|  |  |  |
| --- | --- | --- |
| **本科生课程论文** | | |
|  | 题 目: | 中国网络安全 |
|  | 姓 名: | 董自经 |
|  | 学 院: | 人工智能学院 |
|  | 专 业: | 计算机科学与技术 |
|  | 班 级: | 1 |
|  | 学 号: | 19222126 |
| 2023年6月 07 日 | | |
| 南京农业大学教务处 制 | | |

**南京农业大学课程考核情况表**

**2022—2023学年第 2 学期**

**学 院： 人工智能学院 班级： 计科221**

**课程名称： 国家安全教育 学分： 1**

**学号姓名： 19222126 董自经**

**考核方式： 课程论文**

**考核内容：**（论文题目）**中国网络安全**

**评分标准：**

|  |  |  |
| --- | --- | --- |
| **课程论文评分标准** | **分 值** | **得 分** |
| 论文选题价值与合理性 | 15 |  |
| 理论联系实际及创新性 | 20 |  |
| 课程内容掌握程度 | 30 |  |
| 文字表达水平及文章的逻辑性 | 20 |  |
| 写作规范化程度（包括摘要、关键词、参考文献） | 15 |  |
| 课程论文成绩 | | 得分合计： |
| 按70%折合： |
| 平时成绩 | | 按30%折合： |
| 总成绩 | |  |

**教师签名：**

**时 间：**

中国网络安全

计科221董自经

摘要：中国作为一个拥有庞大互联网用户群体的国家，网络安全问题一直备受关注。随着互联网的不断发展，网络安全也面临着日益严峻的局面。本文将从中国网络安全的现状、主要威胁、安全措施和未来展望等方面进行综合分析，以期为读者提供一个全面了解和认识中国网络安全问题的视角。

关键字：网络安全，网络攻击，数据泄露，未来发展

一、中国网络安全现状

随着互联网的普及和网络应用的推广，中国已经成为整个互联网生态系统中比较大而且比较活跃的国家之一。2019年中国互联网网络发展报告显示，截至2018年底，中国网民规模达到8.29亿，互联网普及率达到59.6%[1]。但与此同时，中国网络安全问题也逐渐浮出水面。根据2019年中国互联网安全报告数据显示，2018年全年中国互联网安全事件数量超过6100万起，其中涉及恶意程序、漏洞利用、网络钓鱼、欺诈等各种类型。主要有以下几种类型：

（一）网络攻击事件呈现快速增长趋势

近年来，网络攻击事件呈现出急剧增长的趋势，破坏力不断上升。以2019年7月至9月中国互联网网络安全态势为例，我国互联网社会面临的攻击事件有恶意程序传播、网络钓鱼、勒索软件、DDoS攻击等。这些攻击方式的破坏能力十分强大，不仅会导致重要信息泄露，因此对社会经济和民生造成很大的影响。

除此之外，一些热门应用程序也成为了网络攻击者的重点攻击目标。例如，在2018年全年对全球智能手机设备的攻击中，中国占全球约21%，居全球前列。此外，随着人工智能、云计算、物联网等前沿技术的快速发展，网络攻击也不断借助其中的漏洞进行攻击，对网络安全造成了新的威胁。

（二）数据泄露问题引发广泛关注

在网络时代下，各项个人隐私已被数字化管理，因此数据泄露问题也引发了广泛关注。中国加强了对数据安全的监管规定，同时也执行了一些数据保护的法令标准。

据图迹科技数据显示，截至2018年底，全国网络数据泄露监测中心共监测到数据泄露事件17万多起，涉及企业和个人用户6300万多人次，其中中小企业是遭受数据泄露事件的主要受害者。这些泄露事件对个人隐私权和商业机构的利益产生了相当大的威胁，同时也引发了政府和其他机构对网络安全和数据管理的大规模关注。

（三）网络安全市场规模较小

针对于网络安全，自然有相应的公司去做相应的工作，根据中国网络安全产业联盟去年发表的报告统计，21年我国网络安全市场的规模在600亿元（人民币），同比增长超过15%，三年以来，我国的网络安全市场正在逐步增长，即使是疫情期间受到影响，但是这个行业的增长速度还是超过了10%。有关人员估计，未来几年里，网络安全市场的增长速度都会超过15%

二、中国网络安全主要威胁

随着中国网络使用量的剧增，网络安全问题不断增加，各种网络攻击手段也日益繁琐。下面分析中国网络安全的几个主要威胁。

（一）恶意代码危险性增加

恶意代码可以通过病毒、木马、蠕虫和间谍软件等形式入侵计算机，从而控制计算机中的重要信息。近年来，恶意代码已经成为了中国网络安全的主要威胁之一[2]。

根据iTrust公布的数据，我国恶意软件感染量排名前十的是：木马、广告软件、普通病毒、钓鱼网站、僵尸网络、蠕虫、间谍软件、安全漏洞网络扫描、后门和代理服务。

（二）社交媒体攻击变得更具威胁

随着社交媒体的普及，网络攻击分子也开始利用这种新型的攻击手段进行网络攻击，对个人隐私和网络安全造成威胁。社交媒体攻击主要包括社交工程、钓鱼攻击和被动攻击等，这些攻击方式的威胁性日益增加，因此对于用户来说也需要加强对于网络平台的保护和隐私管理。

（三）大规模网络攻击事件

随着网络技术的升级，大规模网络攻击事件也正在变得越来越常见。例如，有名的“黑色星期五”网络攻击事件，就导致了全球超过10万部手机被感染，用户的个人信息被盗窃。这种大规模的网络攻击事件对于受害者的损失和对网络安全的影响是相当大的。

三、中国网络安全的安全措施

（一）网络安全法的实施

2016年，中国通过了网络安全法，这标志着中国官方开始系统化、法律化地加强对于网络安全的立法和监管工作。该法包括了对个人用户和企业技术部门的网络安全保护要求，对于涉及网络安全的犯罪行为也进行了集中打击。

此外，政府组织了“网络安全协会”和“网络安全检测与预警中心”等机构，加强对于网络攻击和数据泄露事件的应对和管理。在一些重要信息系统中，中国还推行了安全认证标准，通过技术手段对网络安全问题进行监管和限制。

（二）加强企业网络安全管理

企业网络安全是整个网络安全体系中的重要组成部分。强化企业网络安全意识，加密网络保密，提高企业网络安全运营的能力，都是当前中国加强网络安全的关键。因此，中国的一些企业通过提供培训、资金和技术等支持，提高员工网络安全意识，优化网络安全管理模式，实现加密和保密工作的合理布局。

（三）多方合作，共同推进网络安全

中国政府多次强调网络安全的重要性，并与其他国家的政府、组织和企业保持着合作关系，共同推进网络安全。例如，中国与美国、俄罗斯、欧盟等国家与地区之间都有网络安全合作的协议，共同成立了网络安全联合论坛和网络安全领导力小组。这些国际合作机制在确保网络关键设施的安全和信息安全方面发挥了重要的作用。

四、中国网络安全未来发展

随着人工智能、5G等新技术的不断发展，中国网络安全所面临的挑战也逐渐加强。因此，在加强技术研发、加强政策法律和打击网络犯罪等方面，中国政府还需加大努力，同时个人与企业也要更加重视网络安全工作。

（一）加强技术安全防范

技术安全是未来网络安全的核心，加强技术防范是未来网络安全的重点。因此，在人工智能、5G等新型技术的发展过程中，要加强网络安全和数据科技的研究，对网络攻击形式进行不断的更新和完善，提高相应的网络防御能力和抗击能力。

此外，应加强对于数据安全的建设，2021年，我国的大数据产业规模达到了1.3万亿元（人民币），数据量较大。应当进一步对数据的分类、分块进行划分。而且现在对于数据的走私较为便捷，一个小的SD卡上可能就有上亿公民的身份信息。所以，数据一旦泄露，后果将不堪设想。

（二）完善法律法规

完善有关于网络安全方面的法律法规，现有的法律法规在一些方面岁可以有效的保护国家的网络安全，但还存在着些许的漏洞，一些不法分子还是有机可乘，应当将这些漏洞填补，让这些不法分子无从下手[3]。而且，在一些较为偏远的地区，网络警察的数量严重不足，导致及时有法律也无法有效地执行，国家会提高边缘地区的工作的待遇，招募更多的网络警察维护网络安全。

网络安全法旨在加强网络安全法律规范和管理，强化网络安全监管是确保中国网络环境安全的重要保障。中国政府应加大力度完善法律和法规制度，形成完整的法律要素体系，提高网络法制化水平。

（三）加强个人网络安全意识

个人网络安全意识是构筑网络保护体系的基础。因此，政府和企业应该加强对于公众的普及教育，提高人们对于网络安全的认识，使个人和企业具备更高的防范意识，切实增强对于网络安全的保护工作。尤其是对一些年纪较大的公民，他们对于网络安全的概念很模糊，对自身的防范也很弱，很容易就成为不法分子的目标。

（四）对海外的监督更加严格

近年来，随着科技的发展，中国与其他国家的交流变得更加频繁，导致和其他国家的网络交流也变得频繁起来，虽然有着“长城防火墙”的隔离，但是我国国民教育已经达到了较为高等的水平，基本上每个人的身边都或多或少的存在着“翻墙”的行为，国家不会制止这些行为，但有一些对中国不当言论的网站，中国会加强相关信息的检索并及时将网站查封，减少国家的损失。

五、总结

中国网络安全问题近年来日益繁琐和复杂，解决网络安全问题需要政府、企业、个人共同努力[4]。政府要加大对法律法规和技术研究的投入，在网络安全立法、技术研发、加强管理等方面发挥重要作用。企业同样需要思考和投入网络安全建设，任何一家企业的网络安全事件都会对整个互联网生态系统产生影响。个人和企业也应加强网络安全自保，增强网络安全意识和技能，做好网络保护工作，彻底杜绝网络安全事件。只有共同合作、共同发展，才能保障网络安全和保护所有人的数字生活安全。"

参考文献：

[1] 高微.习近平关于思想政治教育的重要论述研究[D].陕西师范大学博士论文,2020:15

[2] 吕臻,王宝红.浅谈政府机关计算机网络安全[M].计算机光盘软件与应用,2012:45-46

[3] 李秋江.基于网络处理器的防火墙安全过滤设计与实现[D],中国科学院研究生院（计算技术研究所）硕士论文.2014:28

[4] 高岚.云南对ASEAN国家贸易中电子合同及单据的风险及控制研究[D],昆明理工大学硕士论文.2009:9