我国网络空间安全治理政策过程研究

胡灿仲

广东南方通信建设有限公司，广东广州，510630

摘　要：互联网的飞速发展催生出网络意识形态的新样态，网络已成为各种意识形态交锋的新战场，网络意识形态安全是总体国家安全观的重要组成部分。在日益严峻的网络安全威胁态势下，维护国家网络空间安全的人才需求十分旺盛。世界各国从政策、管理、投入、演习、人才、技术等方面发力，全力推动网络安全产业发展。在实际的工作之中相关单位和人员必须跳出传统的思维方式，以当前的技术和人才作为基础，积极地进行网络空间安全防护体系的建设，从而才能为我国经济社会的进一步发展形成条件。

关键词：网络空间安全；挑战；治理措施

中图分类号：TP393.08　　**文献标志码：**A

0　引言

网络空间的安全风险泛化叠加，网络空间的和平与安全是非常重要的工作。与此同时，国家和地区间的“数字鸿沟”不断拉大，数字空间正在成为大国竞争和抢占国际话语权的新高地，不同国家、地区间的发展更加不平衡，数字经济的红利未能有效惠及各国人民。面对网络空间发展治理的新形势新挑战新威胁，国际社会必须携手合作，共商共治，为网络空间治理提供更加公正、合理、有效的解决方案[1]。

1　网络空间安全体系

以“四横八纵”网络空间安全层次模型为例，在该模型之中对网络空间安全体系进行了层次划分，认为当代的网络空间安全体系建设可以从设备层、系统层、数据层和应用层四个层次来进行具体着手，在相应的安全层次之中，均存在差异化的网络安全问题，要实现对网络空间安全的有效保障，就需要从这些层次的安全问题入手从而达到保障目标。同时网络空间安全的研究领域按照不同的安全需求，又可以划分为网络信息安全、信息保密、信息对抗、云安全、大数据安全、物联网安全、移动安全和可信计算等方面。除此之外，也有研究者提出，在网络空间安全体系的四个层次基础上，形成贯穿全部安全层次的安全体系模型是进行当代我国网络空间安全体系建设的方向。依托这一模型，在进行网络空间安全体系建设的过程中，通过对设备指纹、硬件身份认证、云计算等环境的建设，将能够极大地提升网络空间的安全性。除了对上述理论模型进行建设，以推进网络空间安全体系建设之外，对人才的培养也是当代我国网络空间安全体系建设的关键内容。由于网络空间安全体系建设所涉及的学科较多，涵盖数学、计算机、信息通信、物理等多个学科的内容，因此在进行人才培养的阶段也需要对当代我国的相关教学的学科进行科学合理的设置，从而为后续的网络空间安全体系建设输送充足的人才。通过对相关理论和研究方向的分析可以发现，当前我国的网络空间安全面对的主要问题是云安全、隐私保护、数据可信、安全防护、内容安全、信息隐藏和大数据安全等。而为实现对这些安全问题的有效解决，必须从网络空间的物理层面、信息传输层面和软件应用层面进行相应的安全保障。同时为了确保我国网络空间安全体系建设的持续性推进，需要从多个学科的人才培养入手，确保相关人才具有较强的网络空间安全意识、形成过硬的专业技术能力。

2 网络空间安全面临的挑战

2.1 网络风险理解偏差

考虑到数字经济快速发展的性质，网络安全风险在某种程度上是一种具有新的复杂性的风险，而这种复杂性本身尚未得到充分理解。比如，我们缺乏足够的历史数据和对重大潜在事件的系统性风险的清晰认知。缺乏足够历史数据是详细了解网络风险基本方面的主要障碍。在可用性数据有限的情况下，建立足够的模型以确保风险管理的准确性是一项挑战。尤其对于再保险公司来说，这代表着巨大的承保风险。而从另一个角度来说，缺乏适当的网络安全风险的再保险覆盖又是保险公司的主要担忧。两个互为因果的困难成了网络安全保险发展的障碍。重大潜在事件的系统性和相关性是另一个重要外部挑战，这使得我们很难理解整个市场的规模和累积风险。从保险的角度来看，或有业务中断的处理和潜在的风险聚合是一个很值得关注的问题。网络攻击相关性的增加以及IT服务（例如云服务）的单一化，将使市场很难正确量化从而难以对这种风险提供保障。其主要担忧在于由市场标准、累积风险控制和评估工具而导致的累积风险估值错误[2]。

2.2 网络安全治理难度大

首先，新一轮信息技术革命与人类经济社会活动日益交融，安全风险无处不在。尤其是我国网络基础设施有待完善，网络基数较为庞大，危害社会秩序和个人权利的安全问题更为突出。2015年国务院发布的《关于促进大数据发展的行动纲要》，首次将信息化发展上升到了国家信息化发展的战略全局高度。随着社会信息化进程加快，过度强化信息化发展程度，超越了安全和自由保障的限度。其次，在社会信息化高速发展的同时，网络安全威胁和风险日益突出，并向政治、经济、文化、社会、生态等领域渗透，网络安全已经成为国家安全的重要组成部分。网络不良信息败坏社会文明风尚，网络恐怖主义破坏社会和谐，网络暴力影响公民自由和权利的实现。合理的网络安全标准既有利于促进信息化技术发展，又有助于保障国家利益和人民的基本权利。正确的网络安全与信息化发展理念，应该抛弃极端的发展观与绝对的安全观，促进经济社会信息化健康有序发展。

2.3 主流意识形态需要维护

信息时代人人都是自媒体，人人都是麦克风。网络信息传播迅速又海量，互联网对网民身份特征的隐匿，对信息内容的非限制往往会刺激网民发布一些未经证实的消息，从而造成虚假信息满天飞，掩盖了事实与真相。特别是有些拥有大量粉丝的网络大V、意见领袖和网络主播，他们为了“挣流量”，利用网民盲目从众的心理，蓄意夸大社会事件，炒作网络热点，制造和传播网络谣言，导致社会恐慌。甚至有些所谓的公知和网络人物，以“学术争鸣”为掩护，煽动一些不明真相的群众参与意识形态的讨论，恶化了网络空间的政治生态。这些谣言的不断发酵和放大，增加了舆情管控的难度，容易引发群体性事件，同时也易降低人们对主流意识形态的认同，需要采取有效措施维护网络空间安全及主流意识形态。

3 网络空间安全治理有效措施

3.1 规范网络法律法规

运用好法律杠杆，控制好网络自由与法律秩序之间的张力，既允许网民在合法的范围内畅所欲言，又严格落实网络管控的法规制度。同时对各种违反网络安全的行为依法严肃处理，特别是对公然挑战主流意识形态地位、煽动网络舆情事件、激化社会矛盾的个别言行要重点打击，严惩不贷。近期国家及时亮剑、重拳出击，依法整顿和查封了一大批违法网站、公众号，及时清理了大量虚假、淫秽、反动网络信息，严厉惩处一些违背原则、影响恶劣的网络“大V”。这些措施极大地彰显了我国依法治网管网的决心，既净化了网络空间，强化了治理能力，维护了法律的权威性和公正性，同时又保障了普通网民的话语权，捍卫了主流意识形态的核心地位，有效震慑了危害中国意识形态安全、诋毁社会主义制度的西方敌对势力[3]。

3.2 威胁及保障技术

从实际情况来看，应用层的安全威胁主要集中在操作系统、应用软件和工业控制系统等层面。首先，操作系统是保障相应的计算机系统正常使用的关键，要保障操作系统安全主要需要从相应的安全系统开发技术和操作系统安全增强机制建设两个方面入手。相对操作系统而言，应用软件具有更强的丰富性，其所面对的安全问题也更为多样，在以往的生产生活之中，各类计算机病毒是导致计算机软件产生安全问题的重要原因，针对这种现象，充分地应用恶意代码检测、软件检测与安全评估等方法可以在一定程度上对潜在的安全漏洞进行把握，并有针对性地对当前存在的安全漏洞进行修补，有鉴于此，在后续的网络安全体系建设过程中也需要加大对这些技术的应用力度。此外，工业控制系统的安全也是当前网络安全体系建设中的重点内容，当前的工业控制系统面对着计算机病毒等的威胁，影响到实际的工业生产。针对这一系列现象，采取远程访问控制技术、漏洞管理技术和异常检测技术等，可以强化对工业控制系统的安全防护，达到保障其安全的目的。

3.3 完善国家总体统筹协调机制

当下网络空间的内涵和外延随着技术创新的加速仍然在不断扩展，特别是元宇宙概念的横空出世更是向世界展示了数字技术融合创新的广泛应用前景，这也意味着构建网络空间命运共同体需要统筹协调国内更广泛的力量和资源。与其他领域相比，网络空间治理本就具有多主体、多领域、多维度的特征，构建网络空间命运共同体不仅需要统筹政府各部门的力量和资源，还需要推动政府部门与产业界、学术界及其他民间机构的多向交流，特别是来自产业界的技术、资金、人才和商业模式的创新推动。此外，构建网络空间命运共同体的发力点众多，基本覆盖科技、政治、经济、军事、社会等各层次各领域，加强国家总体统筹协调，还有助于在顶层设计上实现各方资源的有效合理配置，集中力量解决构建过程中出现的主要问题和主要矛盾，在网络空间的快速发展变化中把握全局，在世界百年未有之大变局中开新局，在世界乱局中化危为机，让和平、安全、开放、合作、有序的网络空间成为推动构建人类命运共同体的重要实践。

3.4 建设国际网络空间治理格局

网络空间具有主权边界，网络空间治理体现的是国家意志和人民利益，过度开放网络空间容易引发国家安全问题。在网络安全治理国际合作的过程中，应该注意网络开放的边界，坚持国家安全不容动摇和人民利益不可侵犯的基础上，有序推动网络空间合作治理。共建网络空间国际规则是推进网络空间国际合作共治的根本保障。网络空间超越物理空间的虚拟性与扩张地域范围的跨国性，对属地管辖原则构成严重冲击，导致传统的国内规则体系无法有效应对国际网络安全问题。国际网络合作治理的重要条件是遵循相同的话语体系和规则体系，才能有效协调多边治理分歧，共同遏制网络恐怖主义、打击新型网络犯罪、反对信息技术滥用、加强公民权益保护，共同维护网络空间和平安全。由于各国的核心价值准则和网络文化差异，网络空间治理领域的法律规制方式存在分歧，导致国际合作治理的法治壁垒。为此，应该秉持价值多元理念，将网络安全与发展作为互利共赢的治理目标，推动制定全球互联网共治规则，形成共识性的国际网络空间秩序。具体而言，在尊重各国法治秩序的基础上，协调国际网络安全治理规则的冲突，维护以国际法为基础的网络空间治理国际秩序，构建完备良善的国际网络空间治理规则体系[4]。

3.5 信息传输保障

信息的传输是连接网络空间物理层和应用层的中间环节，在该环节之中存在多种传输模式包括有线、无线和演进中的网络体系等，这些网络体系形成的根本目标在于对信息进行有效传输并保障其安全。在推进信息传输安全的过程中，首先需要注重的是当前网络自身的安全，通过针对不同的信息传输需求进行相应的信息传输安全协议设计，将能够有效地保障网络自身的安全。从当前的信息传输技术发展之中可以看出，诸如工业控制网络、5G网络和SDN网络等

的出现，相对于以往能够更好地对信息传输网络本身的安全形成保障。其次，信息传输过程中访问控制也是确保信息传输安全的重要技术手段。访问控制是用户在对信息资源进行访问的阶段，对用户的身份进行验证的一种方式，通过有效地验证用户的身份，并对访问行为进行授权，将能够避免恶意访问对信息造成的威胁。目前在信息访问控制方面已经形成了包括DAC、MAC、RBAC 等一系列技术，相关的技术在应用阶段可以针对不同的访问需求进行验证与授权。随着当前云计算技术的进一步发展，新的访问控制需求也随之产生，并形成了新的访问控制方案。

3.6 建设双重认证机制

在接入认证方面，可以对核心区、公共区的公共基础设施按照顶级、行业级和区域级进行设计；在访问控制方面，考虑与区块链及边缘计算技术的结合，通过敏感标记的优化设计综合考虑分级管理的访问权限与城市规划单元中的功能区-街区-地块相结合的组合应用，设置3+3的管理控制和功能控制双重认证机制。在访问控制管理方面，建议核心区设施由国家指定的业务部门或授权机构执行审核，即国家网络安全的中心管理节点；公共区由相应的行业主管部门或授权机构执行审核，即对应的行业管理节点（如电力、电信管理部门等），管理节点可以进一步采用联盟链的形式进行建设。在访问应用服务时则通过识别敏感标记中的权限定义信息，将对应区内设施纳入到区域级的功能节点进行管理，提高管理效率。进一步，可以将网络空间公共基础设施的访问用户按照相应的控制等级及标记要求进行分类对应。例如，核心区关键基础设施的认证对应顶级访问控制节点，其服务对应用户敏感标记中相适应的功能节点。公共区基础设施的管理对应行业控制节点及相应的功能节点，开放区对应区域自主访问控制节点，用户的高、中、低级也可分别与之对应，或者根据实际需求进行更细化的分类。

3.7 构建协同联动机制

党委作为统筹全局的领导核心，要肩负起政治责任，把握正确的政治方向。政府要坚持“一元主导、多元共治”的治理原则，以扁平化的管理手段突破传统的行政科层限制，发展与其他治理主体的平等合作关系，完善组织架构，明确权责义务，厘清治理目标，推动网络安全治理方式由命令向协商，由指挥向引导，由管治向疏导转变，形成多元协同共治、部门上下联动、运转高速有效、保障全面有力的科学治理机制。同时政府要承担网络安全管理的主要职责，构建网络意识形态安全的多元共治机制[5]。

4 结语

网络空间也受到来自各个方面的安全威胁，在一定程度上阻碍了社会发展，针对这种情况，我国的发展过程中需要提高对网络空间安全的重视程度，形成统筹网络空间安全体系建设，积极面对网络空间安全挑战的全局眼光，依托在技术上的不断创新和人才培养的关注，实现完善网络空间安全体系建设的目的。

参考文献

[1] 范玉吉,张潇.网络空间命运共同体理念与网络空间治理[J].西南政法大学学报,2020,22(3):105-116.

[2] 吴世娟.网络空间治理现代化:意义、阻滞与推进途径[J].南京理工大学学报(社会科学版),2020,33(3):38-43.

[3] 杜爽.新时代网络空间意识形态安全问题研究[D].沈阳建筑大学,2020.

[4] 张坯.网络空间全球治理机制的中国方案研究[D].湖南师范大学,2020.

[5] 张治远.量子时代的网络安全挑战及其应对研究[J].IT经理世界,2020,23(4):180.