新时代背景下网络安全问题与对策探讨

刘保明
山东裕隆矿业集团有限公司唐阳煤矿　山东　济宁　272508

摘　要：当前社会的电子化水平愈来愈高，互联网开始渗透到我们日常生活的方方面面，人们在互联网上实现信息与资讯的传递与互动。但是，在运用互联网的进程中，安全问题给国家信息安全以及我们的个人信息造成了极大的危害。本章内容主要针对新时期下的网络安全状况与问题展开研究，并指出了新时期下的网络安全防范措施。

关键词：网络安全；信息安全；问题及对策

引言

虽然每年国内公司在互联网领域花费很多，但在对如何正确认识并处理互联网威胁领域，大量公司还是技术水平不够。从安全性角度来讲，各种网络系统都不安全，由于具有许多未知的安全缺陷(漏洞)，每当新的系统安全缺陷被发觉，都被许多国外情报机构和黑客组织悄悄利用而目前的入侵检测手段都已经完全不能感知，防范也更无从谈起了。尽管所有的网络安全弱点都已经及时进行了公开，但网络上不法公司或犯罪分子的传播速度却极快，即使用了所谓的"零日漏洞"，抢着在系统恢复前就进行了入侵，并且往往会伴随着大量的勒索病毒攻击、数据泄漏等行为产生。新时期，随着物联网、计算机和五G网络等新兴科技的相继问世，安全问题显得越来越多样化。所以，怎样保障安全也变得特别重要。

1 对计算机网络安全问题的特点分析

1.1 影响网络安全的因素多

计算机网络从发展以来就一直受到着人们极大的重视，在当前的时代背景下计算机网络技术也获得了前所未有的发展。目前，随着计算机网络的基本架构和特性日益复杂，对计算机网络系统的管理显得愈来愈困难，同时近些年计算机网络的实际应用也在越来越的深入，因此导致影响其稳定性的原因也愈来愈多。为对付黑客攻击和病毒入侵，网络的管理员们专门成立了专业的抗黑客和防病毒机构，目的就是保护计算机网络上的主要服务器不遭受外来侵入[1]。然而，对于计算机安全的防护还不仅限于对服务器的保护，更重要的是计算机网络上传输的各种信息的安全性，必须过滤出其中的所有负面数据，以遏制网络中不良信息的蔓延。在网络攻击问题日益复杂的今天，网络安全技术的涵盖面也日益宽广。所以现阶段有关技术人员应该对影响网络安全的因素重点分析研究，归类整理，结合具体的网络安全问题进行针对的逐一解决，以提升网络安全的稳定性。

1.2 网络安全具有一定的相对性

计算机网络的绝对安全从来都不是绝对的安全性，并且目前没有、今后也不能出现绝对的安全性保障产品，所以所有企业机构都不能保证企业内部计算机网络的绝对安全。网络安全防范体系在和网络攻击系统的对抗过程中，不可避免的要出现完全瘫痪的情况，但是通过现代科技保护与法律制度的结合，就可以过滤掉了很多的网络安全危害。

1.3 网络安全管理需要适当的取舍

由于网络安全的保障需要一定的资金保障，也就必须兼顾网络安全稳定性和互联网经济的发展。不管是B-B的模式或是C-C的模式，盲目的强调系统的效率必定是以牺牲其安全为代价;相反，一旦明确要提高其安全，则其运营效率必定会作出相应的妥协[2]。计算机网络系统的研究发展和运营管理工作，也必须着重思考这个问题。

1.4 网络安全的黑盒性

网络安全的黑盒化主要表现为我们在运用网络安全防御的手段上，常常还不能完全知道是不是已经完全能够把病毒和木马程序与这样的网络攻击隔绝开来了，更无法了解杀毒软件究竟会对系统文件的安全产生怎样的危害。一般情况下，一般应用的功能都十分明确，但网络安全防范应用及管理系统的作用却具有相当的模糊性，需要专业的机构对其进行测评并加以推广应用。

2 网络安全形势及问题分析

其实，网络犯罪的出现有着深刻的社会根源，因此本文将就现阶段中国网络犯罪的主要形成根源加以总结剖析，大致包括了以下几层面的内容:

2.1 网民的网络安全意识不到位

互联网是一个虚拟的社会空间，本身也面临着很多的社会不稳定问题，这也是网络犯罪能够发生的主要原因。但是，任何犯罪只要能够得到有效的管控，就必定会被扼杀在摇篮里面，这也就表明了广大网友们如果能

够形成了相应的保护意识，也就一定能够大幅度降低了网络犯罪的发生概率。但是从总体上来说，因为网络的普及时间在我国来说还是相对比较短，以及中国很多数公民触网年限还不长，对网络的虚拟性了解不深，也没有建立科学的网络安全规范认识，这也给互联网违法事件的大量出现，创造了必要的"群众基础"。

2.2 配套法律法规不完善

自从人们走进网络世界以后，互联网治理便变成一种老大难现象，造成这一现象的根本原因就是相关立法的漏洞。从立法方面来说，立法存在着一定的权威性，但一定要进行系统的理论研究和实验才能有效落地执行;但是，互联网科技的发展非常快速，这也使得互联网法制建设和互联网犯罪现实存在严重脱节。有些互联网犯罪甚至是打着法制的擦边球，而在具体的处理流程中却出现没有法律依据的保护，这样在极大程度上纵容了互联网信息安全漏洞现象的出现。

2.3 网络安全技术发展滞后

相比于常规刑事管理，信息技术在互联网刑事犯罪管理中起到了决定性影响。要想完成对互联网犯罪活动的整治，还需要加大对安全科技的研究投入力度，以此达到对互联网犯罪行为的有效打击和防范。而从总体上看，由于互联网科技研究支持能力的薄弱，大部分公司还是把科技研究集中在企业服务领域以求获得更多利润[3]。最近几年，由于我国对互联网认可度的持续提高，部分网络公司提高了对互联网科技的关注度，并开始逐步向安全技术的应用领域倾斜。而就整体的市场安全性研究现状而言，由于安全科技无法有效形成投资效益，也就使得广大中小企业对安全科技研究的热情不高，安全管理缺少强大的科技保障。

2.4 网络违法犯罪活动高发

截至到二千零二零年的统计表明，中国互联网消费者已达到了十个多亿，包括外卖群体的网民四点四四亿，网约车人群已超过二点二五亿，利用这种庞大数据显示，他们的消费规模将越来越大，消费频次也越来越多。在二零一九年全年的互联网总消费额已经达到19715.8亿元，其中以淘宝的"双11"成交量尤为巨大，已经达到了三千亿人民币。互联网的便利显而易见的，由于网络与我们的生活联系得更加密切，在过去我们所担心的丢失银行卡、打不到车的问题已经得到了基本解决的今天，不法分子们又想出了新的"高招"。像生活中的二维码，其代表着用户的个人信息，至此给一些非法盈利机构和个人带去了盈利的机会，利用"二维码生成器"对各类病毒、流氓软件等进行改造，并利用网络等各种渠道大量传播，借此诈骗社会群众的金钱。这种非法牟利的做法直接侵犯了个人的经济利益，对经济安全和社会安定也将造成巨大的破坏。所以，保障消费者的财产安全、建立良好的网络平台已经成为当前相关机构和组织急需解决的问题。

2.5 计算机故障产生的潜在威胁

尽管目前电脑的系统功能非常强悍，并且工艺相当完善，但是计算机仍是一个精密的计算机，一旦使用不当或者运行环境不合适，很容易造成各种系统的机械故障。特别对于用作核心器件的存储器来说，假如发生问题，必将造成计算机用户数据，个人信息等重要文件的破坏，甚至极难修复。另外，环境温度的急剧改变和强烈振动也可能造成重要问题的出现。

2.6 缺之系统化的网络安全管理平台

其实，互联网犯罪管理是一项科技和管理相结合的事业，既不可完全依靠科技，也不可完全依靠管理。从近年来全球发展的管理案例分析，建立有效的互联网治理模式已是现阶段很多发达国家与地方的共识，它主要基于通过系统化网络平台的构建，可以高效集成信息技术的监管能力，进而达到对互联网犯罪行为的高效防范[4]。而就当前阶段中国互联网犯罪行为的控制和防范而言，网络安全管理工作还处在摸索时期，系统化安全服务的没有开展也将使得安全管理工作无法聚集各方资源，由此引发互联网刑事案件的时有发生。

3 网络安全防范对策

3.1 培养网络安全意识，做好安全防范

在中国互联网的这片新天地中，人在整个网络空间中扮演着至关重要的地位，这就更需要我们培养正确的互联网安全意识。在工作中，我们还需要做好:对重要数据、档案等资料进行备份，以保证安全;对未知U盘进行病毒查杀检测之后再使用;及时更换软件的安全补丁;加大用户口令管理力度;使用软件程序、软件时一定要做好提前检查，特别是可执行文件;不盗用他人资料，不盗用他人帐号。

3.2 完善与网络犯罪有关的法律条款

及时健全补充信息网络安全罪相关的法规规章，应当尽快形成信息网络罪相关的法规制度。现在中国在信息网络犯罪方面的法律体系日益完善，在《刑法修正案》中也明确提出了关于修改有关计算机与信息网络安全方面立法规则的规定，从中也可以看到，现在我国已经对更多的计算机与信息网络安全方面更加重视。不过在法规体系方面的调整和健全工作还一定要继续做好，而且由于中国网络的增长速度很快。所以网络安全技术

领域的法规规章还需要进一步调整，使之更为灵活[5]。在调整和健全刑法制度的过程中，要根据现在中国刑法所认定的非法进入计算机信息系统罪犯罪的范围比较狭小情况，制定刑罚措施能有效降低互联网犯罪的发生。尤其是针对公共信息安全违法的规模小的问题，应该通过已有立法的情况加以完善，同时在将要出台的《中华人民共和国网络安全法》中反映出来，从而完善我国的公共信息安全立法制度。

3.3 建立网络安全管理平台

网络安全维护对技术层面的要求较高，但是纯粹的技术无法实现绝对的网络安全。计算机网络管理工作人员需要建立专业的网络安全管理平台，制定安全管理预案和紧急事件紧急反应处理方案，从而把互联网信息技术纳入安全控制。另外，还要能够利用当前日益完善的大数据处理手段提高安全性，从而能够确保安全的可靠性。

3.4 培养和选拔高素质技术人才

对于安全防范需要专门的人员做保证，所以公司要针对企业的市场特性，合理选择高素质的专业人才;同时要增加对安全防范的投入，要提高人才的责任感，同时给人员提供培训知识和继续培训的机会。

3.5 做好5G时代信息安全防御工作

现在我们已正式走向了五G网络时代，因为五G网络在密度、传输速率等方面都有着超高的优势，而且时延超低，为人们提供了极大方便。不过目前中国五G网络的发展还处于初级阶段，其安全并不能获得较高的保证[6]。因此国家相关机构不但需要建立关于发展五G网络方面的制度与技术，而且还必须在对与五G网络相关的安全技术加强支持同时注意从技术层面，强化应用保密措施和隔离技术，以保障客户的信息安全，同时强化安全性检测，以建立更加安全稳健的五G网络，从而提高了五G网络中安全技术的安全稳定性。

3.6 加强网络安全监督体系的建设

科技发展的问题，使得互联网无法自行屏蔽这些不良信息。所以，可以通过强化互联网监督的手段减少对互联网形成的负面作用。针对网络，应由监管部门进行有效管理，这样对网络的环境安全性进行了保障，从而避免不法分子入侵网络平台，从而有效保障了用户和企业的利益，从而对国家的安全进行了保障。互联网监督不但要控制互联网整体和全部内容，而且必须有效的管理网络人群，防止其他不法分子的非法进入。加强对互联网监督力度可以有效减少互联网中的"病、毒、害"，进而维护无数网友的权益。随着目前科学技术的迅速发展和提高，与此同时，也需要通过科技这种更加有效的监管手段有效遏制传播不良信息的犯罪，在这个行业中，人工智能科技将会对未来发展起到很大的作用。

结语

新时期下，网络安全问题十分关键，我们应当提高互联网意识，指导全体网络成员自觉地遵循和保护网络空间的合理秩序，打击网络犯罪活动，为网络发展提供全面保障，主动进行人工智能、5G等新兴技术的研究。安全影响着我国安全和现代化的建设，必须要多管齐下，多措并举，才能从根本上解决互联网安全问题，促进我国的互联网建设和现代化建设，真正保障全体国民的权益，进而维护社会稳定和国家安全。

参考文献

[1]熊泽明. 计算机网络信息安全及防护策略研究[J]. 网络安全技术与应用，2020（04）：5-6.

[2]陈正欣.基于网络信息安全的研究与应用[J]. 内蒙古科技与经济，2020（05）：70-70+157.

[3]沈荃. 大数据时代下计算机网络信息安全问题分析[J]. 电脑编程技巧与维护，2020（02）：156-157+172.

[4]宋济明. 信息安全前沿技术及未来发展研究[J]. 信息与电脑（理论版），202032（03）: 204-206.

[5]王青峰.人工智能技术在网络安全防御中的应用研究[J]. 网络安全技术与应用，2020（05）：8-10.

[6]杨硕.浅谈计算机网络信息安全及防护策略[J]. 河北农机，2020（02）：63.