数字国土与泛在边疆：俄乌冲突背景下主权互联网的效果与影响*

杨安卓　吴玉茗

[**内容摘要**] 自互联网诞生以来，关于互联网主权的争论就一直是学术界的焦点。经过网络例外论及网络自由者、多利益相关者治理模式的争论和变迁，如今互联网主权的建设已是大势所趋。面对美国网络安全战略的霸权威胁，各民族国家陆续通过制定相关法律法规、建设相关基础设施等来阐明捍卫网络主权、对抗网络霸权的决心，形成了民族国家以互联网主权对抗数字帝国主义霸权的世界格局。同时，互联网主权战略的效果与影响也于2022年2月底爆发的俄乌冲突中得到了战时检验。

[**关键词**] 俄罗斯“主权互联网法”；互联网主权；独立互联网；网络空间治理

于2022年2月底爆发的俄乌冲突当前呈现持久化趋势，其在人类历史上的重要地位已经受到了学术界的广泛关注，被国外学者称为“第一次混合战争、第一场真正意义上的网络时代的战争以及未来战争的一次全景式呈现”[①]。在全球性网络治理完美规则缺失的现实背景下，俄乌冲突更是一次极具研究和借鉴价值的网络战争极限测试。

俄乌冲突爆发以来，随着美国隐藏在多边主义中的数字帝国主义面目一一显现，西方国家多个互联网公司纷纷踏破“网络无国界”的理念，宣布对俄罗斯进行全方位、多维度的大规模网络制裁行动，对俄罗斯发起了全面制裁行动。美西方国家肆意地推进网络霸权行动，导致俄罗斯面临“断网”的威胁。而俄罗斯于战前进行的互联网主权建设为其在关键时刻保证本国网络正常运转、大幅降低美欧对俄罗斯网络空间的威慑和断网威胁具有重大战略意义。[②]这场混合式大战不仅揭示了俄罗斯本身互联网主权建设的意义和效果、印证了民族国家互联网主权建设的必要性，更为我们展示了民族国家以数字主权对抗数字帝国主义网络霸权的世界格局。

早在1997年，弗雷德里克·杜泽特就在一篇题为《互联网地缘政治化世界》的文章中宣布：“互联网未能缓和地缘政治冲突，相反，互联网似乎使它们倍增和复杂化。”[③]随着全球数字经济的发展，与地理边界和主权终结的乐观声音浪潮相反，我们已然看到了全球信息和通信系统所扩张的地缘政治问题：数据流动在赋予全球经济新增长动能、推动现代社会发展的同时导

* 本文系国家社科基金重大项目“数字社会的法律治理体系与立法变革研究”（项目编号：20&ZD178）的阶段性研究成果。

① Ujang Priyono, “Cyber Warfare as Part of Russia and Ukraine Conflict”, *Jurnal Diplomasi Pertahanan*, 2022, Vol.8, No.2, pp.44−59.

② 颉靖、王斌：《从俄乌冲突看俄罗斯“断网”演习的意义》，《中国信息安全》2022年第6期。

③ Frédérick Douzet, “La géopolitique pour comprendre lecyberespace”, *Hérodote*, 2014, Vol.152−153, No.1−2, pp.3−21.

致了严峻的领土紧张局势。众多国家之间在互联网控制和监管方面的压力激增，与网络犯罪相关的新威胁出现，在政治冲突、军事战斗、经济战、情报战、外交战等背景下使用计算机网络的紧张局势正在加剧。棱镜门事件以及互联网技术在“颜色革命”中显现的种种突出作用，使主权国家不可避免地产生了对个人隐私、国家安全和经济前景的风险担忧，数字主权的概念也已逐渐成为政治话语体系中又一个强有力的术语。这些都证明了互联网主权存在的必然性，迫使主要国家和地区在数字领域加速布局技术和法律工具等政府干预和监管措施。

自 2014 年乌克兰危机以来，美俄两国在世界经济、军事领域上的长期对峙逐渐扩大延伸至网络空间。[①] 在当今全球互联网基础设施领域和国际网络数字经济领域，俄罗斯正面临着严重的经济损失威胁和国家安全威胁的双重考验。基于此，俄罗斯国家领导层对于进一步推行俄罗斯“主权互联网法”展现出了坚定的决心。该法案作为俄罗斯在信息科技发展领域的立法及实践的重要政策性延续，体现了俄罗斯政府对国家网络技术安全保障乃至国家安全保障方面的前瞻性战略布局。该法案公布三年来，俄积极推动主权互联网的建设，其成效已在现阶段的俄乌冲突中得到初步显现。此外，中俄两国互联网治理上有众多相似理念，都较早在国际社会中提出了“互联网主权”概念。中国提出的构建网络空间命运共同体的倡议也得到了俄方政治领导人和互联网企业巨头们的高度认同。[②] 因此，研究俄罗斯“主权互联网法”出台的背景内容以及其在俄乌冲突中产生的影响与作用，对我国互联网主权建设具有现实意义。

一、美国网络安全战略下的霸权威胁

享有军事技术重大前沿创新成果的国家往往会向该领域持续性地倾注资源，以期将暂时性的先发优势转化为长久性的领先优势。美国作为高度依赖互联网的网络开创者与互联网全球化的推动者，互联网的发展在给其带来发展与繁荣的同时，也使该国面临着网络安全方面的威胁。

美国国家安全界率先将网络空间作为一个新兴战略领域进行长期探索，陆续制定推行了系统化的网络战略体系规划设计及战略部署，以切实强化网络空间主导权意识和自身整体网络技术安全发展能力。例如，自克林顿政府将网络安全定位为国家安全战略，小布什政府以反恐为核心推进“安全优先”的网络空间发展战略，到奥巴马时期提出的用美国软实力强化塑造美国网络空间规则，以谋求全球网络空间霸权地位等一系列阶段战略。[③]

随着全球网络空间与现代国际体系之间的关系愈加深入紧密，特朗普就任总统后面临更复杂的网络形势。[④]2016 年，美国大选进程遭受来自外部的网络干扰，其政治体制根基被动摇；美国国家安全局开发出的漏洞利用程序“永恒之蓝”遭到数据泄露而引发全球性电脑病毒“wannacry”，造成世界各地大约 150 个国家，超过 230 000 台计算机系统受到灾难性影响。[⑤] 种种网络安全大事件表明网络空间已经成为全球大国军事相互竞争、地缘政治对抗的重点新技术

① 官晓萌：《俄罗斯网络安全领域最新法律分析》，《情报杂志》2019 年第 11 期。

② 陈春彦：《试析〈俄罗斯互联网主权法〉的背景与影响》，《传媒》2020 年第 24 期。

③ 耿贵宁、张格莹、刘丽：《美欧俄网络安全战略与政策发展趋势研究》，《网络安全技术与应用》2021 年第 10 期。

④ 汪晓风：《“美国优先”与特朗普政府网络战略的重构》，《复旦学报》（社会科学版）2019 年第 4 期。

⑤ 王顺业：《美国网络安全战略的演变与启示》，《江西警察学院学报》2019 年第 5 期。

领域，各国军方已经将强化网络空间作战防御能力问题当作未来国际军力发展方向的研究重点。

在此背景下，美国在 2018 年 9 月公布了渗透着网络霸权主义的新《国家网络安全战略》。这是自从 2003 年小布什政府《保护网络空间国家战略》推出 15 年以来，美国再次推出的国家网络战略。[①] 该战略以 2017 年美国《国家安全战略》为基础，阐明了特朗普政府在互联网治理和网络安全方面的立场。“战略”中包含指责伊朗、俄罗斯、朝鲜等国家发动黑客攻击带给美国及其盟友重大损失的内容，并明确宣称了“以武维和”的行为准则。[②]

该《国家网络安全战略》虽然并没有指明可对俄罗斯实施“断网”，但仍具有突出的“侵略特性”，如其明确指出“利用网络空间实施攻击”的措施可轻易成为美国针对不友好国家实施制裁的措施。[③] 此外，自 2016 年“黑客门”事件发生以来，美国财政部以涉嫌网络攻击为理由，对不同的个人或公司进行了数轮经济制裁，严重阻碍了俄罗斯网络信息行业的发展。此类被美国“经常”且“无证据”地指控为“黑客攻击发起者”的事实，大大刺激了俄罗斯立法者和执政者不惜牺牲普京总统的支持率，在《宪法》修订即将公投之前批准了俄罗斯“主权互联网法”。相关立法者认为，面对美国新的“更富进攻性的网络安全立场”，俄罗斯“必须采取措施保证俄罗斯互联网的长期稳定与安全，提高俄罗斯互联网资源的运行可靠性”。[④]

二、俄罗斯“主权互联网法案”的独立宣言

2019 年 5 月 1 日，俄罗斯总统普京签署了《关于对俄罗斯联邦〈通信法〉〈信息、信息技术和信息保护法〉进行修订的第 90 号联邦法案》（以下简称“《法案》”），即“主权互联网法案”，于 2019 年 11 月 1 日起正式生效。[⑤] 这标志着俄罗斯在网络空间主权维护和网络安全战略部署方面迈出了坚实的步伐。

“主权互联网法案”是俄罗斯在网络安全领域最著名的国家法案，但它本身并不是横空出世的。在此之前，随着俄罗斯学术界“信息主权”及“数字主权”理论探讨的逐步深入，俄罗斯国家立法机关便陆续将其理念融入更具体领域的地方立法与实践。2014 年，杜马就通过了第一部关于数据本地化的立法，要求运营商和平台将俄罗斯个人或法律实体的数据托管在俄罗斯联邦境内。两年后，以该倡议背后的参议员命名的所谓“Yarovaya 法”，要求平台必须将其用户的元数据存储三年，设置后门并传达其解密密钥，以方便安全部门的审查。此外，俄罗斯还陆续发布了大量与互联网发展与管理相关的法律，形成了以《俄罗斯联邦国家安全战略》（2015 年）为主，以新版《俄罗斯联邦信息安全学说》（2016 年）为辅助，以《俄罗斯信息社会发展战略》（2017 年）、《关键信息基础设施安全法》（2017 年）等为重要支撑因素的国家信息空间和安全区域治理法律体系，从而为 2019 年著名的“主权互联网法”的颁布奠定了法理基础。[⑥]

① 官晓萌：《俄罗斯网络安全领域最新法律分析》。

② 陈春彦：《俄罗斯互联网主权立法创新与启示》，《中国广播电视学刊》2021 年第 11 期。

③ 江欣欣：《2019 年俄罗斯信息网络安全建设综述》，《保密科学技术》2020 年第 6 期。

④ 转引自王智勇、刘杨钺：《“主权互联网法案”与俄罗斯网络主权实践》，《信息安全与通信保密》2020 年第 10 期。

⑤ 江欣欣、由鲜举：《俄罗斯“主权互联网”建设一年回顾》，《保密科学技术》第 2020 年第 8 期。

⑥ 陈春彦：《俄罗斯互联网主权立法创新与启示》。

俄罗斯的“主权互联网法”共三章，分别为对《通信法》的相关重点修订的条款、对《信息、信息技术和信息保护法》的相关重点修订的条款，以及上述不同内容修订的条款的具体生效时间。[①] 俄罗斯在“主权互联网法”中的概念是基于其对互联网安全的方法，将互联网安全比作信息安全，把国家对信息流的控制放在首位。其在“主权互联网法”中对数字主权的理解主要包括对数据的控制（以内容过滤和数据本地化的形式）、对基础设施的控制（国家软件保护主义和监控互联网流量的中央设备系统），以促进俄罗斯互联网治理的两大方面举措，达成安全、自主、稳定的要旨，加强俄罗斯联邦境内信息通信网的安全建设。让俄罗斯拥有一个独立于国际互联网的信息基础设施——“Runet”（俄罗斯互联网），确保俄罗斯通信运营商可以在无法接入国外互联网根服务器的情况下，依然能够保证其境内的网络系统可以安全、稳定、完整地运行，维护俄罗斯在信息空间领域的国家利益。[②]

“主权互联网法”颁布后，俄积极推进主权互联网建设，加强大型断网演习。据俄新社莫斯科 2019 年 12 月 23 日电，俄联邦数字发展、通信和大众传媒部副部长阿列克谢·索科洛夫于当日傍晚向国内外媒体宣布，23 日在全俄进行了确保俄罗斯国内互联网基础设施有效运行的首次演习，演习在莫斯科、弗拉基米尔、罗斯托夫等几个城市顺利举行。测试场景包括通信稳定性、手机安全、个人数据保护、信息拦截和网络安全等。结果表明，俄罗斯不需要访问全球 DNS（服务器）系统就能成功链接国内网。[③]

综上所述，俄罗斯主张并强化了互联网主权的概念，并通过立法活动与关键信息基础设施的建设，加强对互联网主权的捍卫，以保障本国互联网和数据的自主可控，减少对境外网络的依赖。但俄罗斯“主权互联网法”亦在其国内外产生了不小争议：在国际上，该法引起了全球网络安全领域的高度关注；在国内，其法案审议过程也引发了各方议论，被指为有损网络自由的“互联网巴尔干化”，标志着互联网时代早期的全球网络一体化空间梦想破灭，进入了一个“被主权壁垒分割”的“碎片化”时代。

此外，俄罗斯主权互联网的实践也面临种种问题。首先，俄罗斯的主权互联网在市场层面上面临难以克服的历史遗留问题。俄罗斯互联网的基础设施最初设计为高度分散的，获得对俄罗斯主权互联网的集中控制成为难题。而且俄持续到 2012 年的互联网监管自由化阶段塑造了该国较为固定的在线国际市场以及依赖国外平台的大众用户习惯，一定程度上在俄罗斯通向数字主权的道路上埋下了隐患。[④] 其次，国家集中规制的技术风险也被质疑。具体来讲，如果俄罗斯管理当局在集中统管时遭受网络入侵，就意味着攻击者可以直接获取并接管俄罗斯国内网络的最高权限，导致俄罗斯落入“牵一发而动全身”的极端被动局面。[⑤] 再次，国内互联网行业的运行模式改造过程中的腐败风险、过度管控、质量下降等潜在问题也都无法被忽视，甚至将延缓俄罗斯整体行业发展，进而造成一系列重大战略性失误。最后，在全球网络和政治经济多方交

① 王智勇、刘杨钺：《“主权互联网法案”与俄罗斯网络主权实践》。

② 王智勇、刘杨钺：《“主权互联网法案”与俄罗斯网络主权实践》。

③ 转引自刘建明：《俄罗斯的断网风波与未来网络战》，《新闻爱好者》2020 年第 3 期。

④ Anna Litvinenko, “Re-Defining Borders Online: Russia’s Strategic Narrative on Internet Sovereignty”, *Media and Communication*, 2021, Vol.9, No.4, pp.5−15.

⑤ 王智勇、刘杨钺：《“主权互联网法案”与俄罗斯网络主权实践》。

融、互联网技术日新月异的时代，怎样在提高封闭安全系数的同时保证长期使用也是一个难题。

国家需要适应新的环境条件，网络空间改变了世界的地缘政治格局已成为既定事实。俄罗斯作为网络主权的实践领头羊，其关于“主权互联网法”的理论争议和实际效果都在正在进行中的俄乌冲突中得到了更加真实又深入的检验。

三、欧盟与乌克兰的互联网主权建构

国际数据主权博弈日趋激烈，国际网络空间尚处丛林规则时代，在政治、经济等多重因素交叉影响下，数据主权安全风险更为多变与隐蔽，治理难度极大提升。[①] 面对美国强势扩张型的数字安全战略以及俄罗斯紧锣密鼓的互联网主权建设，各国也纷纷加快了互联网主权的建设。

欧盟在长期受制于美国的长臂管辖、市场数据红利被美国攫取、数字科技技术被美国垄断的严峻背景下，[②] 从 2019 年起便持续关注网络安全和数字主权的战略问题。欧盟认为，欧盟和欧洲利益相关者制定管理数字技术、规范数字技术公司的规则和标准的能力，对其战略自主、构建网络主权至关重要。欧盟倡导从保护机制和促进数字创新工具两个方面来维护数字主权。保护机制主要是针对个人隐私和数据安全的保护；数字创新工具是指为欧盟实现技术自主权而营造值得信赖的安全环境，制定促进公平竞争和监管的规则，推动科技投资和联合科研等。从欧盟推进“数字主权”的政策议程来看，欧盟的数字贸易主张与传统意义上的主权观密切相关，即高度重视数字化背景下的领土、居民、政府权力等问题，具体表现为跨境数据流动和数据本地化、公民隐私权保护、对数字行业的监管权。[③] 与此同时，欧盟在数字全球化和数字主权之间采取了均衡策略，这体现在欧盟决策者提出的“开放的战略自主权”这一概念上。欧盟不仅希望在全球舞台上制定自己的路线，借此领导和参与塑造世界，同时又要维护欧洲的利益和价值观的战略诉求，[④] 即欧盟希望建立一个具有公平竞争环境的开放市场，欢迎世界各地的公司参与其中，但是需要遵循符合欧洲价值观的数字规则。

与此同时，乌克兰面临着长期的大规模网络攻击，乌克兰的政府、银行系统、工业设施和私人企业遭受了重大的物质和声誉损失。在俄罗斯以网络战争辅助占领克里米亚以及踏入乌克兰顿巴斯后，建立有效的网络安全系统以捍卫互联网主权对乌克兰来说愈发紧迫。[⑤] 乌克兰政府逐步开始意识到网络安全作为国家安全组成部分的重要性，采取了建立乌克兰网络警察部门、制定国家网络安全战略、出台多项网络安全法规、加强国际合作、全面加强保护国内网络空间的公共防御等多重举措。

2017 年乌克兰首次发布信息安全战略，其中表示“乌克兰信息安全的主要威胁是作为侵略

① 黄海瑛、何梦婷、冉从敬：《数据主权安全风险的国际治理体系与我国路径研究》，《图书与情报》2021 年第 4 期。

② 卢英佳：《欧盟数字主权观在大国博弈背景下的实践及发展趋势》，《中国信息安全》2021 年第 8 期。

③ 肖宛晴、刘传平：《欧美数字主权与数字贸易政策比较分析》，《世界经济与政治论坛》2021 年第 6 期。

④ Bernd Beckert, “The European Way of Doing Artificial Intelligence: The State of Play Implementing Trustworthy AI”, in *2021 60th FITCE Communication Days Congress for ICT Professionals: Industrial Data — Cloud, Low Latency and Privacy (FITCE)*, Vienna, Austria, 2021, pp.1−8, doi: 10.1109/FITCE53297.2021.9588560.

⑤ Pavlo Katerynchuk, “Challenges for Ukraine’s Cyber Security: National Dimensions”, *Eastern Review*, 2019, Vol.8, pp.137−147.

者的俄罗斯和乌克兰应对信息攻击的脆弱性”[①]。截至 2020 年，乌克兰形成了保护网络安全、维护国家互联网主权的一系列法案体系——《乌克兰宪法》《乌克兰信息法》《乌克兰国家安全法》《乌克兰网络安全基本原则法》《保护信息和电信系统中的信息原则法》《电子信托服务法》《个人数据保护法》等，[②]以及乌克兰总统和政府签署的章程，包括《乌克兰国家安全战略》《乌克兰安全和国防部门的概念发展》《乌克兰的战略防御公报与国家网络安全协调中心》《国家网络安全的威胁以及应对措施》《关于批准建立国家关键基础设施保护体系的构想》等。[③]

此外，乌克兰高度重视网络安全领域的国际合作，在权力框架内与北约、欧盟等伙伴国家建立合作关系，共同执行网络安全任务，在公共生活的各个领域保护互联网主权。2021 年 6 月，在第一轮乌克兰–欧盟网络对话中，各方同意需要维护法治以确保全球开放、稳定和安全的网络空间，并就网络空间领域的体制结构和机构权力、制定立法举措的最新进展进行了交流。乌克兰和欧盟重申了《布达佩斯公约》（2001 年第 2824–IV 号法律）的重要性，推动完善国家立法，并在国际和区域范围内深化打击网络犯罪的国际合作。[④]此外，乌克兰总统泽连斯基宣布创建并启动网络安全和反虚假信息中心，该中心与欧盟、北约合作，以向其承诺实施发展网络安全和国防部门在网络空间行动的必要能力，并与联盟建立网络安全的互操作性合作中心。

四、网络主权建设在混合战争中的检验

虽然于 2022 年 2 月底爆发的俄乌冲突仍未结束，但是它对网络空间国际治理的深远影响已初步显现。战争是政治的延续，网络空间作为地缘政治博弈的工具，也成为冲突各方博弈的战场。作为发生在数字时代的混合战争，网络战和信息战的形态逐步清晰，特别是“硅谷军团”等高新科技企业作为非国家行为体的参战，使俄乌冲突中网络空间的对抗态势更趋复杂化。[⑤]在这一过程中，俄罗斯互联网主权的建设在混合战争中得到了前所未有的检验。

此次俄乌网络信息战有席卷全球之势，许多神秘黑客组织都参与其中。这场网络战争涉及不可逆数据擦除、断网攻击、僵尸漏洞等网络作战手段，甚至其开始的时间可能早于现实战场上的火力交锋。综合俄乌冲突期间国内外新闻报道和专家报告来看，俄罗斯在网络战战场上的主要战略包括对外进行网络攻击、对内以断网防御为底线，并成功捍卫了俄罗斯的互联网主权。

（一）对外进行网络攻击

2022 年 4 月 27 日，微软数字安全部门发布了一份报告，列举并分析了俄罗斯在俄乌冲突爆发前几个月对乌克兰发动的所有已知网络攻击。报告得出的结论是，俄罗斯军事情报局（GRU）、

① УКАЗ ПРЕЗИДЕНТА УКРАЇНИ, №47/2017, “Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України» ”, http://www.president.gov.ua/documents/472017-21374, retrieved May 10, 2023.

② Andrii Semenchenko, Valentyna Pleskach, Oleh Zaiarnyi and Mariia Pleskach, “Organizational and Legal Mechanisms of Cybersecurity and Cyber Defense in Ukraine: Essentiality, Conditions and Development Prospects”, *Problems in Programming* 2020, Vol.2, No.3, pp.278–286.

③ Pavlo Katerynchuk, “Challenges for Ukraine’s Cyber Security: National Dimensions”.

④ Roman Chernysh, Ruslan Prozorov, Yaroslav Tytarenko, Vitalii Matsiuk and Olexander Lebedev, “Legal and Organizational Aspects of Destructive Information Impact Counteracting: The Experience of Ukraine and the European Union”, *Amazonia Investiga*, 2022, Vol.11, Iss.54, pp.169–177.

⑤ 郎平：《从俄乌冲突看网络空间武器化倾向及其影响》，《中国信息安全》2022 年第 6 期。

外国情报局（SVR）和联邦安全局（FSB）联合攻击乌克兰海陆空军队以及网络信息空间，其目标是破坏或削弱乌克兰政府和军事职能，并破坏公众对这些机构的信任。

越来越多的乌克兰政府、军事和银行网站由于经常遭受大规模 DDoS 攻击和黑客入侵而处于瘫痪、高延迟和不时中断的状态。此外，俄罗斯对卫星互联网供应商 Viasat 的网络攻击导致整个乌克兰与其他国家（德国、法国、匈牙利、希腊、意大利和波兰）之间的通信大范围中断。微软还观察到俄罗斯特定军事行动与网络攻击之间的联系，如网络攻击在地理上集中在基辅和顿巴斯附近，并在俄罗斯占领乌克兰最大的扎波罗热核电站的同时针对乌克兰的核电公司。总之，在战时，俄罗斯的网络攻击更加频繁、更具破坏性，并且与军事行动相协调。[①]

但是，乌克兰对于俄罗斯的网络攻击早有准备，其于 2017 年便开始制定国家网络战略、备份关键数据和服务，以加强其网络安全并提高其网络的弹性，进而保护经济和政治统治的连续性。此外，乌克兰一直持续性得到北约、欧盟和全球情报机构的支持。2018 年，它从美国国务院获得 1 000 万美元用于保护关键基础设施，2020 年又获得 800 万美元，美国陆军和北约承诺再提供 300 万美元和网络援助。俄乌冲突爆发前夕，乌克兰请求并获得了欧盟网络快速反应小组的帮助，通过检测攻击何时发生来防御网络攻击。澳大利亚网络小组也被派来帮助乌克兰远程或现场防御俄罗斯支持发动的网络攻击，并为乌克兰官员提供网络安全培训。此外，“星链”为乌克兰提供了稳定持续的网络通信能力，为乌军在战时实现上下信息畅通、全军统一行动提供了科技保障，削弱了俄对乌克兰电力、通信等基础设施破坏行动的实际效果。尽管乌克兰在此次俄乌冲突期间受到沉重的网络攻击，但因持续性依靠欧美的网络技术支持，其仍能于此期间与外界保持联系。[②]

尽管如此，国外学者对俄乌冲突开始后的前两个月内的互联网性能进行了测量研究，并得出了并不对称的测量结果：乌克兰的互联网性能显著下降，俄罗斯的互联网性能却有所改善。[③]一方面，乌克兰的网络连接因基础设施方面遭受沉重打击而受到影响，例如，大规模停电或损坏的通信线路和设备，使路由更改和瓶颈拥塞，从而导致互联网性能下降。另一方面，Netflix 和 You tube 等领先服务的流媒体停止向俄罗斯客户提供服务等制裁行为，反而客观上提高了俄罗斯用户在其他平台上的下载和上传速度，俄罗斯的网络性能得到了改善。

（二）对内以断网防御为底线

与中国“互联网治理与互联网创建共同发展”背景下产生的“防火墙”不同，俄罗斯的互联网治理在很大程度上是被动的——一个姗姗来迟的控制系统被动地嫁接到一个曾经免费且开放的乌托邦式数字空间。尽管控制历史并不悠久，但在此次俄乌冲突中，俄罗斯仍以断网防御为底线，以“主权互联网法”的建设成果为基础，实现了对数字信息空间的全面控制。2022 年 3 月初，俄罗斯通过禁止虚假信息的法律，明确规定传播涉及俄罗斯武装部队虚假信息的人要承担刑事责任，同时封锁脸书、推特等西方社交媒体。同时，国际制裁加上苹果、Netflix、

① Elizabeth Gibney, “Where Is Russia’s Cyberwar? Researchers Decipher Its Strategy”, *Nature*, 2022, No.603, pp.775−776.

② Damjan Štrucl, “Russian Aggression on Ukraine: Cyber Operations and the Influence of Cyberspace on Modern Warfare”, *Contemporary Military Challenges*, 2022, No.2, pp.103−123.

③ Tal Mizrahi and Jose Yallouz, “Internet Performance in the 2022 Conflict in Ukraine: An Asymmetric Analysis”, *ArXiv*, May 18, 2022, doi:10.48550/arXiv.2205.08912.

Spotify 和微软等科技公司的“企业自我制裁”，原本垄断俄罗斯市场的西方互联网公司正无意间“将信息空间拱手让给克里姆林宫”，切断了俄罗斯用户与国际平台的联系，使俄罗斯政府更容易将俄罗斯公众与不利于俄罗斯国家安全的所有叙述内容隔离，从信息源头上避免“颜色革命”的爆发。

此外，在此次俄乌冲突中，“乌克兰请求切断俄罗斯网络”事件被视为当前地缘政治形势下对互联网多方模式的一种极限测试。尽管负责欧洲 IP 地址分配的机构欧洲地区互联网注册网络协调中心（RIPE NCC）、国际互联网协会（ISOC）和互联网名称与数字地址分配组织（ICANN）先后拒绝了乌克兰的请求，多方模式暂时经受住了考验，但它们所能发挥的与全球互联网断联的垄断式权力，仍成为决定俄乌在网络战场上胜负的关键。然而，俄罗斯早已在“主权互联网法案”中预见了此类极端情况，在一次次的断网实验中做好了充分的准备。面对乌克兰庞大的志愿“IT 军队”以及其西方国家盟友的“网络战运动”对俄罗斯在线服务网络造成的种种打击与威胁，俄罗斯的战时政策文件规定，所有俄罗斯网站必须采用俄罗斯域名系统服务（DNS），完善、记录和保存网络日志，并对重要网络数据进行备份，以应对西方运营商服务的“中断”。为防止网络访问证书的缺失，俄罗斯财政部表示拟成立一个国家认证中心，为俄罗斯组织机构网络免费发放网络访问证书，用以确保所有浏览器和操作系统的访问兼容性。此外，俄罗斯立法委员会已批准将退出俄罗斯的外国企业资产国有化的议案，“国有化名单”中包括关闭在俄全部业务的英特尔公司。此举将俄罗斯境内的网络电信设备国有化，缓解俄罗斯面临的网络电信设备短缺问题。[①]

当前，俄罗斯已经有足够的能力断开与外部的连接，有效地阻止俄罗斯未明确允许的所有访问。尽管俄罗斯有足够的能力进行彻底的断网，但是俄罗斯当局否认计划切断互联网。2022 年 3 月 8 日，俄罗斯数字发展、通信和大众传媒部就否认了切断俄罗斯互联网的计划。其副部长表示，我们正在为各种情况做好准备，以确保俄罗斯在线资源的可访问性。俄罗斯外交部新闻处也表示，没有从国内切断互联网的计划。[②] 由此可见，完全断网作为底线防御措施并不会被轻易使用，但是如核弹一般作为对攻击方国家的威慑已经达到了保卫的效果。正如苏联在冷战期间从未使用过核武器的一个常见解释是，预期任何攻击都可能引发毁灭性的核反应，这种对相互毁灭的恐惧足以阻止美国发动核攻击，即使他们花了几十年时间积累了大量的武器库存。

五、美西方媒体对俄罗斯互联网主权的扭曲

随着西方主要通信和技术公司从俄罗斯撤销服务，以及莫斯科随后对独立媒体的严格审查，美国新闻媒体称此次俄乌冲突为俄罗斯黑暗专制的“1984 年”。他们认为来自俄罗斯内部的互联网审查制度越来越像一个世界末日的铁幕，俄罗斯妄图建立自己的封闭互联网，并通过其强有力的数据内容控制措施使该国的网络舆论和社会舆论在更大程度上向内倾斜，使该国国民丧失所谓的向外界探索“冲突真相”的机会。

① 颉靖、王斌：《从俄乌冲突看俄罗斯“断网”演习的意义》。

② David Gilbert, “Russia Is Preparing to Cut Itself off from the Global Internet: The Kremlin Is Getting Ready to Bring down the Digital Iron Curtain” (March 8, 2022), Vice News, https://www.vice.com/en/article/88gevb/russia-is-preparing-to-cut-itself-off-from-the-global-internet, retrieved May 10, 2023.

不仅如此，美国媒体还有意无意地拿俄罗斯的主权互联网与中国的防火墙进行类比批判，并认为主权互联网是碎片化的网络，是逆全球化的。究其实质，这不过是美国玩弄西方政治话语、通过互联网技术概念掩盖西方世界对他国国家主权的践踏所催生出的一种奴役与政治束缚的障眼法，[①] 体现了美国霸权主义在网络空间中的延展，暴露了全球数字安全治理规则的缺位和网络空间国际规则的缺失。实际上，相较于我国的长城防火墙和俄罗斯的主权互联网，美国对全球互联网的互联性威胁才是最大的。

从技术基础上讲，美国掌握着根域名服务器系统（包括镜像）及与其相配套的任播节点和基站，以及硬件、软件和开发工具，如果 DNS 解析被切断，顶级域名被删除并停止应用服务，我们自行建造的镜像服务器（群）将无从镜像，并将导致网络信息空间的混乱。从主观战略来讲，美国早在 2018 年就颁布了“以武维和，防御前置”这一赤裸裸的霸权主义版本的网络安全法案。从客观实践上讲，美国屡屡在战争期间采取基于数字技术优势的舆论战、网络战和认知战的数字混合攻击措施，在和平时期针对优势企业和技术领域进行定点狙击，旨在消除威胁美国在未来科技领域优势的健康竞争力量。所以，美国所谓对主权互联网的抵制、对网络空间独立性的捍卫，不过是披着号称“自由羊皮”的霸权恶狼行径。

与美国媒体的攻击相反，俄罗斯互联网主权的建设从未以分裂、封锁互联网为目的。“主权互联网法案”联署人之一柳德米娜·波科娃解释，“建立自己的互联网”的说法本身就自相矛盾，因为“不可能在一个国家里建立所谓的国际网络”。[②] 她进一步解释，此法只是旨在建立一个替代性基础设施，即建立一个备份网络，以便在非常状态下不至于无法正常上网，其设计目的是维护俄罗斯互联网资源完整和互联网不间断地运行。俄罗斯杜马副主席沃洛金也公开向公众解释，该法“不是要封锁，不是要切断，而是要保障俄罗斯互联网的安全”[③]。尽管当前处于俄乌冲突，俄罗斯也从未明确公布自己试图切断俄罗斯与全球互联网的连接。所以，俄罗斯在俄乌冲突前就为切断与国际互联网的连接做未雨绸缪的战略准备，丝毫不代表俄罗斯希望主动与世界断连。

断网是俄罗斯政治、经济和社会难以承受的打击。正是为了避免外部断网可能产生的灾难性后果，俄方才坚持多年断网演习，寻求自主路径。[④] 这只不过是国家和民族长期以来形成的居安思危意识的体现，以及传统地缘政治博弈在网络时代的延续和发展。[⑤]

六、余论：互联网主权的未来

“网络空间主权是国家主权在位于其领土之中的信息通信基础设施所承载的网络空间中的自然延伸”[⑥]，即网络空间主权是主权国家基于各种信息基础设施和通过互联网等信息网络技术形成的在网络空间中享有的国家最高权力，是数字时代不容侵犯的国家主权。尽管俄罗斯“主权互

① 张舒：《透过俄乌冲突谈对“网络无国界”的再认识》，《中国信息安全》2022 年第 4 期。

② 转引自陈春彦：《试析〈俄罗斯互联网主权法〉的背景与影响》。

③ 转引自陈春彦：《试析〈俄罗斯互联网主权法〉的背景与影响》。

④ 陈春彦：《俄罗斯互联网主权立法创新与启示》。

⑤ 穆琳、李维杰：《俄罗斯应对国家断网威胁的启示》，《中国信息安全》2017 年第 11 期。

⑥ 赤东阳、刘权：《从网络空间国际合作战略看我国维护网络空间主权的思路》，《网络空间安全》2017 年第 Z1 期。

联网法”自颁布以来饱受争议，但俄方在此次俄乌冲突中面临断网等“卡脖子”的危险时，其针对互联网主权未雨绸缪的建设的价值得到了在枪林弹雨中前所未有的检验和显现。

网络主权本质上是一种保护本国互联网安全的主动作为的能力，而不是被动性的闭关锁国。许多西方民主国家都担心“互联网巴尔干化”问题，即网络的物理和政治碎片化将导致其失去自由和开放的特征。[①] 但是，国家的互联网主权终究是意味着在网络世界中积极管理依赖关系、创建可操纵性的基础架构；意味着一种主动作为的、妥善管理网络并达成政府利益目的的能力。所以，各主权国不会轻易地尝试中断全球互联网不同部分之间的连接，但是会努力确保本国互联网至少在其影响范围内符合国家法律和利益。不仅如此，互联网的技术性内在架构也决定了这些数据信息形式的部分、短暂的碎片化是互联网自我保护机制的一个方面，也是互联网治理走向有序光明的未来所必经的阵痛。

中国是网络空间主权的主要积极倡导者。2010 年 6 月，国务院新闻办公室在发布的《中国互联网状况》中首次公开提出“互联网主权”。2014 年 11 月 19 日，国家主席习近平在向首届世界互联网大会致贺词时提出“尊重网络主权”[②]，成为世界上首位倡导“网络主权”的国家元首。2016 年 10 月 9 日，习近平总书记在主持中共中央政治局第三十六次集体学习时也强调：“要理直气壮维护我国网络空间主权，明确宣示我们的主张。”[③] 2016 年 12 月，国家互联网信息办公室发布了我国首份《国家网络空间安全战略》，再次强调要“尊重维护网络空间主权”[④]。

随着主要民族国家互联网主权的建设，当今世界已形成了民族国家以网络主权对抗数字帝国主义网络霸权的世界格局。为切实打破网络霸权国家倡导的“网络无国界”之假象、有效地捍卫网络空间整体安全，必需迅速补齐我国在网络空间领域的意识缺陷、坚定维护网络主权的决心、积极捍卫网络主权的信念。

在俄乌冲突中，各方网络战、认知战与网络基础设施攻防战的经验提示：网络世界大同愿景正在破灭，在数字世界权势格局的暗流涌动中，我们应当防患于未然，洞悉霸权主义国家以自由之名行损害互联网主权的图谋，完善有关国家互联网主权保障的立法，提升关键信息基础设施保护领域的国家能力，推动国际合作，积极参与全球和区域性的网络安全合作，与各方共同构建互惠、民主、透明的全球互联网治理体系，如此则能得道多助，有裨于中国的“网络空间主权”理论主张与实践方案在国际上获得更为广泛的认同。

第一作者系江西财经大学数据法律研究院研究员、江西财经大学法学院副教授

第二作者系江西财经大学数据法律研究院助理研究员

① Frédérick Douzet, “La géopolitique pour comprendre le cyberespace”.

②《共同构建和平、安全、开放、合作的网络空间　建立多边、民主、透明的国际互联网治理体系》，载《人民日报》，2014 年 11 月 20 日，第 1 版。

③《加快推进网络信息技术自主创新　朝着建设网络强国目标不懈努力》，载《人民日报》，2016 年 10 月 10 日，第 1 版。

④《国家网络空间安全战略》(2016 年 12 月 27 日)，中国网络安全和信息化办公室委员会网站，http://www.cac.gov.cn/2016-12/27/c_1120195926.htm，最后浏览日期：2023 年 5 月 10 日。