《学术界》(月刊)
总第261期,2020.2
ACADEMICS
No.2 Feb. 2020

地缘政治视域下的网络空间及其安全

陈文胜

(西南科技大学　马克思主义学院,四川　绵阳　621010)

〔摘　要〕地缘政治是通过地理表征和实践来认识和建构世界的一种方式。网络时代,在由协议和软件代码等计算机技术基础构成的网络空间,传统的地缘政治观念受到冲击,支撑地缘政治的三个地理假设——主权、领土和边界被赋予新的内涵。它们以意识形态地缘政治为背景,突破了传统的管辖范围,已从领土、领海、领空延伸到"信息边疆",网络空间成为各国角逐权力的新战场,展现了全新的地缘政治风险和愿景。因而,构建网络命运共同体、制定网络空间行为规范、消除数字鸿沟和信息霸权、完善对话协商机制、推动互联网治理模式变革,对于消除全球化时代网络空间地缘政治风险显得尤为重要。

〔关键词〕网络空间;地缘政治;网络空间安全;网络主权
DOI:10.3969/j.issn.1002-1698.2020.02.007

地缘政治是人类政治和地理环境相互作用的产物,通俗地讲,它是权力在空间中的分布和互动。互联网技术的诞生使世界进入一个权力转移的时代,赋予了主权国家一道无远弗界的"信息边疆",改变了传统地缘政治的内涵、外延以及逻辑,在造就更高等级的、更独特的地缘政治问题的同时,也进一步拓展了国家利益的疆域,动摇了固有的国家主权观念,危及部分国家的安全。法国"数据处理与自由委员会"曾指出:"信息就是力量……跨国界的数据流通也可能导致国家主权的丧失。"[1]互联网不断作用于国际政治之核心——国家利益、权力、空间、安全,使主权国家置身于一个没有固定边界的虚拟的信息世界之中,在这样的世界里,国家不仅要维护传统边界的安全,还要维护互联网主权边界的安全。作为科学技术工具的典型代表,"互联网展示出来的力量史无前例",[2]已经成为国际地缘政治博弈的手段、场域和载体,引起传统国家主权和国家安全、世界地缘秩序和权势格局的大变革。

随着互联网的成熟,各国开始在网络空间中维护传统的领土观念,从现实主义的角度看待互联网潜在的安全风险。在学界,相对于已为世人耳熟能详"空间有机体""生存空间""海权""心脏地带""世界岛"等地缘政治概念和理论,网络空间的地缘政治意蕴一直是相对较少的地理研究方面的主题,"就目前而言,网络空间中地缘战略和地缘政治思维的'学派'并不多",[3]"围绕

作者简介:陈文胜,法学博士,西南科技大学马克思主义学院教授,研究方向:网络政治学研究。

网络空间的地理学文献很匮乏”,[4]因而该领域被肯希利斯(Ken Hillis)描述为“人类地理学‘家族’中可怜的继姐妹”。[5]而“正是由于地缘学研究中缺乏对网络空间的批判性研究,表明这是一个充满希望且富有成效的研究领域,这种研究将挑战对领土和非领土化的二元化理解,并为认识当今世界地缘政治本质提供重要洞见”。[6]在今天这个信息高度政治化的时代,大多数通信、贸易、金融、娱乐、文化、知识创新都将发生在网络空间。“可以肯定的是,关于网络空间未来的辩论将在未来多年成为世界政治的一个显著特征。”[7]本文从网络地缘政治的视角,探索网络空间的复杂形势、政治风险及应对之策,希冀为这一充满活力的研究领域提供一己之见。

一、网络空间的地缘政治学意蕴

地缘政治学是“时代的产物”,随着时代的变迁而不断被赋予新的内容。它脱胎于地理,成长于人文地理,成熟于政治地理。西方地缘政治学起源于19世纪末、20世纪初。1899年首创这一概念的鲁道夫·契伦(Rudolf Kjellén)将地缘政治学描述为“把国家作为地理的有机体或一个空间现象的理论”。[8]德国地缘政治学之父卡尔·豪斯浩弗(Karl Haushofer)认为“地缘政治学是新的关乎本国利益的国家科学……一种关于空间决定一切政治过程的学说,它以地理作为广泛基础,而尤其是政治地理。”[9]美国海权论代表人物马汉认为地缘政治是指“国家政治权力与地理环境之间的关系”。[10]对杰弗里·帕克(Geoffrey Parker)来说,地缘政治学是“从空间或地理视角出发的国际关系研究”。[11]

对这些传统地缘政治思想家的地缘战略思想进行分析,不难看出,无论是陆权时代,还是海权时代,自然地理环境和社会经济环境是影响地缘关系和地缘结构形成的基础,地缘政治学展现了政治空间化的逻辑。传统的地缘政治思想认为,世界被划分为离散的空间单元,每个国家都可以在自己的领土内自由行动。国家可以采取行动的空间是由其边界划定的领土,在这些边界内采取行动的自由是其主权,领土、边界和主权是支撑国际、国家体系的地理假设。传统地缘政治把世界本身看作一个从全球到区域的政治实体,各国作为不同规模的政治实体在其中采取行动。而世界的政治多样性已被浓缩成各种地理容器,包括世界本身。[12]显然,传统地缘政治的落脚点都是从国家利益出发,主张通过军事手段开疆拓土,实现地理空间的增量。这一模式映射了零和博弈中严格界定领土和空间的现有国家逻辑,即所有的领土收益都是以牺牲他国利益为代价的。

随着全球化和网络时代的深入推进,地缘空间的“非地理化”趋势日益显露。全球化和网络化的发展打破了国家垄断地缘政治学的格局,国家主权管辖的地缘空间开始逾越领土边界的限制,包括全球互联网系统、通讯基础设施、物联网、云计算、大数据、区块链等,构建了具有政治逻辑的“全球网络空间”。在网络空间中,地理范围大小、资源多寡、人口数量、相对位置、气候等传统地理环境要素,被技术、标准、基础设施、接入设备、关键应用和核心能力等新的地缘环境要素所取代。可以说,网络空间的边界或领域是由强大的网络力量所决定的。库尔(Kuehl)认为,网络力量是一个国家在网络战期间利用其网络资源的真实或潜在的能力。[13]网络力量所体现的潜力可以在空间上组织起来,即“网络力量应该具有地缘政治维度,就像陆地、海洋、天空、太空等战略领域一样,这是自然和不可避免的”。[14]随着国家将大量的行动转移到网络空间,各国开始通过技术、法规监管和过滤互联网,这在广泛的理论背景下被视为其确立领土意识。可见,“网络空间确实与地理环境有关,具有地缘政治意义”。[15]正如伊恩·F. 波帕(Iulian F. POPA)所言,“毫不夸张地说,网络空间的地缘政治很可能是一种特殊的演变”,“在不久的将来我们会发现网络力量对历史的重大影响,以及网络空间作为一个虚拟有机体对国际关系体系的重

要性”。[16]

在全球化和信息化的背景下,地缘政治学从以国家为中心的政治领土概念,转向对与权力有多重关联的空间性更细致入微地理解,甚至有学者将这种国家权力的转变视为“地理的终结”。它表明,无论是在历史上还是今天,空间性并不局限于地域性,也不简单地等同于国家领土性。正如约翰·阿格纽(john Agnew)指出的那样:“国家权力并没有被完全地控制在国家领土之内,它也可以发生在非领土之上或跨空间的网络之中”。[17]这种观点具有深远的影响,因为它突破了政治严格的地域观念(权力行使于相互排斥的空间之中),也反驳了国家是全球政治的自然而又稳定的主体的观点。当代地缘政治学表明,国家权力是以领土和非领土的形式在实际外交关系中产生的,国家权力在不同领域、不同主体间的运用中是不同的,国家权力的建设有大量的工作是通过在国内和国际领域的网络空间完成的。也就是说,互联网改变了地缘政治权力的重心,开辟了承载权力的虚拟空间,把地缘政治的范畴从国家权力的中心扩大到更广泛的网络空间,这个全新的空间模糊了国家的边界,展现了新的权力运行逻辑。这就需要我们密切关注网络战略制定的各种背景,这些背景包括制网权、信息权、话语权、传播权等。

然而,互联网从来都不是天使模样。正如约翰·斯通(John Stone)所指出的那样,互联网空间的“领土化”存在很大的安全挑战和漏洞。[18]在网络空间同样存在着国家之间、非国家和其他行为体以及其他形式的冲突和暴力。迈克尔·华纳(Michael Warner)指出,早在20世纪60年代,人们就对信息系统的物理安全开始担忧。[19]随着技术的发展和国家对信息技术依赖的增加,网络攻击的复杂性也在增加。早期对窃取国家机密的担忧,演变为对网络攻击能力的恐惧——依赖互联网的通信变慢或瘫痪,以及超级病毒(如StuxNet恶意软件)等网络超级武器不断的被开发等。互联网潜在的安全风险使得各国开始重视在网络空间中维护传统的领土观念。如今,美国通过咄咄逼人的互联网过滤和控制,强化数字边界,巩固其地缘政治愿景。在美国霸权主义和全球主义制度背景下,网络空间成为意识形态地缘政治的延续。目前,以深度渗透、长期窃密和战略控制为目标的各种网络危险比历史上任何时候都要复杂,这一切使得网络空间安全作为一个极其重要的问题被提出来。

二、网络空间对传统地缘政治的超越

一些学者认为,“自互联网诞生时起,它就被认为是一个全新的、独立的空间,与现代、日常生活紧密相连,是普通事物的延伸”。[20]互联网建构了新的物质世界和精神世界,以数字化和虚拟化的方式,延伸和突破了传统的实体空间,引发了空间的内涵和外延的巨大变化。同时,互联网拓展了地缘政治博弈空间,将各个国家卷入全球彼此依赖而又相互竞争的网络,使得“制网权”成为国际政治的新型国家权力和各国在网络空间争夺的焦点。互联网时代,地缘政治关于国家权力在空间中如何展开的逻辑发生了重大变化,地缘政治战略要素面临的变数呈现出全新的特征和明显的突破性。

(一)全新的空间类型:全球网络空间

网络空间是由人类通过技术手段创建的逻辑空间,在实践和理论上继承了地缘政治传统。互联网时代开放的网络结构改变了时空维度,扩展了人类活动场所,也扩大了主权范围,模糊了传统的主权边界,赋予国家疆域新的含义。一是网络空间与地理空间并存。互联网技术的兴起为人类政治、经济、文化的互动创造了一个更丰富、更灵活、更容易被使用的新的地理环境和非物质空间。互联网技术将物理和电子元素结合起来,实现了地理空间与虚拟网络空间的并存。正如胡尚·阿什拉夫(Hooshang Ashraf)所言:“网络空间既不是一个独立于现实物理世界而存在的领域,也不仅是一个物理空间概念的领域。网络空间根植于世界,网络空间内的行为与外界

的行为是不可区分的。”[21]二是赋予了“近”和“远”新的定义。作为人类居住的地球表面的延伸,互联网无限缩小了空间几何意义上的距离,造就了大规模的“全球时空压缩”,重新组织了社会关系结构。正是由于这种被曼纽尔·卡斯特称作为“网络社会”的形成,人们越来越多地把地点和领域看作是“社会关系和网络中相互联系的时刻”,而不是历史上认为的被边界包围的物理区域。[22]在网络技术的支持下,人们彼此间的联系很大程度上不再取决于地理距离,无论人们身居地球任一位置,都将实现沟通的零距离。三是造就了“流动空间”。卡斯特区分了“流动空间”(space of flows)和“地方空间”(space of place)。他指出地点和新通信技术的相互作用正在创造一个网络社会,在这个社会中,一个以电子技术为表征的具有明确的社会、文化、物理和功能特征的“流动空间”将一个地方连接到一个社会和经济相互作用的全球网络之中,有力地消除了地方空间的国家壁垒,实现了信息空间的全球化。[23]

(二)全新的地缘目标:制网权

网络与权力密切相关,权力的虚拟化、技术化、弥散化体现了网络空间中权力的运行逻辑。正如美国学者汉斯·摩根索认为:“国际政治像一切政治一样,是追逐权力的斗争。无论国际政治的终极目标是什么,权力总是它的直接目标。”[24]在互联网时代,国家追求的权力目标不再是集中于获得某一领土或地理的支配权,而是聚焦于制网权。制网权是国际网络空间安全研究的核心概念和基础问题之一。制网权是网络空间内的国家权力,是一个主权国家在网络空间生存的根本保障,是国际政治领域中继制路权、制海权、制空权和制天权之后的一种新型的国家权力形态,是国家权力的新型构成要素,它具有地理背景和地缘政治意义。技术、标准、数据、网络空间则构成了制网权的核心资产和蕴含权力的场所。因此,谁拥有 IP 地址分配、域名解析、通信干线、硬件制造和软件制造、技术理念等网络实体基础设施或技术的优势,掌控着互联网通讯标准、链接标准、域名解析标准等项标准制定的权力,以及拥有大规模的数据和信息丰富的网络空间,谁就能够顺理成章地掌握制网权。当前,随着信息革命的发展和深化,“信息主权”已经成为国家主权概念中的重要内容。以美国为首的西方国家以建立网络威慑、掌握互联网制网权为目的,相继制定了网络空间战略,而广大发展中国家则遇到了冷战结束之后“信息殖民”的新险情,世界开始步入“网络霸权时代”,一场侵犯与捍卫“信息边疆”的“网络战”已经打响,制网权已成为地缘政治中争夺的新焦点。

(三)全新的资源基础:软实力作用凸显

在传统地缘政治理论中,地理位置和地缘环境的优劣直接关联着主权国家生存和发展的潜力。而这种地理优势或地理矛盾具有天赋性、致命性、差异性和可变性等基本特征,更多依赖的是硬实力上的资源丰寡或布局。这些资源包括人口、领土、自然资源、经济规模、军队和政治稳定等,它们都是权力的隐喻。无论是马汉的“海权论”、麦金德的“路权论”还是杜黑的“空权论”都是主张力争在拥有更多硬实力资源的基础上赢得地缘政治优势的一种战略思维,带有明显的物质决定论倾向。互联网具有独特性,它蕴含着以信息资源为基础的权力,它是人为创造的、新近出现的权力域,比其他权力域更容易受到技术变化的影响,基础设施、网络、软件、人的技能等资源都定义着网络权力。互联互通的互联网降低了地理矛盾的政治效能,引导世界地理体系步入了“地理全球化时代”,世界的权力性质也正在发生变迁,获得软实力资源成为左右世界地缘政治局势的重要因素。正如约瑟夫·S. 奈所言:“在评估当前的国际权力时,技术、教育和经济发展等因素变得更为重要,而地理、人口和原材料变得越来越不重要。”[25]时至今日,以互联网为代表的信息技术的飞速发展,使得国家所能调集的资源形态发生了很多变化,软实力在赢得地缘政治优势中的作用被日益凸显出来,世界各国越

来越重视智力资源的挖掘和开发,致力于软实力的争夺,地缘政治正日渐被以知识、技术等为特征的智缘政治所取代。

(四)全新的地缘秩序:以制度为主导的秩序

传统地缘政治学致力于从权力视角、空间结构主义视角、冲突视角等来解读国际秩序和国际关系,帝国主义、霸权主义和强权政治成为地缘政治的基本形态。“互联网的出现动摇了制度,打乱了传统秩序”。[26]互联网是通过国际过境协议、域名管理、自主系统部署以及国家在审查和控制方面的努力所共同搭建的,这为网络空间带来了复杂的公共问题。跨国界、跨文化、跨语言的网络空间和信息流使任何一个国家单独的治理能力捉襟见肘。在国际社会框架中,秩序主要是通过国际制度和法律协定来维持的。法律、规范和国际法律协定,是传统国家的基础。近年来,无论是在全球层面还是区域层面,在互联网安全治理上都呈现出了不同程度的合作主义趋势。这正如斯塔夫里阿诺斯所言:“人类作为一个群体所面临的问题是,如何使自身不断增长的知识与如何运用这些知识的智慧保持平衡。”[27]对于全人类而言,共建网络空间命运共同体是良途。安德鲁·利亚罗普洛斯(Andrew Liaropoulos)指出:“在网络空间行使国家主权是建立国际网络秩序的必要步骤。”[28]然而,发达国家往往以大国强势地位施展信息霸权的“魔杖”,在有形和无形空间拓展硬实力和软实力的战略张力,营造霸权政治下的国际和平,建立西方国家主导下的国际秩序。基辛格曾指出:“秩序问题,尤其是国际秩序,乃是困难问题。”[29]这意味着,寻求治理网络地缘空间的制度和机制,建立能够约束各方的国际公约还任重道远。

三、地缘政治视域下网络空间面临的安全风险

在国际政治领域,国家安全是地缘政治研究的重点。比如,尼古拉斯·斯皮克曼(Nicholas Spykman)把地缘政治定义为“根据地理要素来筹划一个国家的安全政策”。[30]互联网隐藏着地缘政治因素,再现了主权和领土性的概念,使传统的空间性质和国家安全观正发生着新的变化,国家安全威胁的来源、主体及手段等都发生了天翻地覆的变化。近年来,网络空间国际博弈日趋激烈,“发生利益冲突的利益相关者试图将网络空间塑造成为自己的优势”。[31]加之网络技术的滥用、开放和匿名的设计理念、国际规范的缺失,导致网络虚拟空间各种安全威胁、冲突持续增长。“阿拉伯之春”“茉莉花革命”“占领华尔街”“斯诺登泄密案”等事件,凸显了网络时代地缘政治新的安全风险。

(一)传统的主权和安全观念受到冲击

网络主权是国家主权在网络虚拟空间的自然延伸和体现,是国家新的主权形式。“网络空间的出现开辟了通往一种新型国家主权的道路:网络主权”。[32]早在 16 世纪法国思想家让·博丹就创立了主权理论,认为“主权是一种绝对的和永恒的国家权力”。[33]随后,英国政治学家蒂姆·乔丹从技术权力、媒介力量和想象力量等层面阐释了“网络权力”学说,后来学者引申出“网络主权”思想。互联网时代,自由、虚拟、开放和无中心的信息交流方式削弱了主权国家对信息垄断的权威,也突破了传统国家主权的管辖范围和独立性。国家的管辖权、独立权、平等权、防卫权等传统意义上的主权在网络空间中发生异变并遭受侵蚀。在过去,对大多数政府来说,主要的威胁是基于“州际”的,“现在威胁已扩展到整个社会,不分国界”。[34]正如弗朗索瓦·杜兰所言:“如今,国家主权正在丧失其领土形式。”[35]网络空间重组国家权力结构,承载着国家利益的分配,各国开始将网络空间视为现有地理现状的延伸,并将法律领域扩展到网络空间,以安全和经济可持续的名义在网络空间确立其主导的主权制度。而在网络主权上,美国提出互联网开放和自由的主张,将网络空间视为全球公域,对全球网络空间从海底电缆到代码等进行大规模开发,以此维护其网络强国地位,攫取更多利益。作为信息弱国,树立网络主权观念,维护主权空

间安全就显得十分重要。在“斯诺登事件”被曝光后,“互联网自由”阵营的合法性和可信度已被大大削弱,人们对网络安全治理的未来再度感到担忧。

互联网在冲击国家主权观念的同时,也使得非传统国家安全问题凸显。由于互联网具有普遍性、跨国性、战略性等一系列特征,减弱了各个领域物理隔离的有效性,使得风险主体扩大化和全球化。网络空间主权的理论与实践伴随着网络技术的漏洞、网络犯罪的频发、网络恐怖主义的威胁、网络话语权的争夺、网络意识形态的渗透、网络间谍活动的增加等,愈发引起各国政策制定者和研究者的关注。在 Stnxnet 病毒被发现之前,很少有人相信网络入侵会导致战略伤害。尤其是自“棱镜门”事件之后,基于网络空间的“另类作战”正趋于常态。一些国家开始更新传统的安全观念,抛弃以往对待网络价值中立的观念,从整体和系统的国家安全战略视角出发,大力加强网络空间安全建设和顶层设计。“从国际安全的角度来看,国家行为者坚决应对特定网络威胁的权利几乎是无可争议的,尽管它超越了国家领土”。[36]当今,越来越多的国家意识到,“谁掌握了网络,谁就将拥有整个世界”,信息主权和话语主权越来越成为各国网络博弈的核心内容,而网络安全则为网络主权奠定了现实基础。在现实中,由于网络空间中人类行为活动的隐蔽性、广泛性、脆弱性、瞬时性等特征,使得网络空间“易攻”却“难守”、归责难。随着计算机的迅速发展和用户数量的大增,网络空间安全问题将成为一个更加严峻的显性问题。

(二)大国虚拟空间战略博弈态势加剧

网络空间的战略博弈,可以简称为“网络战”。它是“各国为改变信息、破坏属于或被认为对另一个目标国家至关重要的计算机系统、网络或互联网设备而采取的行动”。[37]“网络战是一个广泛而复杂的领域,尽管它只是在 20 世纪 80 年代初开始进入公众意识”。[38]兰德公司曾指出,工业时代的战略战是核战争,而发生在信息时代的战略战更多是网络战。如今,网络战作为一种全新的作战形态登上了人类的战争舞台。正如阿奎拉(Arquilla)等所宣称的那样,“网络战来了”。[39]随着技术的发展和国家对信息技术依赖的增加,网络攻击的复杂性也在增加。网络战争发生在现有权力结构和权力模型的空间范围内,实现了自由和公开地跨越国际法律边界的运作。网络战在很大程度上忽视了传统的领土边界,国家地理边界和地理环境变得毫无意义,技术成为影响战争后果的决定性因素。网络战意味着利用知识减少资本和劳动力的消耗,将“信息和知识的平衡”转向对自己有利的一方。而一个国家的“国家网络力量”或潜在网络资产的总和对其在海外投射力量和话语权、国内的网络主权和安全至关重要。

当今,“网络空间已经成为另一个争夺经济和政治权力的竞技场。在这种背景下,各国政府越来越坚决地要求对网络拥有管辖权”。[40]它们按照地缘政治愿景对网络空间进行边界和领土划分,努力利用互联网不对称的性质获得投射实力和创造信息优势,从而达到其政治目的。2007 年爱沙尼亚遭受了长达三个星期的大规模分布式拒绝服务攻击(DDOS),这标志着一种新的难以追踪、没有固定模式的、影响国际安全的网络战威胁的开始。又如伊朗对 DigiNotar web 浏览器安全证书颁发机构的攻击则具有全球性的影响:世界上所有的 Internet 浏览器,如 Internet Explorer、Firefox 和 Google Chrome,都必须进行更新,以保护它们免受伊朗的攻击。在美国政府和某些军事指挥家的大肆渲染下,美国及其西方盟友被描绘成被黑客包围和渗透的国家以及不断受到各种威胁或攻击的对象。他们将网络空间视为美国可以实现并保持主导地位的领域,认为需要采取强有力的措施防御“数字珍珠港”。[41]一些西方学者还主张利用冷战地缘政治框架以及冷战经验和专业知识,重新构建针对中国和俄罗斯等传统对手的网络战框架,主导和统治网络空间领域。但是,“正如国际安全动态中经常出

现的请求一样,当一个国家重新确立其目标和建立其能力时,其他国家也会这样做。现在,数十个国家的政府在其武装部队内部都有专门的‘网络司令部’或类似的机构”。[42]这也使得网络空间逐渐成全球政治博弈新的“角斗场”。

(三)“网络边疆”存在着巨大安全漏洞

相较于传统地缘政治的物理疆域,网络边疆存在着巨大的信息安全漏洞。漏洞是网络安全问题的根本,厂商设置的后门漏洞、地下黑市交易的零日漏洞等为黑客入侵、病毒木马、恶意攻击等网络犯罪、网络恐怖主义、网络间谍行为提供了可乘之机,导致了各类网络安全事件频发。从网络的技术安全逻辑上讲,网络空间通过各种活动和技术法规日益成为各国领土。但由于个人、团体或国家针对互联网上别的国家的信息技术漏洞发动的网络攻击活动,则会对这些目标国造成严重的国家利益的损失和带来严重的安全威胁。网络空间的技术风险主要来源于网络技术的不完备性和滥用。互联网技术诞生后使人类进入了数字化生存阶段,而过度依赖网络则可能因为计算机网络遭遇破坏、存在漏洞和产生故障使国民经济正常运行所依赖的重要政务、金融、交通、通讯、电力等部门信息网络系统的瘫痪,从而引发巨大的经济损失和社会动荡。此外,互联网诈骗、黑客入侵、计算机病毒、信息的泄露、财产安全、网页仿冒等一系列问题也屡见不鲜。

从理论上讲网络安全漏洞是广泛存在的。无论是网络基础设施还是组成系统的代码,其自身的缺陷是与生俱来的,大量已知、未知的漏洞和错误不同程度地存在于其中。一个国家的网络技术的安全逻辑往往表现为“木桶效应”,一旦一个环节出现问题,就会成为国家的“命门死穴”和“阿喀琉斯之踵”,越发达就越依赖、越脆弱就越恐惧,这也是网络空间的不安全特质和困境。通常在面对各种网络安全威胁事件时,传统的捍卫国家主权和边疆的手段已难以适应新的复杂的网络生态,各种未知的后门漏洞、不断花样翻新的计算机病毒、日益智能化的网络入侵方式使得传统的网络安全防御手段日益捉襟见肘。如,2017 年 6 月,代号为“Petya”的电脑病毒在全球多国肆虐,极具高危性、突发性、高破坏性和大规模性,在给多国的政府、银行、电力系统、通讯系统、企业和机场等国民经济部门带来不同程度损失的同时,也为各国的网络安全和防御敲响了警钟。无论是“棱镜计划”,还是“索尼黑客攻击事件”“震网病毒”“火焰病毒”等事件都表明,各种网络安全事件和冲突将愈加频繁和突出,主动防御的难度加大,维护“新的国防动态边疆”主权与安全的任务十分艰巨。

(四)数字资本主义带来了“信息殖民”

数字资本主义是指信息时代的资本主义。互联网诞生后,它以前所未有的方式与规模渗透到资本主义经济文化之中,带动政治经济的数字资本主义的转变和资本主义运行模式的变革,在使信息通信产业成为资本主义政治经济结构新的支撑点的同时,也使得信息技术的资本竞争和逐利成为一种全球化的趋势。互联网设备、软件程序和基础设施成为各种国际力量觊觎掌控的利润积累的源泉。互联网是跨国资本主义积累战略的前沿阵地,也是各国激烈争夺的一块全新的地缘政治空间。西方传播政治经济学研究的代表人物席勒在《数字化衰退》一书中把数字与传播产业置于争夺互联网的地缘政治框架中进行考察,揭示了资本主义各种力量围绕全球网络管辖权和产业控制权展开的激烈竞争。美国依仗其在信息技术领域的控制权、主导权和全球话语权,通过对信息权力的巧取豪夺,建构了信息资本主义模式,实现了从技术控制到资源控制、从信息控制到法理占领,先发制人地占领国内外市场。可见,互联网加快了全球市场化程度的同时,也带来了不平等以及发达资本的霸权控制,造成了困扰市场制度的种种弊端。

在网络时代,“信息殖民”取代土地殖民成为地缘政治的新目标。互联网是一场由强者操纵和制定规则的游戏,它在使人类迎来地球村时

代和网络民主幻象的同时,也充当着支配、殖民和剥削信息不发达国家的工具,使社会分裂加剧、数字鸿沟扩大,人们陷入新的"信息殖民"的樊笼之中。正如阿尔温·托夫勒在《权力的转移》中所言,未来的世界将控制在信息强权者手中。[43]与传统地缘政治博弈中的攻城略地的争夺方式不同,网络时代的信息殖民主义更具隐蔽性,网络空间成为霸权争夺的新场所,门户网站、社交网络、虚拟社区、数据中心等成为新的战略核心和"战略要地"。事实上,"'网络社会'的兴起并没有破坏美国资本在信息和通信技术(ICT)领域的霸权",[44]"在很长一段时间里,美国是唯一负责管理互联网的国家。美国当局在不需要强制的情况下主导互联网的监管、配置和发展。它通过控制和定义互联网的战略规划、操作实践、共同的信仰、文化愿景和代表性来行使自己的权力"。[45]美国在互联网发展过程中所扮演的"信息宗主国"的历史角色,对世界地缘政治发展产生了不利影响。

四、网络空间安全的维护路径

当今,网络空间安全已经成为"非传统安全"和全球性威胁。尤其是2013年"斯诺登事件"发生之后,如何维护网络空间地缘政治的安全,制约信息霸权国家在网络空间的权力滥用,成为世界各国关注的焦点。随着网络安全战略意义的提升,各国围绕网络空间发展权、主导权和控制权展开的竞争更加激烈,大有一触即发之势。对于国际社会而言,如何使用好互联网,避免全球网络空间地缘冲突和纷争,制定被大多数国家共同接受的全球性国际规范成为当务之急。

(一)形成对网络空间命运共同体理念的共识

当今,世界多极化、经济全球化、社会信息化深入发展,各国利益彼此勾连,同舟共济、合作共赢成为时代的要求。随着全球治理体系和国际秩序变革的强力推进,世界面临的不稳定性、不确定性也日益突出。针对日益复杂的国际局势,在众多的全球化议题中,全球网络空间安全是一项重要的国际安全议程。中国领导人提出了建设网络空间命运共同体的构想,以取代网络空间零和博弈的"修昔底德陷阱",为维护网络空间安全提供了中国方案。同网络霸权国家奉行的单边主义方案不同的是,我们主张在尊重网络主权平等的基础上,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。网络命运共同体思想是网络空间秩序重建的大逻辑,也是全球互联网治理的大道理。它的提出,为携手共建网络空间命运共同体提供了根本遵循,有利于实现世界各国共建共享网络信息资源。从网络空间地缘政治安全的视角来看,它还有利于减少网络空间内各国网络主权的纷争,规避网络单边主义文化对网络空间的操控,消弭网络攻击、网络犯罪、网络恐怖主义、网络战争等带来的安全风险。全球互联网的健康发展有赖于各国的协作共建,而遵守"相互尊重、相互信任"的原则,加快形成对网络命运共同体重要性的共识成为当务之急。

(二)制定共同的网络空间安全国际行为规范

随着互联网在国家政治经济生活中作用的加强,国际关系中源于网络安全问题的冲突和摩擦日益增加,如网络战、网络犯罪和网络恐怖主义等频繁发生。有学者指出,网络空间的政治性已不容忽视,它正在成为由政府、军方、私人企业和公民网络等利益相关者"参与的,高度竞争、殖民化和重塑的领域"。[46]日益突出的网络安全问题,已严重危及主权国家的安全,要维护各国网络空间地缘政治的安全,必须制定合理的、一致的法规制度,但由于网络空间的复杂性和特殊性,目前国际社会却没有一套专门针对网络空间安全的行为规范,也没有一个统一的国际网络安全组织和技术主权联盟。正如斯科特·贝德曼(Scott Beidleman)所指出的那样:"当下的网络空间犹如19世纪初美国蛮荒的西部。"[47]虽然各国在构建网络空间国际秩序方面有共识,但在网络空间的主权、结构、功能、话语权,以及技术、军事安全和对策等方面却有着不同观点。中美在

网络空间规则制定方面既有合作又有竞争。两国都对制定网络空间规则高度重视,但美国希望依仗在网络技术和资源方面的优势维系其网络霸权,中国则倡导多边主义原则,主张制定反映发展中国家利益诉求的行为规范,避免网络空间“巴尔干化”的风险。目前,各国对达成“全球网络空间协定”还没有形成共识,不同的利益诉求决定了网络安全国际规范的制定还任重道远。

(三)消除国际政治中的数字鸿沟和信息霸权

数字鸿沟是人们(组织、社会团体或地缘政治实体)在通信技术使用意识、使用技能、使用权等方面的不平等。近年来,世界网络发展水平不一,各国之间和各国内部的互联网使用极不平衡。发达国家与发展中国家在信息基础设施建设和使用信息技术上的差距正在迅速扩大。例如,“全球流动空间和‘信息高速公路’似乎在很大程度上绕过了非洲大陆。无论以何种标准衡量,该地区都是世界上联系最少的地区,处于全球数字鸿沟的最底层”。[48]2011 年底,全球 32% 的人使用互联网,而撒哈拉以南的非洲地区的平均互联网普及率仅为 11%;非洲有 8.5 亿人口,占世界的 12%,但其互联网用户不到全球的 5%。普遍的贫困、经济停滞、文盲、电信基础设施不足、不可靠的电力系统、缺乏技术技能,以及常常漠不关心的政府,这些都使非洲步履蹒跚。与此相反的是,美国控制着信息领域的核心技术,掌握着制定标准和规范的实际权力,妄图独霸网络空间控制权,构建以美国为主导的国家地缘政治新秩序。面对这种信息化差距和美国的信息霸权,发展中国家要坚持以合作求秩序、以斗争求秩序,积极推动建立“国际信息新秩序”,共同维护网络空间的主权安全;另外,发展中国家必须加快网络基础设施和信息安全建设,消除各国在信息权力上的不平等。

(四)完善网络空间安全国际合作和对话机制

当前,全球经济范式正从以封闭、独占、垄断为特征的工业经济走向以开放、共享、连接、服务为特征的数字经济,显然,冲突、隔阂与对抗无益于各国经济的发展和政治的稳定。随着网络技术的飞速发展,网络安全问题也日益凸显出来,因特网成为亟待全局管制的全球资源。粗略统计,全球已有 50 多个国家制定了网络安全方面战略和政策。但是由于互联网的开放性和虚拟性,使得任何一国的网络空治理能力都显得相形见绌。正如亚历山大·利洛夫(Александър Лилов)所言:“互联网遍布世界。任何人要把自己隐藏起来,孤军奋战,都将一事无成。”[49]加之当前大国争夺网络空间制高点的博弈日益激烈,因而,对于各国来说,建立合作关系和信任机制至关重要,它有助于实现对彼此主权的尊重,改变政治安全逻辑发展方向。合作的内容包括加强危机管控、冲突预防、网络反恐、打击网络犯罪、数据和信息共享内容。当前,除联合国之外,无论是欧盟、北约、八国集团,还是上合组织、经合组织等国际或区域组织都在网络安全问题上进行了合作。但网络空间安全对话仍然存在着明显的两大阵营:一是以美国为首的西方发达国家集团,另一个就是以俄罗斯、中国等新兴国家组成的发展中国家阵营。因而,从多边、区域、大国双边等方面加强网络安全国际合作战略,建立机制化的沟通互动渠道,提升网络空间安全全球治理的共同认知,显得尤为重要。

(五)打造共建共治共享的网络空间治理模式

随着全球网络空间的态势和格局的演进,针对网络空间的治理模式也经历了技术治理模式、自我规制模式、“多利益相关方”模式、“多边”和“多方”融合并存模式等阶段。“多利益相关方”是一种与传统的自上而下的“统治”和“管制”的方式完全不同的全新治理路径,它契合了全球治理时代互联网的复杂多元特性。以美国为首的西方发达国家以网络开放和自由为借口,主张“多利益相关方”的治理模式,试图通过其人才和价值观方面的“软实力”,削弱政府权威和边缘化联合国作用,以操控网络空间的主导权和话语权;以中俄为代表的新兴市场国家和发展中国家则坚持网络主权原则,认为应采用“多边主

义”的治理模式,力图推动全球网络空间治理朝着更加公正合理的方向发展。习近平在世界互联网大会等场合上,多次提出打造共建共治共享的网络空间治理模式,主张“建立多边、民主、透明的全球互联网治理体系”,[50]“做到发展共同推进、安全共同维护、治理共同参与、成果共同分享”,[51]为互联网空间治理贡献了中国智慧,为互联网发展擘画美好蓝图。未来,世界各国应在加强沟通、扩大共识、深化合作的基础上,推动网络空间实现平等尊重、创新发展、开放共享、安全有序的目标,让互联网更好地承载人类梦想、增进人民福祉。

五、结　语

网络空间的出现重新定义了我们理解和感知国界的方式,它挑战了国际传统的地缘政治观念,在很大程度上改变了国家安全治理的方式。今天,我们正处于人类历史上最深刻的通信进化之中,赖以生存和发展的网络环境从未像现在这样变幻莫测。“在这个时期,网络空间构成的国家安全挑战的复杂性创造了一种新的不安全级别”。[52]围绕着互联网的一些相关领域的紧张局势正在加剧,包括互联网治理、大规模和有针对性的监控,以及军事竞争等。正如罗恩·德伯特(Ron Deibert)所指出的:“网络空间的未来正在上演一场地缘政治之战”。[53]此刻,我们正处在一个历史的岔路口,如何在对网络空间进行限制和监控的同时,以鼓励自由的方式确保其安全,如何在坚持网络空间主权的同时,协调国际网络空间治理机制与各国自身最大利益之间的矛盾,将是严峻的挑战。

事实上,尽管网络空间有其独特的特点,但它仅仅是对当前国际体系的反映,网络空间的国际政治将受到国家竞争、地缘政治关切、共同利益和现有准则的影响。此外,“网络力量不太可能改变大陆和海洋强国之间永恒的地缘政治斗争的性质”,[54]而且“网络行动本身不太可能给我们带来足够的战术和作战优势,以取代传统的军力部署,保护民族国家的相对实力”,[55]网络空间的国家安全仍然不能脱离地区或全球安全的范畴。因此,将网络安全控制在最佳范围内,需要国际行动者实施多边合作和跨国安排,建立共同的网络空间原则和规范,形成网络空间制度的基石。正如迈克尔·切尔托夫(Michael Chertoff)所言:“现代国际法律秩序必须建立在一项新原则的基础之上,各个国家有义务遏制来自其境内的跨国威胁,以防止这些威胁侵犯世界各地其他国家的和平与安全。”[56]而习近平总书记所倡导的世界各国共建网络空间命运共同体的主张,无疑为构建全球网络空间安全新秩序,破解“治理困境”,提供了新路径和指明了正确方向。

注释:

〔1〕郭庆光:《传播学教程》,北京:中国人民大学出版社,1990年,第250页。

〔2〕Jose Vericat,“Is the Google World a Better Place”, *Journal of International Affairs*,2010,24(1),pp. 181 – 194.

〔3〕〔16〕〔32〕〔36〕〔55〕Iulian F. POPA,“Cyber Geopolitics and Sovereignty. An Introductory Overview”, *The 5th International Scientific Conference, National and International Security 2014*, published by Armed Forces Academy of General Milan Rastislavteťánika, 2014, pp. 413, 413, 417, 415,.

〔4〕〔6〕〔12〕〔20〕〔21〕〔37〕Cameran Hooshang Ashraf, *The Spatiality of Power in Internet Control and Cyberwar, Dissertations & Theses*, Los Angeles: University of Calfornia, 2015, pp. 27, 298, II, 152, 163 – 164, 125 – 126.

〔5〕Ken Hillis,“On the Margins: The Invisibility of Communications in Geography”, *Progress in Human Geography*, 1998, 22(4), pp. 543 – 566.

〔7〕〔26〕〔34〕〔42〕〔53〕Ron Deibert,“The Geopolitics of Cyberspace After Snowden”, *Current history*, 2015, 114(768), pp. 9 – 15, 9 – 15, 9 – 15, 9 – 15, 9 – 15.

〔8〕Rudolf Kjellén, *Staten som Lifsform, Published in German as Der Staat also Lebenform*, Leipzig: Hirzel, 1917, pp. 34 – 35.

〔9〕Richard Hennig, Geopolitik, *Die Lehre von Staat als Lebewesn*, Leipzig: Hirzel, 1931, p. 9.

〔10〕〔美〕阿尔弗雷德·塞尔·马汉.:《亚洲问题及其对国际政治的影响》,范祥涛译,上海:三联书店,2007年,第64页。

〔11〕Geoffrey Parker, *Geopolitics: Past, Present and Future*, London: Printer, 1998, p. 5.

〔13〕Kuehl, D. T., *“From cyberspace to cyberpower: Defining the problem”, in Franklin D. Kramer, ed., Cyberpower and National*

Security, Washington DC:. Potomac Books, 2009, pp. 26 – 28.

〔14〕〔15〕〔54〕John B. Sheldon, "Geopolitics and Cyber Power: Why Geography Still Matters", *American Foreign Policy Interests: The Journal of the National Committee on American Foreign Policy*, 2014, 36(5), pp. 286 – 293, 286 – 293, 286 – 293.

〔17〕KUUS, M. and AGNEW, J., "Theorizing the State Geographically: Sovereignty, Subjectivity, Territoriality", in K. Cox, J. Robinson and M. Low eds., *The Handbook of Political Geography*, London: Sage Publications, 2008, pp. 117 – 132.

〔18〕Stone, John, "Cyber War Will Take Place!", *Journal of Strategic Studies*, 2013, 36(1), pp. 101 – 108.

〔19〕Warner, M., "Cybersecurity: a pre – history", *Intelligence and National Security*, 2012, 27(5), pp. 781 – 799.

〔22〕Doreen Massey, "Power – geometry and a Progressive Sense of Place", in J. Bird, B. Curtis, T. Putman, G. Robertson and L. Tickner, eds., *Mapping the Futures: Local Cultures, Global Change*, London: Routledge, 1993, p. 66.

〔23〕Castells, M., *The Rise of the Network Society*, Cambridge, MA: Blackwell, 1996, p. 423.

〔24〕〔美〕汉斯·摩根索:《国家间政治——权力斗争与和平》,徐昕等译,北京:北京大学出版社,2006 年,第 55 页。

〔25〕〔美〕约瑟夫·S. 奈:《硬权力与软权力》,门洪华译,北京:北京大学出版社,2005 年,第 113 页。

〔27〕〔美〕斯塔夫里阿诺斯:《全球通史——从史前史到 21 世纪》,吴象婴、梁赤民等译,北京:北京大学出版社,2014 年,第 7 页。

〔28〕Andrew. Liaropoulos, "Exercising State Sovereignty in Cyberspace: An International Cyber – Order Under Construction", In 8th International Conference on Information Warfare and Security, Denver Colorado, 25 – 26 March 2013.

〔29〕〔美〕亨利·基辛格:《世界秩序》,胡利平等译,北京:中信出版社,2015 年,"序言"第Ⅸ页。

〔30〕〔美〕尼古拉斯·斯皮克曼:《和平地理学》,刘愈之译,北京:商务印书馆,1965 年,第 14 页。

〔33〕Jean Bodin, *On Sovereignty: Four Chapters from the Six Books of the Commonwealth*, 《剑桥政治思想史原著系列(影印本)》, 北京:中国政法大学出版社,2003 年,第 1 页。

〔35〕〔法〕玛丽 – 弗朗索瓦·杜兰:《全球化地图:认知当代世界空间》,许铁兵译,北京:社会科学文献出版社,2007 年,第 6 页。

〔38〕Wagner, B., "Push – button – autocracy in Tunisia: Analysing the Role of Internet Infrastructure, Institutions and International Markets in Creating a Tunisian Censorship Regime", *Telecommunications Policy*, Vol. 36, No. 6, 2012, pp. 484 – 492.

〔39〕Arquilla, J., and Ronfeldt, D., "Cyberwar is coming!", *Comparative Strategy*, 1993, 12(2), pp. 141 – 165.

〔40〕〔45〕Mauro Santaniello and Francesco Amoretti, "Electronic Regimes: Democracy and Geopolitical Strategies in Digital Networks", *Policy & Internet*, 2013, 5(4), pp. 370 – 386.

〔41〕Lynn, W. J., "Defending a New Domain: The Pentagon's Cyber strategy", *Foreign Affairs*, 2010, 89(5), pp. 97 – 108.

〔43〕〔美〕阿尔温·托夫勒:《权力的转移》,周敦仁等译,成都:四川人民出版社,1992 年,第 105 页。

〔44〕Miriyam Aouragh, "Infrastructures of Empire: Towards a Critical Geopolitics of Media and Information Studies", Media, *Culture & Society*, 2016, 38(4), pp. 559 – 575.

〔46〕Nazli Choucri, *Cyberpolitics in International Relations*, Cambridge, MA: The MIT Press, 2012, p. 8.

〔47〕Scott Beidleman, *Defining and Deterring Cyber War, Strategy Research Project*, US Army War College, 2009, p. 21.

〔48〕Barney Warf, *Global Geographies of the Internet*, Springer, 2013, p. 37.

〔49〕〔保〕亚历山大·利洛夫:《文明的对话:世界地缘政治大趋势》,马细谱、葛志强等译,北京:社会科学文献出版社,2007 年,第 239 页。

〔50〕习近平:《在第二届世界互联网大会开幕式上的讲话》,《人民日报》2015 年 12 月 17 日,第 2 版。

〔51〕习近平:《致第四届世界互联网大会的贺信》,《人民日报》2017 年 12 月 4 日,第 1 版。

〔52〕Chris C. Demchak and Peter J. Dombrowski, "Rise of a Cybered Westphalian Age: The Coming Decades", *Strategic Studies Quarterly*, 2011, 5(1), pp. 31 – 62.

〔56〕Michael Chertoff, "The Responsibility to Contain: Protecting Sovereignty Under International Law", *Foreign Affairs*, 2009, 88(1), pp. 130 – 137.

〔责任编辑:刘　鎏〕