天津外国语大学

国际关系学院

《非传统安全问题研究》课程作业

题　目：	**非传统安全视角下的网络安全问题研究—以俄罗斯为例**		
课程名称：	非传统安全问题研究	**任课教师：**	杨佳伟
开课时间：	2025 -2026 学年第 1 学期		
专　业：	外交学		
学生姓名：	Matveeva Anastasiia 黑玉	**学　号：**	GGXL22002
任课教师评语：			
评　分：			

内容

引言

在数字化进程不断加快以及全球相互依存程度不断加深的背景下，网络空间已逐渐成为现代国家运行的重要领域之一。信息通信技术广泛应用于国家治理、经济运行、金融体系和社会领域，一方面显著提升了社会运行效率与系统韧性，另一方面也在客观上加剧了国家在网络空间中面临的安全脆弱性。网络攻击、数据泄露、网络犯罪以及信息影响活动，能够在不直接使用军事力量的情况下，对政治稳定、经济安全和社会信任产生深远影响。

在此背景下，网络安全被纳入非传统安全分析框架，被视为一种具有跨国性、复杂性和高度动态特征的安全威胁[1][4]，其传播速度快、溯源难度大，并对政治、经济和社会领域产生综合影响。对俄罗斯联邦而言，地缘政治紧张、制裁压力、经济数字化以及关键信息基础设施保护和数字主权问题，使该议题具有突出的现实紧迫性，因此从非传统安全视角研究网络安全及相关国家政策具有重要理论和实践意义。

研究目的与研究任务

本研究的目的在于对网络安全作为一种非传统安全威胁进行系统分析，并在国家安全体系转型与数字化背景下，探讨俄罗斯联邦在应对网络威胁方面的国家政策特征。为实现上述研究目的，本文拟重点完成以下研究任务：

- 阐明非传统安全威胁的内涵、特征及其主要表现形式；
- 明确网络安全在非传统安全体系及国家安全体系中的地位与作用；
- 分析当前阶段俄罗斯联邦面临的主要网络安全威胁类型；
- 探讨俄罗斯网络安全领域的规范性法律框架与制度性安排；
- 研究国际合作在网络安全保障中的作用及其实现方式；

研究对象与研究内容

研究对象为数字化与全球安全威胁转型背景下的俄罗斯联邦国家安全体系。研究内容（研究客体）为作为非传统安全威胁的网络安全问题，以及俄罗斯联邦在该领域所实施的国家政策及其调控机制。

研究方法

本文以系统、综合的研究思路为基础，综合运用多种**一般性与专门性研究方法**，具体包括：

- **分析与综合方法**：用于梳理和归纳网络安全相关理论研究成果；
- **系统分析方法**：将网络安全视为国家安全与国际安全体系中的重要组成部分进行整体考察；
- **比较分析方法**：对不同国家和不同政策模式下的网络安全治理路径进行对比研究；
- **规范分析（法理分析）方法**：用于分析俄罗斯联邦网络安全领域的战略文件与法律规范；

- **官方文件与政策文本分析法**：通过研究政府文件和权威分析报告，评估俄罗斯网络安全政策的实际运行情况。

一、 非传统安全与网络安全的理论基础

(一) 非传统安全威胁的概念与特征

在传统安全观中，国家安全主要是通过军事威胁和领土完整保护的视角加以理解的。然而，随着全球化进程的不断深化、科技发展的加速以及国家间相互依赖程度的显著提升，安全威胁的内涵不断扩展，逐渐形成了**非传统安全**的概念。非传统安全主要涵盖一系列非军事性质的安全威胁，这些威胁能够对国家、社会以及国际关系体系的稳定性产生深远影响。

具体而言，非传统安全威胁包括生态与气候危机、传染病流行与全球性疫情、跨国犯罪、恐怖主义、经济与金融不稳定，以及伴随社会各领域数字化进程而产生的网络安全威胁等。这类威胁往往不以直接军事冲突的形式出现，但其破坏性和长期影响不容忽视。[3]

非传统安全威胁具有跨国性、复杂性和高度动态等特征，并与传统安全威胁相互交织，其影响往往超越国界并同时波及政治、经济和社会等多个领域。因此，应对非传统安全威胁不能仅依赖军事手段，而需要通过政府、私营部门与国际组织的协调合作，采取综合性治理路径。[2]

(二) 网络安全作为非传统安全的重要组成部分

网络安全是指通过法律、组织和技术等多种手段，对网络空间进行系统性保护的总体安排，其保护对象包括信息网络、数字数据和信息系统，旨在防范未经授权的访问、网络攻击以及其他破坏性行为。与传统安全威胁不同，网络威胁通常不以直接使用武装力量为表现形式，但其所造成的后果在影响范围和破坏程度上，往往能够对国家安全产生同等甚至更为严重的影响。[5]

针对国家信息资源、关键基础设施、金融系统以及大众传媒系统的网络攻击，充分表明网络安全在本质上符合非传统安全威胁的核心特征。这些特征主要体现在威胁的非物质性、传播速度快、跨国性显著，以及其可能造成重大的社会、经济和政治损害。网络攻击不仅能够破坏技术系统的正常运行，还可能引发社会秩序紊乱、经济损失扩大和政治稳定受损。

随着数字化深入发展和国家对信息技术依赖的增强，网络安全在非传统安全体系中的重要性日益突出，成为影响国家治理、经济安全和社会稳定的关键因素。因此，网络安全不仅是应对非传统安全威胁的重要领域，也是保障国家可持续发展和维护国家主权的重要支撑。

(三) 网络安全在国家安全体系中的地位

在当代背景下，随着国家治理、经济运行和社会生活的深度数字化，网络安全已成为国家安全体系中的重要组成部分。信息通信技术是关键基础设施、金融体系、

国家机关和公共服务正常运行的基础，其受损不仅会造成经济损失，还可能破坏政治秩序、社会稳定并削弱公众对国家治理的信任。

基于对网络威胁规模性和复杂性特征的清醒认识，各国逐步将网络安全纳入国家安全战略框架之中，通过完善法律法规体系、设立专门管理机构，并推动跨部门及国际层面的协调与合作，构建系统化的网络安全治理机制[7]。在这一过程中，网络安全逐渐发挥出**连接性与系统性枢纽作用**，将信息安全、经济安全与政治安全有机整合，成为国家安全体系中的关键支撑因素。

二、 俄罗斯联邦国家安全面临的主要网络威胁

(一) 当代国际网络安全环境与俄罗斯的地位

当代国际网络安全环境呈现出网络威胁数量持续上升、影响范围不断扩大以及技术复杂性显著增强的趋势，这一点已得到国际组织和各国网络安全主管机构的普遍确认。根据联合国以及国际电信联盟（ITU）的评估，[13],[16]网络威胁已成为当今发展最快、影响最广的安全风险之一，其影响对象涵盖关键基础设施、国家治理体系、金融系统以及社会领域。大规模数字化进程显著增强了国家对信息通信技术的依赖程度，并由此加剧了国家系统在网络攻击面前的脆弱性。

在此背景下，网络空间已演变为独立的国际竞争领域，国家与非国家行为体通过网络行动、网络犯罪和信息影响等方式参与其中。联合国相关文件已正式确认这一趋势，[13]强调网络威胁的跨国性及其对国际关系稳定的潜在影响。

俄罗斯联邦在国际网络安全领域的国家政策正是在上述背景下逐步形成的，其核心在于将**国内治理措施与对外政策工具相结合**，以维护国家在数字空间中的安全利益。近年来，俄罗斯持续推进网络安全领域的规范性法律体系建设和制度化合作机制，明确将应对网络威胁与巩固数字主权作为国家安全政策的重要目标。

在该领域具有基础性意义的文件是《俄罗斯联邦国际信息安全领域国家政策基本原则》（2021 年通过）[9]，该文件明确提出若干优先方向，包括：深化国际合作、防止利用信息通信技术引发冲突、完善信息通信技术领域的法律规范，以及加强关键基础设施的保护。文件明确指出，国际信息安全是国家整体安全体系中不可分割的重要组成部分。

俄罗斯一贯主张在联合国框架下推进网络空间的多边国际法律规制。2024 年，联合国大会通过了在俄罗斯积极参与下制定的《打击将信息通信技术用于犯罪目的的公约》，该文件旨在加强对网络犯罪的打击，保护数据安全，并维护国家在数字领域的主权。[14]

除多边合作机制外，俄罗斯还积极发展**双边信息安全合作**。例如，俄罗斯联邦与伊朗伊斯兰共和国于 2024 年生效的信息安全合作协定，明确规定双方将在关键基础设施保护、经验交流以及网络威胁应对法律框架协调等方面开展合作。这类双边机制有助于在实践层面提升国家间网络安全协同能力。

在国内层面，俄罗斯已建立起较为完善的**跨部门协作体系**，涵盖俄罗斯内务部、联邦安全局等主管机构的专门部门，以及打击网络犯罪和保护关键基础设施的跨部门工作组。这些机制旨在提高对网络安全事件的快速响应能力，并确保国家网络安全战略目标的有效落实。

(二) 主要网络威胁类型：针对俄罗斯的网络威胁

1. 对关键信息基础设施的网络攻击

针对关键信息基础设施的网络攻击是俄罗斯联邦面临的最为严重的网络安全威胁之一。关键信息基础设施涵盖能源系统、交通运输体系、银行与金融部门以及国家信息资源等关键领域。这些基础设施一旦遭受攻击并导致运行中断，可能引发大规模经济损失、公共服务失灵以及社会秩序不稳定。这一点已在国家安全领域的相关学术研究和法律文件中得到官方确认。

根据行业分析报告和权威研究数据（包括网络安全公司 F6 发布的分析材料），近年来针对俄罗斯组织的网络攻击在数量和技术复杂程度上均呈现出持续上升趋势。其中，**分布式拒绝服务攻击**、**高级持续性威胁组织活动**、**恶意软件攻击**以及**数据泄露事件**仍是最为常见的攻击形式，并且其攻击目标日益集中于数字基础设施中的关键环节。[18],[17]

随着数字化和自动化进程的推进，国家治理和经济运行对信息技术的依赖不断加深，客观上加剧了关键信息基础设施的脆弱性，使针对其的网络攻击成为系统性风险，亟需国家层面的综合治理与制度化应对。国际组织的相关研究亦表明，此类网络威胁具有明显的跨国性和系统性，已成为全球网络安全领域的共同挑战。

2. 信息安全与网络影响

信息安全在网络威胁结构中占据着特殊而重要的地位，其内涵不仅涵盖信息保护的技术层面，还涉及对信息空间的操纵、虚假信息的传播以及通过数字平台和社交媒体对社会意识的影响。将网络技术用于信息影响活动，可能加剧社会分化，削弱公众对国家机构的信任，并为国内政治不稳定埋下隐患。

当代关于信息战和网络影响的研究表明，信息行动日益呈现出**综合化特征**，即将技术层面的网络攻击与心理战、舆论操控和媒体传播相结合。在国际网络竞争加剧的背景下，此类威胁逐渐具备战略属性，并被视为非传统安全威胁的重要组成部分。[10]

对于俄罗斯联邦而言，信息安全保障与维护国家信息空间安全、抵御外部信息影响以及巩固数字主权密切相关。这一立场已在俄罗斯官方战略文件及相关学术研究中得到明确体现，凸显了信息安全在国家安全体系中的关键地位。

3. 数据保护与数字主权

在数字化进程不断推进以及数据处理规模呈指数级增长的背景下，个人信息、企业数据和国家信息的保护重要性日益凸显。数据泄露、对信息系统的未经授权访问以及对外国数字平台的依赖，已在官方层面被视为可能削弱国家稳定性并危及数字主权的重要因素。

对于俄罗斯联邦而言，**数字主权**意味着国家具备对本国信息资源、关键技术以及关键信息基础设施进行自主掌控和有效管理的能力，从而确保国家治理体系和经济系统在数字领域的独立、安全运行。在这一语境下，数据保护不再仅仅是技术

层面的安全问题，而是上升为国家安全和国家政策的重要组成部分，具有明显的战略意义。

三、 俄罗斯网络安全领域的国家政策

(一) 规范性法律基础与战略性文件

俄罗斯联邦在网络安全领域的国家政策，建立在一系列战略性与规范性法律文件之上，这些文件共同构成了在信息与数字空间中维护国家利益的法律与制度基础。其中，《俄罗斯联邦国家安全战略》（2021 年）在整体安全框架中占据核心地位，文件明确将信息安全与网络安全列为保障国家主权、社会稳定以及在数字化条件下实现可持续社会经济发展的关键方向。[7]

在国家政策的具体构建过程中，《俄罗斯联邦信息安全学说》（2016 年）发挥着重要作用。该文件系统界定了信息领域面临的主要威胁及其应对原则，强调将关键信息基础设施、国家信息资源以及公民在数字环境中的合法权益置于优先保护地位，同时明确提出通过综合性、跨部门协作机制来保障信息安全与网络安全的必要性。[11]

作为对国内法律规制的重要补充，《俄罗斯联邦国际信息安全领域国家政策基本原则》（2021 年通过）进一步明确了俄罗斯在国际层面的政策取向。该文件确立了发展国际合作、防止利用信息通信技术引发冲突以及推动形成网络空间国家行为国际法律规范的官方立场，并特别强调巩固数字主权的重要性，明确反对将信息通信技术用于破坏国家安全的行为。

(二) 网络安全保障的制度性机制

俄罗斯联邦网络安全政策的实施依托于专门国家机构体系和跨部门协作机制。其中，俄罗斯联邦安全会议负责总体战略协调，联邦安全局（FSB）承担信息空间和关键信息基础设施保护职能，内务部（MVD）负责打击网络犯罪，而数字发展、通信和大众传媒部则在数字治理和数字化转型过程中统筹落实安全要求。[8]

制度性机制中的重要组成部分是**跨部门协调体系**，该体系通过信息共享、联合研判和协同行动，实现对网络安全事件的快速响应和预防性措施的制定。相关机制主要通过跨部门工作组以及专业化的监测与应急响应中心加以落实，从而有效提升国家网络安全体系的整体韧性，并缩短对网络安全事件的处置时间。[12]

在国家政策层面，俄罗斯高度重视**政府与私营部门之间的协作**，尤其是与关键信息基础设施运营方、金融机构以及信息技术企业的合作。鉴于大量关键数字资源由私营主体负责运营与维护，国家—私营部门伙伴关系被官方视为提高网络安全防护能力和应对复杂网络威胁的必要条件。

(三) 俄罗斯在网络安全领域的国际合作

国际合作是俄罗斯联邦网络安全国家政策的重要方向之一，这主要源于网络威胁所具有的**跨国性特征**以及仅依靠国家层面手段难以实现有效应对的现实。俄罗斯始终主张在网络空间建立普遍适用的国际法律规范，并积极参与联合国框架下关于网络安全问题的讨论与磋商。具体而言，俄罗斯参与了政府专家组（GGE）和开放式工作组（OEWG）的相关工作，在这些多边机制中推动以国家主权原则、反对将信息通信技术用于进攻性目的以及防止网络冲突为核心的治理理念。[13]

多边合作的重要成果之一，是**联合国于 2024 年通过的《防止将信息通信技术用于犯罪目的的公约》**。该公约在制定过程中得到了俄罗斯联邦的积极参与，其主要目标在于协调各国在打击网络犯罪方面的国家政策，完善司法协助、引渡和信息交换机制，体现了国际合作在网络安全领域的务实取向和制度化发展。

在区域层面，俄罗斯高度重视在上海合作组织（上合组织）框架内开展网络安全合作。上合组织成员国在国际信息安全领域形成了较为一致的政策立场，通过开展网络威胁信息共享、联合磋商以及在国际组织中的立场协调，共同推进区域网络安全治理。其中，《上合组织成员国关于国际信息安全领域合作的协定》为成员国在打击网络犯罪和保护关键信息基础设施方面的合作提供了制度基础。

在金砖国家（BRICS）机制下，网络安全合作主要通过主管部门与专家层面的对话机制加以推进。合作重点集中于巩固数字主权、交流数字经济治理经验以及在全球网络空间治理问题上的政策协调。金砖国家发表的联合声明多次强调，应推动建立公正、非歧视性的国际信息通信技术治理体系。

此外，俄罗斯还积极发展**双边层面的信息安全合作**。例如，俄罗斯联邦与伊朗伊斯兰共和国于 2024 年生效的信息安全合作协定，明确了在关键信息基础设施保护、经验交流以及网络威胁应对法律框架协调等方面的合作方向。此类双边协议有助于在实践中探索具体合作机制，并增强国家间在网络安全领域的互信。

四、 俄罗斯网络安全保障面临的问题与发展前景

(一) 国家政策面临的主要挑战与制约因素

尽管俄罗斯联邦已逐步建立起较为完善的网络安全规范性法律体系和制度性保障机制，但该领域的国家政策在实践中仍面临一系列显著挑战。其中，最为关键的制约因素之一是**数字技术发展速度明显快于法律规制与政策工具的更新速度**，这在一定程度上限制了立法和治理体系对新型网络威胁的及时响应能力。尤其是在多阶段复杂网络攻击以及自动化攻击工具不断普及的背景下，现有法律与监管机制难以及时覆盖不断演变的威胁形态。

另一个突出的结构性问题是**对外国软硬件技术的依赖程度较高**，特别是在微电子、通信设备和基础软件等关键领域。在制裁压力持续存在的条件下，这种技术依赖显著增加了关键信息基础设施的脆弱性，并对数字主权政策的有效实施构成现实挑战。这一问题已在多项网络安全领域的法律研究与政策分析报告中得到反复强调。

此外，**网络安全专业人才短缺**也是制约国家网络安全能力提升的重要因素。专家普遍指出，网络安全领域对高技能人才的需求持续增长，而公共部门在薪酬与发展空间方面与私营部门存在竞争劣势，加之人才培养体系仍有待完善，这在一定程度上削弱了国家网络安全事件响应体系的整体稳定性和持续运行能力。

最后，**国际合作受限**同样构成不可忽视的挑战。受地缘政治紧张局势和国家间信任不足的影响，网络安全领域的国际协作面临现实障碍。当前尚缺乏统一、有效的国际法律机制来规范网络犯罪调查和涉案人员引渡问题，这使得跨国网络威胁的防范与打击难度显著上升。

(二) 非传统安全威胁背景下网络安全发展的前景

在非传统安全威胁持续上升的背景下，俄罗斯联邦将网络安全视为一项综合性、跨部门的治理议题，不再局限于技术层面，而是纳入政治、经济和社会治理体系之中。这一取向已在《俄罗斯联邦国家安全战略》（2021 年）和《俄罗斯联邦国际信息安全领域国家政策基本原则》中得到明确体现。

进一步发展的关键方向之一，是通过推动本土数字技术与软件产业发展来**巩固数字主权**。在多项官方政策文件与国家发展规划中，信息通信技术领域的进口替代被确立为战略重点。具体措施包括：研发和推广国产操作系统、数据库管理系统、信息加密与密码防护工具，以及建设本国的数据中心和通信基础设施。这些举措旨在降低对外国数字平台的依赖程度，提升关键信息基础设施抵御外部冲击的能力。[6], [15]

人工智能与大数据技术在网络安全体系中的应用被视为重要发展方向，已广泛用于网络监测、异常识别、攻击预警和应急响应自动化，在应对隐蔽性强、传播迅

速的非传统网络威胁方面具有现实意义。同时，鉴于大量网络事件源于人为因素，俄罗斯联邦正通过教育和宣传措施提升公众与组织的网络安全素养，以预防网络威胁并增强国家整体韧性。

(三) 俄罗斯经验对全球网络安全治理的意义

俄罗斯在网络安全保障方面的实践经验，对全球网络空间治理具有重要参考价值，尤其体现在**数字主权理念**以及**国家在安全保障中发挥主导作用**的治理路径上。俄罗斯联邦的官方战略文件明确指出，信息通信技术不应被用于削弱国家主权和破坏国内稳定。俄罗斯一贯主张制定国家在信息空间中的国际法律行为规范，并强调防止利用信息通信技术引发冲突。这一立场在《俄罗斯联邦国际信息安全领域国家政策基本原则》以及俄罗斯在多边国际场合发布的政策立场文件中得到了充分体现。

在多边层面，俄罗斯积极参与**联合国框架下的网络安全治理进程**，其中尤以其在政府专家组（GGE）和开放式工作组（OEWG）中的作用最为突出。俄罗斯在上述机制中持续推动建立具有普遍适用性和法律约束力的国家负责任行为规则。具有重要现实意义的成果是，**联合国于 2024 年通过了《防止将信息通信技术用于犯罪目的的公约》**，该公约的制定过程得到了俄罗斯的积极参与。该文件旨在加强国际合作、协调各国法律立场，并提升全球范围内打击网络犯罪的整体效能。

俄罗斯在全球网络安全治理中的立场，突出强调**反对网络空间军事化**、坚持信息通信技术的和平利用以及尊重国家主权原则。这一治理理念在一定程度上有别于以军事威慑为核心的网络安全观，有助于推动形成更加稳定、可预期的国际网络安全环境。

此外，俄罗斯的实践经验还表明，**综合性网络安全治理模式**具有重要现实意义。该模式通过结合法律规制、制度性保障、政府与私营部门合作以及国际协作，构建多层次的安全治理体系。在当前全球尚未形成统一网络安全治理模式的背景下，这种综合路径可被视为构建更加稳健、包容的国际信息安全体系的一种可行方案，并能够在一定程度上兼顾不同数字发展水平国家的利益关切。

结论

在全球数字化不断深化和非传统安全威胁持续演变的背景下，网络安全已成为国家安全体系中的重要组成部分。本文基于非传统安全视角，对网络安全的理论内涵、现实威胁及俄罗斯联邦在该领域的国家政策进行了系统分析。

研究表明，网络安全具有跨国性、复杂性和高度动态等非传统安全威胁特征，其影响超越传统军事安全范畴，并对政治、经济和社会稳定产生综合性影响。随着信息通信技术在国家治理和经济运行中的广泛应用，网络空间已成为国家安全不可或缺的领域，相关风险呈现出系统化特征。

分析显示，俄罗斯当前面临的主要网络威胁包括关键信息基础设施攻击、信息安全与网络影响以及数据安全与数字主权问题。为应对上述挑战，俄罗斯逐步构建起以战略文件、法律规范和制度机制为基础的网络安全治理体系，强调保护关键信息基础设施、巩固数字主权并加强国际合作。

同时，俄罗斯网络安全政策在实践中仍面临法律规制滞后、技术依赖和专业人才不足等限制因素。为提升国家网络安全韧性，俄罗斯正在推进综合性治理路径，通过发展本土数字技术、引入人工智能手段以及提升社会网络安全素养等方式，加强对非传统网络威胁的应对能力。

从全球层面看，俄罗斯在网络安全领域所倡导的数字主权理念和多边治理路径，为当前国际网络空间治理提供了有益参考。在全球网络安全治理体系尚不完善的背景下，其经验有助于推动更加稳定和包容的国际网络安全合作机制。

参考文献

[1]余民才：《非传统安全论》，世界知识出版社，2011 年。

[2]阎学通：《国际安全导论》，北京大学出版社，2017 年。

[3]王逸舟：《全球政治中的非传统安全问题》，世界知识出版社，2014 年。

[4]李少军：《非传统安全威胁与国家安全观转型》，《国际问题研究》，2016 年第 2 期。

[5]张建华:《网络安全视角下的非传统安全问题研究》,《国际安全研究》,2020 年第 4 期。

[6]刘建飞：《数字主权与国家安全》，《现代国际关系》，2021 年第 6 期。

[7] Указ Президента РФ：*《Стратегия национальной безопасности Российской Федерации》*，2021。

[8] Президент РФ：*《Доктрина информационной безопасности Российской Федерации》*，2016。

[9] Президент РФ：*《Основы государственной политики РФ в области международной информационной безопасности》*，2021。

[10] Nye J. S. *Cyber Power.* Harvard Kennedy School, 2010.

[11] Dunn Cavelty M. *Cyber-Security and Threat Politics*. Routledge, 2008.

[12] Kello L. *The Virtual Weapon and International Order*. Yale University Press, 2017.

[13] United Nations. *Developments in the field of ICTs in international security.*

[14] United Nations General Assembly. *Convention on Countering the Use of ICTs for Criminal Purposes.*

[15] Shanghai Cooperation Organization. *Agreement on Cooperation in International Information Security.*

[16] International Telecommunication Union. *Global Cybersecurity Index*.

[17] Kaspersky Lab. *Cyber Threats and Critical Infrastructure*.

[18] F6 Company. 网络攻击趋势分析报告.