|  |  |
| --- | --- |
| **所在学院** | **人工智能学院** |

**《形势与政策》学期课程作业**

论文题目： 中国网络安全

姓名学号： 董自经 19222126

专业班级： 计科221

学年学期： 2024-2025学年第一学期

|  |  |  |  |
| --- | --- | --- | --- |
| 参考标准（在相应标准后的方框里打√） | | | |
| 选题正确新颖 优 □ 良 □ 合格 □ 不合格 □  论证严密充分 优 □ 良 □ 合格 □ 不合格 □  领会全面透彻 优 □ 良 □ 合格 □ 不合格 □  行文规范流畅　 优 □ 良 □ 合格 □ 不合格 □ | | | |
| 成 绩 |  | 教师签名：  日 期： |  |

南京农业大学马克思主义学院 制

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

总体国家安全观强调国家安全是一个系统性、综合性的概念，涵盖政治、经济、军事、文化、社会、科技、信息、生态等多个领域[1]。在新时代背景下，网络安全作为国家安全的重要组成部分，愈加受到重视。随着信息技术的快速发展，网络空间的安全风险日益增加，网络攻击、信息泄露等事件频发，直接威胁到国家安全和社会稳定。因此，习近平总书记指出，必须以整体安全观来推进网络安全工作，增强网络空间治理能力，构建安全可靠的网络环境。通过加强网络安全法治建设和技术保障，确保国家在数字化时代的顺利发展和安全[2]。

**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%[3]。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。主要有以下两种类型：

（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。

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两个主要威胁。

（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[4]。

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、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。

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[5]。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。

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。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] 总体国家安全观学习纲要[J].人民出版社,2022:9-11

[2] 中央网络安全和信息化委员会办公室.习近平总书记关于网络强国的重要思想概论[J].人民出版社，2023:20-30

[3] 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

[4] 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

[5] 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