Advances in Social Sciences 社会科学前沿, 2022, 11(10), 4176-4181
Published Online October 2022 in Hans. http://www.hanspub.org/journal/ass
https://doi.org/10.12677/ass.2022.1110568

Hans汉斯

信息通信网络安全管理困境与应对策略研究

吴岳贝，王　鑫

成都锦城学院电子信息学院，四川 成都

收稿日期：2022年8月18日；录用日期：2022年10月2日；发布日期：2022年10月9日

摘　要

随着大数据时代的到来，信息网络安全正逐步发展。但是由于我国当前的信息通信技术还不成熟、国家和企业未能建立监管制度，导致信息网络安全管理较为混乱。本文通过分析我国当前的信息网络安全管理发展现状和问题，提出相关解决方案。

关键词

大数据时代，信息通信，信息网络安全

Research on the Difficulties and Response Strategy of Information and Communication Network Security Management

Yuebei Wu, Xin Wang

Department of Electronic Information, Chengdu Jincheng College, Chengdu Sichuan

Received: Aug. 18th, 2022; accepted: Oct. 2nd, 2022; published: Oct. 9th, 2022

Abstract

With the advent of the big data era, information network security is gradually developing. However, because China's current information and communication technology is not mature, the state and enterprises have failed to establish a regulatory system, leading to the result that the information network security management is more chaotic. This paper analyzes the current development situation and problems of information network security management in China, and puts forward relevant solutions.

文章引用: 吴岳贝, 王鑫. 信息通信网络安全管理困境与应对策略研究[J]. 社会科学前沿, 2022, 11(10): 4176-4181.
DOI: 10.12677/ass.2022.1110568

Keywords

Big Data Era, Information and Communication, Information Network Security

1. 引言

随着时代的进步，互联网已经不断被普及到人们的日常生活中，信息通信网络也开始逐步发展。近年来，随着5G、物联网、大数据技术等高科技信息化技术的出现和普及，智慧城市、远程操控、数字人民币等新型产业在全球范围内得到广泛普及和应用。目前，为了更好地实现信息的快速收集和快捷存储，提高工作效率，进一步加强人与人之间的交流，信息通信已经成为了当前新兴产业发展必不可少的组成部分，不管是线上办公、视频通话，还是因疫情出现的云吃饭、网课学习，信息通信网络技术都发挥着连接他人的纽带作用。与此同时，在全球发展数字经济的大背景下，分析当前信息、通信、网络等方面管理出现的问题，提出一一对应的解决策略，加强对于信息通信网络安全管理的研究，使网络环境进一步得到净化，从而在互联网高速发展的时代中前进。

2. 文献综述

随着科技的发展，信息网络安全已经成为一个不可忽视的内容，学术界也对其从不同方面展开研究。张婧(2021)通过对我国当前网络信息安全管理方面所发展的现状情况进行实证案例分析，指出当下我国信息通信网络安全管理在不断地发展中依旧存在着“安全意识普遍不足、管理体系不健全、设备落后”等一系列主要现实问题隐患和新威胁，并对信息安全与大数据融合进行必要性分析，最后针对当下突出问题提出“构建体系、借鉴各类相关先进技术”等措施方法原则和工作建议，进一步推进大数据与信息安全融合[1]。董满、罗志坚(2022)均认为未来大数据时代的各行各业信息技术的健康发展也都必然离不开海量数据信息技术的强力支撑，基于“大数据时代”的背景下，从大数据自身特点入手分析当下网络安全，凸显目前网络安全正处于“内忧外患”的局面，外部环境因主客观条件束缚，内部条件自身发展存在漏洞缺陷，并以此提出一系列有效的解决方案，抓住重点，从网络安全自身出发，全面建立修复系统，从而维护网络安全[2]。董克彬、朱曈、杜广让(2022)则认为大数据技术应该是一种完全依托于计算机与云计算技术结合的超先进信息处理模式，而要全面实行该种模式，就需要对当下网络安全现状进行数字化的改革，通过对信息通信网络进行硬软件的升级维修，达到逐步健全网络安全体系的目的[3]。庄世伟、王斌(2021)通过归纳概括分析计算机网络和信息安全，指出目前中国计算机网络及其信息安全现在存在着“犯罪率、病毒、安全系数、自然因素、黑客”等弊端，在提出一系列的防护措施中，强调“杀毒软件、监测技术”等的应用[4]。许沙、丁丽华、王鑫(2021)突出表示当下经济发展得益于大数据信息网络，依据实际生活指出目前通信网络安全管理方面仍存在的优势及不足，为了在一定程度上避免损失，而进一步提出优化网络安全管理的解决策略，从而达到提高经济效益、增加收入的目的[5]。丁红梅(2016)则强调当前网络环境安全已经深入国家利益层面，认为当下网络高端职业技术人才能力的提升培养计划和安全相关国家法律法规政策的修订完善工作是目前解决当前网络环境安全形势的关键[6]。胡柏耀(2022)从智慧城市建设背景出发，进一步研究信息安全管理体系的建设、信息安全监管平台的建立、完善智慧城

市安全改革法规，加强信息安全管理技术创新研发等信息安全管理的措施与建议[7]。齐峰(2019)将信息安全与档案信息安全进行结合，分析当前大数据时代档案信息泄露安全及管理带来的重大隐患，并能提出一些相应针对性的处理措施[8]。梅彬(2021)从计算机人工智能分析的新角度去分析中国网络信息基础设施安全中存在着的突出问题及人工智能在安全这几方面取得的领先优势，并最终针对以上这些重要问题分别提出了各自相应具体的技术解决对策方式并且具体给出进行了应用案例的分析[9]。

综上所述，前人通过研究得出的答案主要是中国网络信息服务安全现状存在着的几个问题和一些相应解决的技术对策，这些学者基本上都是较为清晰、准确、客观的分析概括，分析出在当代社会我国网络信息服务安全中存在的若干问题，并据此提出一些相应的有效解决方式。本文首先系统的分析出了目前网络信息及通信系统网络和安全的管理所存在的诸多问题及弊端，再依次针对这些弊端提出相应的解决方式，从而提高网络信息安全管理的可行度和效率。

3. 信息通信网络安全现状

3.1. 电信违法案例日渐增多

随着科技的飞速发展，计算机进入了大众的生活。随着计算机的普及和互联网的快速发展，一些不法分子通过利用网络程序实施违法犯罪行为，例如盗取用户个人信息及账号密码等违法行为，近几年尤为猖獗。根据 2019 年由最高人民法院网站发布的一份大数据公告，我们可知：在我国自 2016 年始算截止到 2018 年，网络融资借贷系列犯罪案全国各地共已累计受理结案了约有 4.8 万多件，在中国近年来全部刑事案件总量结构变化中，此类案件的发生量呈现出逐年明显的上升增长之大趋势，2018 年我国的刑事犯罪案件量也是呈较显著程度的趋势上升，同比累计升幅则降为负 50.91%。通过对以上领域网络信息技术应用犯罪的典型案件的调查显示，从事于因特网信息接入与互联网传输、计算机应用服务领域和计算机信息网络应用软件研发领域犯罪行为的典型案件中受害人最多，占案比达到 37.21%。通过这些数据分析可得，近几年由于互联网的全面普及和计算机技术的发展，越来越多人运用这些技术进行违法犯罪，导致网络犯罪率越来越高。并且计算机网络类犯罪成员大多数为由高级计算机专业技术人员以及计算机互联网专业人士而构成，一旦产生了网络犯罪活动以及其他计算机相关犯罪，会直接破坏计算机互联网内部以及计算机信息系统的宝贵资料信息[10]，这是信息通信网络安全发展的一个巨大阻力。

3.2. 设备安全与技术创新问题

信息网络工程最主要的设备组成部分是计算机软硬件等硬件设备。因此，在信息网络通信技术的实际工作运行管理过程实践中，硬件设施的维护是重中之重，只要保障相关硬件设施能够正常有效运行，就能切实保证信息交换通信网络系统的有效正常运行。但在设备维护工作中仍存在诸多问题，一方面是由人为因素造成的设备损坏，例如由于一部分人不懂得爱惜自己的计算机，常常不正确关机，导致计算机等硬件设备不能正常运行，进一步导致信息通信网络难以正常工作；另一方面是由于设备本身存在的问题，长时间使用该通信设备会出现相关硬件老化、运行速度减慢等问题，而这些问题极大地影响了设备的安全。

当前信息通信网络安全的技术还不够成熟，这导致一些黑客利用相关技术篡改信息，造成用户信息泄露的情况，这是信息通信网络安全建设的又一大重要阻力。与此同时，网络病毒在互联网中随处可见，而网民们没有建立起对于个人信息的保护意识，进一步就增加了企业信息网络通信系统网络环境安全防范管理实施的管理难度。在此基础上，技术人员应该进一步提升自己的能力，研制生产出了不同类型的数据加密技术[11]，加强技术创新，更好程度的保证了用户信息数据传输的绝对安全，从而真正保障网络信息及通信数据网络安全。

3.3. 技术人才和监管从业人员匮乏

近几年来，计算机是一个热门专业，信息通信网络也得到了一定发展，但是技术人才的缺口依然很大，特别是顶尖的技术人才，目前更多的技术人才的技能都比较粗浅，这使得信息通信网络安全技术始终停滞不前，未能取得重大突破。当前许多计算机专业的学生学习程度粗浅，不能很好地理论知识运用到实际操作上，常常导致写出的代码存在众多程序错误，进一步导致信息通信网络安全技术人才缺口很大。另一方面，随着近几年互联网的快速发展，推进计算机行业的迅速壮大，但目前信息通信网络仍处于起步阶段，政府与企业未能及时建立健全信息通信网络安全监管机制、招收相应人才，高校大多还未设立相关专业、培养相关从业人员，进一步导致行业比较混乱。

3.4. 安全监管机制未明确

自从互联网进入人们的日常生活后，信息通信网络安全事故频发，同时用户的信息通信网络安全意识薄弱。为了有效地解决这些问题，国家相关部门联合各地的企业和事业单位建立了信息通信网络安全体系，从而加强相关工作人员对信息通信网络安全管理的防护意识。但是，建立的这个系统并不完善，它没有包含所有行业，没有相应的法律对其进行约束，以至于无法处理突发事件。一旦发生意外，这个系统不能全面处理突发意外事件，更无法结合法律法规惩治威慑犯罪分子。由于我国前期偏重经济发展，对于信息通信网络安全并没有投入太多的精力，没有明确的安全监管机制，这便导致我国的信息通信网络安全管理错漏百出。在企业中，通常使用“补西墙又补东墙”的手段，这样进一步导致我国信息通信网络安全管理处于一个较为混乱的阶段。

4. 持续创新发展的应对策略

4.1. 建立健全信息通信网络安全监管机制

在大数据的时代背景下，国家和企业应该注重建立健全信息通信网络安全监管体制。首先，全面调查我国信息通信网络安全发展现状，进一步分析存在的问题，建立一个严格的信息通信网络安全监管机制，确保覆盖各个行业，提高信息通信网络的安全性。其次，需要做到定期检查该系统，及时发现病毒和程序错误并进行维护修复，提高发现程序错误的效率，确保企业及用户的信息安全。最后，定期对员工进行信息通信网络安全管理的培训，进而提高员工的专业水平和信息通信网络安全意识，从而减小安全监管人员的压力、保证企业的健康发展。与此同时，国家也应该出台一系列相关的法律法规，根据分析存在的问题进一步完善相关法律法规，从而对一些不法分子进行约束和严惩，净化网络空间。

4.2. 加强软硬件设备创新研发与引进

在大数据时代中，网络病毒随着互联网的广泛使用悄然而生。一些病毒具有巨大的破坏性，给互联网带来了极大的损失，杀毒软件也因此出现。但是随着科技的进步，一些黑客研发了更为“凶悍”的病毒，致使杀毒软件也不能完全抵挡。因此需要专业人才进一步创新研发新的、更有效抵挡病毒的软件。同时，由于技术的发展，软件与软件之间的依赖性越来越强，导致设备之间的程序错误更加容易被发现，从而让有心之人有机可乘，增加了相关技术人员的防御难度。因此，应该定期维护软件设备，减少设备漏洞，同时加强研发软件设备、引进更好的软件并研究其构成，提升专业技术人员的能力，保证软件设备的良好运行。

除去软件，硬件设备也是信息通信网络安全中至关重要的组成部分。工作人员必须结合研究发现的信息通信网络安全的现状及其存在的问题对硬件设备进行定期的维护，保障硬件设备的良好运行。因此，信息通信网络安全管理人员需要定期参加维护相关硬件设备体系的培训，了解与学习信息及通信及网络

等安全保障体系框架下各种硬件设备系统的安全运行技术特点要求和运行工作基本模式，从而提升一下自己的专业技能，使自己更能够妥善应对信息通信网络安全的突发情况，构建出一个良好稳定的网络和安全环境。同时，对于信息及通信行业网络设备安全检测管理方面还应该更进一步制定出详细规范的设备硬件及检修设备标准，对硬件设施进行正确的检修和维护，从而延长硬件设备的寿命，防止硬件设备出现零件老化、超负荷运行等问题，确保信息通信网络正常运行，减少企业的不必要支出，降低成本。

4.3. 推进网民基础素质建设

近年来，我国一直注重经济建设，对于信息通信网络安全建设并没有投入过多的精力，以致于人们在使用互联网时缺乏保护自我信息的意识。因此需要国家和政府加大对网民基础素质的建设，可以通过引导网民正确使用计算机，及时、自动地删除所有网络访客记录，关闭所有网络端口，达到及时地避免网络端口因网络管理员或自身原因或由于操作及管理措施不当而造成的网络用户个人信息资料泄露，提高客户网络信息资料以及用户通信设备和计算机网络数据资产的可访问安全性。由于当今社会，互联网已经广泛普及到各家各户，人们从小就开始接触网络，所以应该从小孩子抓起，在他们开始接触网络时，通过宣传海报、视频动画等多种形式引导他们建立一个对于自我信息保护的安全，保护个人信息，进一步推进网民基础素质建设。

4.4. 着力完善专业人才培训与引进规划

信息和通信及网络和安全与管理系统就像是一款性能都极佳的高性能赛车，但是也只有一些操控赛车能力极强和驾驶赛车技术又极好的高人才能轻松驾驭它。信息及通信及网络的安全与管理的设备无论技术多先进、技术多高端，假如相关工作人员不会使用，自己又不肯去学习，最终这些设备也发挥不了其自身应有的价值，甚至还会给企业的运营带来风险。因此专业人才的培养就显得尤为重要，本文认为应该从以下几个方面进行培养。

1) 熟练掌握信息通信网络基础知识，同时加强对信息通信网络安全管理知识的学习。首先必须熟练掌握信息通信网络的基础知识，它是熟练使用网络技术的必要条件。除此以外，更重要的是要进行实际操作，掌握信息通信网络安全的技术，将理论知识运营到实际生活中，达到变理论为实际的效果。除了理论知识和技术以外，还需要获得相关的职业资格证书，证明自己的专业水平，以免空口无凭。

2) 具有较强的责任心。专业人才除了要拥有理论知识和相关专业技能以外，责任心也是必不可少的。当一个人缺乏责任心时，他所做的事将会受到阻碍，因为无法坚定地持续下去，遇到困难也会有迟疑之态。由于信息通信网络安全问题随时都会出现，因此需要相关工作人员有较强的应变能力和洞察力，能够在信息通信网络安全问题出现时，冷静地应对并且快速给出解决措施，及时解决问题。而这些特点其实是高度的责任心，在最短时间内避免信息通信网络安全问题所带来的风险，从而确保信息通信网络的正常运行。

5. 结束语

综上所述，随着全球计算机信息化大数据化时代的快速到来，计算机工业信息化产品正逐步地深入并渗透应用到中国经济社会以及各个国民经济相关各个行业和应用中。但是由于目前中国的信息网络的通信环境与在网络信息传输安全规范及技术管理的领域内仍然将会还存在一些其他的诸多问题，为了进一步保证用户的信息安全，信息通信网络安全管理问题成为了全球聚焦的问题。网民应该提高自己对个人信息的保护意识，同时相关技术人员要提升自己的专业技能，增加自己的实操能力和创新能力，进一步提升自己应对突发情况的能力，政府也应该出台相关法律，联合企业及事业单位建全信息通信网络安

全监管机制，共同构造一个良好的网络环境。

参考文献

[1] 张婧. 大数据背景下信息通信网络安全管理策略研究[J]. 长江信息通信, 2021, 34(10): 145-147+150.

[2] 董满, 罗志坚. 大数据时代计算机网络安全管理策略探究[J]. 网络安全技术与应用, 2022(1): 163-164.

[3] 董克彬, 朱瞳, 杜广让. 基于大数据背景的通信网络安全管理策略研究[J]. 网络安全技术与应用, 2022(1): 56-57.

[4] 庄世伟, 王斌. 计算机网络信息安全管理策略探析[J]. 网络安全技术与应用, 2021(4): 157-158.

[5] 许沙, 丁丽华, 王鑫. 大数据背景下信息通信网络安全管理策略研究[J]. 中国设备工程, 2021(19): 45-46.

[6] 丁红梅. 加强网络安全管理, 保障计算机信息安全[C]//“决策论坛——管理科学与经营决策学术研讨会”. “决策论坛——管理科学与经营决策学术研讨会”论文集(下). 北京: 《决策与信息》杂志社, 北京大学经济管理学院, 2016: 136.

[7] 胡柏耀. 智慧城市建设背景下对信息安全管理的途径探索[J]. 智能建筑与智慧城市, 2022(5): 106-108.

[8] 齐峰. 大数据时代档案信息安全管理策略研究[J]. 智能城市, 2019, 5(23): 76-77.

[9] 梅彬. 基于人工智能理论的网络安全管理关键技术研究[J]. 信息网络安全, 2021(S1): 66-69.

[10] 杨国富. 计算机网络信息安全与管理初探[J]. 网络安全技术与应用, 2021(4): 158-159.

[11] 熊祖雄. 简析大数据背景下信息通信网络安全管理策略[J]. 网络安全技术与应用, 2021(3): 125-127.