人防信息化进程中网络安全保障体系建设

韩亚琼
张家口市人防动员办公室　河北　张家口　075051

摘　要：随着信息技术的迅猛发展，人防信息化已成为提升国家军事能力、增强国家安全的重要途径。然而，人防信息化进程的加速也带来了前所未有的网络安全挑战。本文旨在探讨人防信息化进程中网络安全保障体系建设的重要性、现状、面临的挑战及应对策略，为构建安全、可靠的人防信息化环境提供参考。

关键词：人防信息化；网络安全保障体系；建设

引言

人防信息化是指利用现代信息技术手段，对人防建设和管理进行全方位、深层次的改造和提升。它涵盖了指挥控制、情报侦察、通信联络、武器装备、后勤保障等多个领域，对于提高军队战斗力、实现精确作战具有重要意义。然而，人防信息化进程的加速也带来了网络安全问题的凸显。网络攻击、信息泄露、系统瘫痪等安全事件频发，对国家安全构成了严重威胁。因此，加强人防信息化进程中的网络安全保障体系建设显得尤为迫切。

1 人防信息化进程中网络安全保障体系建设的重要性

人防信息化作为现代国家安全的重要支柱，其深入发展不仅改变了传统战争的面貌，也对国家安全的维护提出了更高要求。在这一进程中，网络安全保障体系建设显得尤为重要，其重要性主要体现在以下几个方面：

1.1 保障国家安全

人防信息化是国家安全战略的重要组成部分，它涉及到军事机密、战略决策、指挥控制等核心利益。网络安全保障体系建设直接关系到这些核心信息的安全传输与存储。一旦网络系统遭受攻击或破坏，可能导致军事机密泄露、战略决策失误，甚至影响国家主权和领土完整。因此，构建坚固的网络安全保障体系，是维护国家军事安全、政治安全和社会稳定的基石。

1.2 提升军事能力

网络安全是人防信息化顺利推进的前提和基础。在信息化战争中，网络系统成为连接各作战单元、实现信息共享和协同作战的关键。只有确保网络系统的安全稳定运行，才能有效防止敌方的网络攻击和干扰，保障信息化装备和系统的作战效能得到充分发挥。因此，加强网络安全保障体系建设，是提升军队信息化作战能力、增强人防实力的必要途径。

1.3 促进人防现代化

网络安全保障体系建设是推动人防现代化的重要手段之一。随着信息技术的飞速发展，人防现代化越来越依赖于网络系统的支撑。构建完善的网络安全保障体系，不仅能够提升人防建设的整体科技水平，还能够增强国家在国际竞争中的信息优势和战略主动权。

2 人防信息化进程中网络安全保障体系的现状

人防信息化作为提升国家防御能力和战略竞争力的重要途径，其网络安全保障体系的建设至关重要。当前，我国人防信息化进程中的网络安全保障体系呈现出以下现状：

2.1 政策法规不断完善

近年来，我国高度重视网络安全法律法规的建设，相继出台了一系列关于网络安全的法律法规和政策文件。这些法律法规明确了网络安全的定义、范围、责任主体以及处罚措施，为人防信息化进程中的网络安全保障提供了坚实的法律支撑。同时，政府还不断加强对网络安全监管的力度，确保各项法律法规得到有效执行，为网络安全保障体系的完善提供了有力保障。

2.2 技术手段不断进步

随着信息技术的飞速发展，网络安全技术手段也在不断更新换代。防火墙、入侵检测、加密技术等传统网络安全技术得到了广泛应用，并在实践中不断完善和优化。同时，新兴的网络安全技术如人工智能、大数据分析等也在网络安全领域发挥着越来越重要的作用。这些技术手段的进步为网络安全保障提供了更加全面、有效的支持，提高了网络系统的安全性和稳定性。

2.3 人才队伍建设加强

国家高度重视网络安全人才的培养和引进，通过加强教育培训、实践锻炼等方式，不断提升网络安全人才的综合素质和实战能力。同时，还积极建立网络安全人才库，为人防信息化进程中的网络安全保障提供强有力的人才支撑。

3 面临的挑战

3.1 网络攻击手段多样化

随着黑客技术的不断进步和演变，网络攻击手段日益呈现出多样化、复杂化的趋势。DDoS（分布式拒绝服务）攻击、APT（高级持续性威胁）攻击等新型攻击方式层出不穷，它们不仅攻击力度强、隐蔽性高，而且难以防范和追踪[1]。这些攻击手段对人防信息化系统的网络安全构成了严重威胁，一旦遭受攻击，可能导致系统瘫痪、数据丢失等严重后果。

3.2 信息泄露风险增加

人防信息化进程中，大量敏感信息需要在网络上进行传输和存储。这些信息涉及国家军事机密、战略决策等核心内容，一旦遭受攻击或泄露，将给国家安全带来巨大损失。随着网络技术的不断发展，信息泄露的风险也在不断增加。攻击者可能通过各种手段窃取、篡改或破坏这些信息，对国家安全构成严重威胁。

3.3 系统脆弱性凸显

人防信息化系统往往涉及众多复杂组件和子系统，这些组件和子系统之间存在诸多接口和交互，使得整个系统变得异常复杂。这种复杂性不仅增加了系统的维护难度，也带来了诸多安全漏洞和脆弱性。攻击者可能利用这些漏洞和脆弱性，对系统进行攻击和破坏，导致系统瘫痪或数据泄露等严重后果。因此，加强系统脆弱性的评估和修复，是人防信息化进程中网络安全保障体系建设的重要任务。

4 人防信息化进程中网络安全保障体系建设策略

4.1 强化顶层设计，完善政策法规体系

人防信息化进程中的网络安全保障体系需要有一个清晰、明确的顶层设计，以确保整个体系的建设方向和目标一致。首先，要加强网络安全保障体系的顶层设计，明确其战略地位和发展方向。这要求从国家安全的战略高度出发，将网络安全保障纳入人防信息化建设的总体规划，确保其与人防信息化的发展同步推进。在顶层设计的基础上，还需要制定和完善相关政策法规，为网络安全保障体系的建设提供法律保障和政策支持。这些政策法规应涵盖网络安全管理的各个方面，包括网络安全标准制定、网络安全认证体系建立、网络安全监管机制完善等。通过立法明确网络安全的法律地位，规范网络行为，打击网络犯罪，保护网络权益，为网络安全保障体系的建设提供有力的法律支撑。同时，要加强与国际社会的合作与交流，共同应对网络安全挑战[2]。网络安全是全球性问题，需要各国共同合作来解决。应积极参与国际网络安全合作机制，加强与国际先进网络安全技术的交流与合作，学习借鉴国际先进经验和技术，提升我国人防信息化进程中的网络安全保障水平。此外，还要加强网络安全国际法规的制定和完善，推动形成国际网络安全新秩序。

4.2 构建主动防御体系，提升安全防护能力

在传统“自卫模式”的基础上，应探索建立以“护卫模式”为核心的新型主动安全防御体系。这种防御体系应具备设陷探查、关联研判和应对拦截等联动机制，实现对网络安全的主动防御。设陷探查是主动防御体系的第一道防线。可以在网络系统中设置陷阱或诱饵，吸引并发现潜在的网络攻击行为。这些陷阱或诱饵可以是虚假的网络服务、漏洞百出的系统组件等，通过模拟真实的网络环境，诱使攻击者进行攻击，从而暴露其攻击手段和意图。关联研判则是对探查到的信息进行深入分析和判断。需要建立强大的数据分析能力和智能研判系统，对收集到的网络攻击信息进行关联分析，识别出攻击者的身份、目的和手段。这要求具备强大的数据挖掘和分析能力，以及先进的威胁情报共享机制，确保能够及时发现并应对网络攻击。应对拦截则是根据研判结果，采取相应的防御措施，阻止攻击行为的进一步发展。这需要建立完善的防御机制和响应流程，确保在发现网络攻击后能够迅速、准确地采取应对措施，防止攻击造成更大的损失[3]。除了建立主动防御机制外，还应加强关键信息基础设施的安全防护。关键信息基础设施是人防信息化的核心组成部分，其安全性直接关系到国家安全和社会稳定。因此，要加大对关键信息基础设施的安全投入，采用先进的技术手段和管理措施，提升其整体安全防护能力。这包括加强网络边界的安全防护、完善访问控制机制、加强数据加密和隐私保护等。同时，还要加强网络安全监测和预警能力建设。通过实时监测网络系统的运行状态和异常行为，及时发现并预警潜在的网络安全威胁。这要求建立完善的网络安全监测体系，具备强大的实时监测和预警能力，确保能够及时发现并应对网络安全事件。

4.3 加强技术研发，提升自主创新能力

技术创新是网络安全保障体系建设的重要支撑。为了应对日益复杂的网络安全威胁，必须加大网络安全技术研发力度，提升自主创新能力。首先，要针对人防信息化进程中的网络安全需求，开展关键技术攻关和产品研发。这些关键技术包括网络安全防护技术、网络攻击追踪技术、网络数据加密技术等。通过攻克这些关键技术，可以为人防信息化提供更加强有力的技术支撑，提升系统的安全防护能力和应对网络攻击的能力。其次，

要推动网络安全技术的产业化和应用推广。将研发出的网络安全技术转化为实际产品，并广泛应用于人防信息化系统中，提高系统的安全防护水平。同时，还要加强对网络安全技术的宣传和培训，提高广大用户的安全意识和防范能力，形成全民参与网络安全的良好氛围。此外，还要加强与国际先进网络安全技术的交流与合作。通过引进和消化吸收国际先进技术，提升我国网络安全技术的整体水平。同时，要积极参与国际网络安全技术标准的制定和推广，提高我国在国际网络安全领域的话语权和影响力，推动形成有利于我国网络安全发展的国际环境。

4.4 加强人才培养，提升队伍素质

人才是网络安全保障体系建设的关键要素。为了提升人防信息化进程中的网络安全保障水平，必须加强网络安全人才培养和队伍建设。首先，要通过教育培训、实践锻炼等方式，培养一批具有高水平网络安全技能和实战经验的专业人才。这些人才应具备扎实的网络安全理论基础、熟练的网络安全操作技能和丰富的实战经验，能够应对各种复杂的网络安全威胁。为此，可以建立专门的网络安全培训机构和实训基地，为人才培养提供有力的支撑。其次，要加强对现有网络安全人员的培训和教育。通过定期组织培训课程、研讨会等活动，更新他们的知识和技能，提高他们的专业素养和实战能力。同时，还要鼓励网络安全人员积极参与国际交流和合作，拓宽他们的视野和思路，提升他们的国际竞争力。此外，还要建立健全网络安全人才激励机制。通过提供优厚的薪酬待遇、良好的工作环境和发展空间等措施，吸引和留住优秀的网络安全人才。同时，还要加强对网络安全人才的宣传和表彰工作，提高他们的社会地位和职业荣誉感，激发他们的工作热情和创新精神。

4.5 加强应急响应机制建设，提高应对能力

网络安全事件具有突发性和不确定性，因此必须建立完善的网络安全应急响应机制，提高应对网络安全事件的能力。首先，要制定详细的应急预案和处置流程。这些预案和流程应涵盖各种可能的网络安全事件类型、等级和处置方法，为应急响应工作提供明确的指导和依据。同时，还要定期对预案和流程进行演练和评估，确保其有效性和可行性，提高应急响应的效率和准确性。其次，要加强应急响应队伍的建设和管理。建立一支专业、高效的应急响应队伍，负责网络安全事件的监测、预警、处置和恢复等工作[4]。通过加强队伍的培训和教育，提高他们的专业素养和实战能力，确保他们能够迅速、准确地应对网络安全事件。同时，还要建立健全队伍的管理制度和工作机制，确保队伍的稳定性和可持续性。此外，还要加强与相关部门的协同配合。网络安全事件往往涉及多个部门和领域，需要各部门之间的协同配合才能有效应对。因此，要建立健全部门间的协同机制和信息共享机制，加强沟通与协作，形成合力应对网络安全挑战。同时，还要加强与行业组织、学术机构等社会力量的合作与交流，共同推动网络安全保障体系的建设和发展。

结语

人防信息化进程中的网络安全保障体系建设是一项长期而艰巨的任务。只有不断加强顶层设计、构建主动防御体系、加强技术研发、强化人才队伍建设、完善应急响应机制，才能构建安全、可靠的人防信息化环境，为国家的繁荣发展和长治久安提供有力保障。未来，随着信息技术的不断进步和人防信息化进程的深入发展，网络安全保障体系建设将面临更多新挑战和新机遇。需要持续关注和研究这些问题，不断创新和完善网络安全保障措施和方法，为人防信息化事业的顺利推进提供有力支撑。

参考文献

[1]王慧珠,李亚鹏,侯志斌.网络空间安全与网络人防建设研究[J].科技经济导刊,2023,31(06):78-82.

[2]秦有权.论信息化时代人防工程技术的创新发展[J].防护工程,2020,42(01):1-6.

[3]齐鹏云.人防网络安全与数据治理研究[J].大数据,2024,10(03):149-162.

[4]刘霄,王平.面向人防工程无线网络的信息安全防护问题研究[J].科技创新与应用,2021,11(34):87-90.