

对我国周边安全环境的认识与思考

——以网络空间安全为例

杨亿酬，3230105697

工科试验班（竺可桢学院图灵班） 周二 1, 2 节

1 国家安全

1.1 国家安全的概念

国家安全是指国家政权、主权、统一和领土完整、人民福祉、经济社会可持续发展和国家其他重大利益相对处于没有危险和不受内外威胁的状态，以及保障持续安全状态的能力。国家安全利益是国家的最高利益。国家主权是国家安全的核心，它不是一个抽象的、孤立的概念，而是体现在国家的政治、经济、社会、文化、军事、外交等诸多方面，抽离任何一方面的内容，都是对国家主权的侵害，也是对国家安全的威胁。因此，我们要坚持总体国家安全观，以人民安全为宗旨，以政治安全为根本，以经济安全为基础，以军事、文化、社会安全为保障，以促进国际安全为依托，维护各领域国家安全。

1.2 国家安全的重要性

国家安全的重要性是多层面的。

首先，国家安全保障国家生存和发展，是国家利益得以实现的根本前提。无论是经济发展、社会稳定，还是国际合作，都需要一个稳定的安全环境作为支撑。没有安全，国家的政治制度、经济体系和社会结构将遭到严重挑战，甚至可能导致国家的解体。

其次，国家安全与国际环境密切相关。在当今复杂多变的国际关系中，任何一个国家都无法完全置身事外。国际上的纷争、战争、恐怖主义等威胁，时刻可能波及到各国。因此，维护国家安全不仅是国家内部的事务，更是参与国际合作与对抗的重要手段。

最后，国家安全关乎的国家综合国力。随着国际竞争的加剧，国家安全的保障不仅仅依赖于传统的军事力量，更依赖于经济、科技、文化等多方面的综合实力。因此，增强综合国力、提升国家安全能力，是确保国家在全球竞争中立于不败之地的关键。

综上所述，国家安全的重要性不容小觑。它是国家生存和发展的基石，是保障国家利益实现的核心保障，是综合国力竞争的关键所在。在全球化和信息化迅速发展的今天，国家安全已经不再局限于传统的军事安全，而是涵盖了政治、经济、文化等多个领域，成为国家综合实力的重要组成部分。

1.3 国家安全的现状

在新时代背景下，尽管我国的综合国力日益增强，国内外局势趋于稳定，但国家安全仍面临诸多复杂和严峻的挑战。随着国际形势的变化和科技进步带来的新威胁，国家安全的内涵已经发生了深刻变化，从传统的军事安全扩展到了经济、政治、文化、网络等多个领域，安全威胁的多元化和隐蔽性使得国家安全形势更加复杂。

外部安全威胁依然存在。经济全球化加剧了各国之间的战略竞争。美国及其盟友在亚太地区的军事存在、频繁的外交压力和意识形态对抗，尤其是中美关系的紧张，仍是我国国家安全的重要外部挑战。此外，地区性冲突、恐怖主义威胁及国际犯罪的跨国性，也使得我国在全球安全环境中面临较大的压力。

非传统安全威胁日益突出。在全球化背景下，信息化、网络化的迅速发展，使得网络安全、数据安全成为新的关键问题。网络攻击、数据泄露和信息战等行为，已经不仅仅是技术问题，更与国家安全息息相关。2023 年，全球范围内的重大网络安全事件层出不穷，我国亦面临着来自外部和内部的网络攻击，尤其是在金融、能源、军事等敏感领域。

尽管我国在维护国家安全方面取得了诸多成就，但面对全球化与信息化背景下日益复杂的威胁，国家安全的挑战依旧严峻。只有进一步加强各领域的综合防范能力，才能确保国家的长期安全与稳定。

2 非传统安全之于我国周边国家安全

2.1 我国周边国家安全

我国国内安全环境受众多因素影响：疆独蠢蠢欲动、藏独伺机而动、台独活动持续不断、泛蒙古主义有所抬头、港独意识重现、海上安全问题突出。

我国周边国家安全还深受国际形势影响，本世纪以来国际形势具有以下特点：国际政治经济秩序面临深刻调整，全球化两极分化加剧；西方国家面临体制结构调整震荡；西亚北非动荡难息；美国战略重心东移；俄罗斯复兴势头增强。

总体而言，大国博弈加强，尤其美国对华发起全面战略竞争；传统与非传统“双安全”风险上升。中国外部环境发生复杂变化，中国坚持和平发展不动摇。

2.2 总体国家安全观

2014 年 4 月 15 日，习近平总书记主持召开中央国家安全委员会第一次会议。^[1] 习近平总书记在讲话中首次提出总体国家安全观，阐述了总体国家安全观的基本内涵。总体国家安全观是指坚持国家利益至上，以人民安全为宗旨，以政治安全为根本，统筹外部安全和内部安全、国土安全和国民安全、传统安全和非传统安全、自身安全和共同安全，完善国家安全制度体系，加强国家安全能力建设，坚决维护国家主权、安全、发展利益。国家安全包含以下领域：

- 政治安全：维护国家政权、制度和意识形态安全。
- 经济安全：保障国家经济稳定和持续发展。
- 军事安全：保卫国家领土完整和军事利益。
- 文化安全：保护国家文化遗产和文化多样性。
- 社会安全：维护社会稳定和公共秩序。
- 科技安全：保障国家科技创新和信息安全。

2.3 国家安全重心正在转移

国家安全的重心随着时代的发展和全球局势的变化，发生了显著的转移。如今，经济安全、能源安全、网络安全、生态安全等非传统安全威胁已成为国家安全的重要组成部分。例如，网络攻击、数据泄露、供应链中断等新型安全问题，不仅影响国家的经济与科技发展，也可能对社会稳定产生严重威胁。

随着全球化的推进，国家间的相互依存关系日益增强，传统的边界防御已不能完全应对全球范围内的安全挑战。跨国犯罪、恐怖主义、气候变化等问题成为新的威胁源。特别是在全球疫情、气候变化等全球性挑战面前，国家安全的范畴不再仅仅局限于国土的防卫，更多涉及全球合作与共治。

我国提出“总体国家安全观”意味着国家安全的重心从单一的军事防御扩展到了国家生活的各个方面，强调系统性、全面性和协调性。国家安全的保障不仅依赖于硬实力，还依靠文化软实力、信息技术、国际合作等多方面的因素。

2.4 非传统安全的重要性

冷战结束后，国际社会出现许多新的安全威胁，即非传统安全威胁因素，包括经济动荡、金融风险、生态环境恶化、网络攻击、资源危机、恐怖主义、武器扩散、疾病蔓延、跨国犯罪、走私贩毒、非法移民、海盗、洗钱等，其中最突出和最严重的威胁来自国际恐怖主义和大规模杀伤性武器的扩散。非传统安全的重要性在于它涵盖了从经济、环境到社会、科技等多方面的威胁，涉及的问题更加复杂和广泛。随着全球化的深入发展和科技进步，非传统安全威胁的表现形式也愈加多样化，这些问题都对国家的稳定与发展构成挑战与威胁，国家安全战略需要从传统的军事防御扩展到更全面的安全观，确保国家在面对多元化安全威胁时能够有效应对，维护社会的长期稳定和可持续发展。

3 网络空间安全概述

3.1 网络空间安全的概念与目标

网络空间安全是指在信息化社会中，保护网络及其相关信息、系统、数据和服务免受来自各种威胁的侵害，确保网络的正常运行、信息的安全传输以及数字化社会的稳定。随着信息技术的迅猛发展，网络空间已成为一个重要的领域，涵盖了互联网、通信网络、云计算、大数据等数字化基础设施。在这一背景下，网络空间安全不仅仅是对网络硬件和软件的保护，更包括信息安全、数据隐私、网络信任等多个维度。

网络安全的核心目标是保障以下几个方面：网络正常运行、信息保护、隐私保护、防范网络攻击、保障网络信任。

3.2 网络空间安全的重要性

“网络空间已成为国家继陆、海、空、天四个疆域之后的第五疆域，与其他疆域一样，网络空间也须体现国家主权，保障网路空间安全就是保障国家主权”——中国工程院院士 倪光南

网络空间安全不仅关乎国家的网络基础设施和数字经济的安全，还直接影响到国家的政治、经济、军事、社会等多个层面的安全。^[2]

网络空间安全的重要性体现在以下几个方面：

1. 保障国家基础设施安全

国家的关键基础设施（如电力、交通、金融、电信等系统）越来越依赖于网络技术，一旦这些基础设施遭受网络攻击或数据泄露，将对国家安全造成重大影响。

2. 维护国家政治安全

在数字时代，政治安全和信息安全紧密相连。网络空间已成为国家间信息战、舆论战和心理战的重要战场。通过网络传播，敌对势力可以通过虚假信息、网络舆论操控等手段，干预国家的政治稳定与社会和谐。

3. 保护经济安全

现代国家经济的运行高度依赖于数字技术，尤其是在金融、电子商务、制造业、物流等领域，网络技术的广泛应用让这些产业更加高效与便捷。然而，这也使得国家经济面临前所未有的网络风险。网络攻击、数据泄露、黑客攻击可能导致重要经济数据丢失、财务损失，甚至干扰国际贸易与跨境金融活动。

4. 加强军事安全

在现代战争中，网络已成为与传统军事力量并列的重要作战领域。网络战、信息战等新型战争形式的兴起，使得国家的军事安全不仅依赖于传统的陆海空军力量，还必须保障网络战能力。通过网络空间攻击，敌对势力可以摧毁军事指挥控制系统、干扰武器装备、瘫痪卫星通信和全球定位系统等，从而削弱国家的防卫能力。随着网络攻击技术的不断发展，网络战在现代战争中的作用愈加突出，网络空间安全对国家军事安全的保障作用愈加重要。

5. 维护社会安全与公共安全

社会安全也受网络空间安全的影响，尤其是涉及到公共服务系统、社会治理和民众生活的网络平台。现代社会中，政府、企业及个人信息的存储和交换都依赖于网络技术。一旦个人隐私或政府敏感信息被黑客窃取或篡改，可能引发社会的不安和恐慌。与此同时，网络诈骗、网络暴力、网络犯罪等社会治安问题的日益严重，也要求国家采取更加有力的措施来保障网络空间的安全。

6. 防范跨国网络犯罪与恐怖主义威胁

网络空间的开放性和无国界性使得跨国网络犯罪和网络恐怖主义成为全球安全的一大威胁。通过互联网，犯罪分子和恐怖组织可以进行非法资金转移、传播极端思想、实施网络攻击等活动。

7. 提升国家综合国力与国际竞争力

网络空间的安全不仅影响国家的内部稳定，还在很大程度上影响其在国际社会中的地位和竞争力。数字经济的发展、网络创新、人工智能、大数据等新兴技术的应用，已经成为国际竞争的重要组成部分。拥有强大网络空间安全能力的国家，能够更好地保护其科技创新成果、数字经济基础设施和网络信息资产，提升其国际话语权和竞争力。

3.3 一个例子

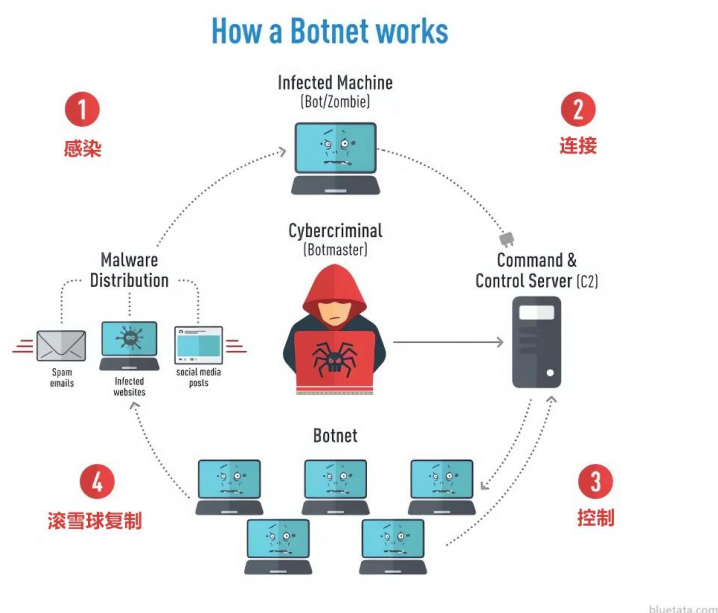


图 1：僵尸网络工作原理^[3]

<https://blog.csdn.net/dietime1943/article/details/13360813>

僵尸网络是一个网络空间安全问题的简单例子，僵尸网络通过病毒等方式传播僵尸程序控制计算机，利用僵尸主机发起攻击行为：发送垃圾邮件、窃取数据、传播勒索软件、进行欺诈性广告点击，以及实施分布式拒绝服务（DDoS）攻击。DDoS 攻击，全称分布式拒绝服务攻击，通过向目标发送大量无效或高流量网络请求，消耗对方系统资源，从而达到使对方系统崩溃的目的。^[4]

2015 年，美国总统办公室的计算机系统就曾遭到网络间谍的入侵，利用僵尸网络等手段，黑客成功获取了大量敏感数据。2016 年美国著名的 Dyn 公司遭受了一次大规模的 DDoS 攻击，攻击者利用了一个大型的物联网僵尸网络（主要由摄像头、路由器等设备组成），使得多个大网站（如 Twitter、Netflix、Spotify 等）无法访问。这起攻击并没有直接针对某个国家或政府部门，但其背后的僵尸网络利用了全球范围内的大量物联网设备。2016 年，美国总统大选期间，有报道称，俄罗斯利用僵尸网络和假账号进行信息战，干扰选举进程和公众情绪。通过社交媒体平台发布虚假信息、煽动对立情绪等手段，俄罗斯被指控在美国大选中通过网络手段进行干预，影响了选民的投票行为。僵尸网络也成为了这种信息战的重要工具。

4 总结与思考

作为新时代的青年大学生，我们肩负着时代赋予的使命。网络空间的安全不仅仅是政府、军队和网络安全专业人士的责任，广大的青年群体，尤其是青年大学生，应该积极参与到这一国家战略中。我们应当增强国家安全意识，树立正确的价值观，理解国家安全在社会中的重要性，并通过自身的行动支持国家的网络安全建设。

在国家安全问题日益复杂和多元化的今天，青年大学生应当充分认识到自己在国家安全中的独特作用。首先，作为新时代的知识分子，我们有责任向周围的同学和社会普及网络安全知识，提高全民的网络安全意识，防止个人信息泄露和网络诈骗等问题的发生。其次，作为未来的科技人才，我们可以将所学的专业知识运用到实际工作中，为国家的网络安全建设提供技术支持和创新方案。例如，人工智能、大数据、区块链等技术可以有效提升网络安全防护能力，预防网络攻击，打击网络犯罪。

作为一个青年大学生，应当发挥自身专业优势维护网络空间安全、新时代的大学生应发挥各自优势维护各类安全，进而发挥总体优势维护我国周边国家安全。

参考文献:

[1] 中央国家安全委员会第一次会议召开 习近平发表重要讲话
https://baike.baidu.com/reference/13777610/533aYd06cr3_z3kATKWCxPn4MXrNmD_5vuXTULdzzqIP0X0pX5nyFI899pk88Lh_HQXctZYtMoZEwqX6D1RE6-hDLrNxF-tm8nT5VjrEzb_4p51s

中央政府门户网站 . 2014-04-15

[2] 高世洁. 中国网络安全国际挑战及应对策略研究 [D]. 河南师范大学, 2023. DOI:10.27118/d.cnki.ghesu.2023.001179.

[3] bluetata. (2023). 【云计算网络安全】僵尸网络详解：工作原理、控制和保护方法. [在线]. CSDN 博客. 取自: <https://blog.csdn.net/dietime1943/article/details/133608132>

[4] 诸葛建伟, 韩心慧, 周勇林, 等. 僵尸网络研究 [J]. 软件学报, 2008, 19(3):14. DOI:10.3724/SP.J.1001.2008.00702.