控计划的基础。一旦明确了自身的安全等级，就需要对安全架构进行全面建设。例如，根据风险等级制定一级风险应对预案和二级风险应对机制，细化具体的应对策略和方法，以便于后期多项工作的顺利开展和实施。其次，根据自身情况实时更新病毒库和防毒软件。全面分析市场上各种新型病毒的特点和影响，以提升自身的防毒能力。定期更新和维护防毒软件可以确保网络环境免受最新病毒和恶意软件的侵害。再次，基于黑客可能对网页、应用程序（App）及网络空间造成的攻击，加强各部门及组织网络的巡查工作是非常必要的。包括实施定期的网络安全检查，以最大程度降低黑客入侵和病毒程序植入的可能性。最后，实施专业化体系建设，将专业技术作为安全管理的核心。总体而言，通过预测黑客和病毒攻击、更新病毒库和防毒软件、加强网络巡查、强化预警系统建设以及实施专业化管理，可以全面增强网络空间的安全性，有效防御和应对各种网络威胁，确保在大数据背景下网络空间的安全和稳定。

结束语

在大数据时代，网络空间安全已成为国家发展的关键问题。为了确保网络空间数据的安全稳定运行，我们需要加强法治建设，提升安全战略意识，加强网络空间监管与安全技术创新，规范网络产品安全设计及稳定运行，根据环境要求开展网络空间安全优化，以及针对黑客病毒实时专业安全管控。只有通过综合的措施和精准的策略，我们才能更好地迎接网络空间安全带来的挑战，为我国网络空间的安全稳定发展提供坚实的保障。

参考文献

[1]王华,杨青.大数据背景下的网络空间安全防御机制研究.[J]计算机科学,2019(4),1-6.

[2]张洪波,齐鹏飞.基于大数据分析的网络空间安全防御策略研究.[J]计算机工程与设计,2019(8),2445-2451.

[3]王亚男,徐志成.大数据环境下的网络空间安全防御技术研究.电脑知识与技术,2019(20),1-4.

[4]杨洪涛,邵华.基于大数据的网络空间安全防御模型研究.[J]计算机科学与探索,2020(10),1523-1530.

[5]赵晓辉,郭辉.大数据时代的网络空间安全防御技术及其应用研究.[J]信息网络安全,2021(1),22-26.