《学术界》(月刊)
总第305期,2023.10
ACADEMICS
No.10 Oct. 2023

从域名领土看网络空间主权的边界〔*〕

杨永红

(西南政法大学　国际法学院,重庆　401120)

〔摘　要〕尽管国家并不以域名为由主张网络空间主权,而是通过宣称物理领土主权扩展至网络空间行使网络空间主权,但是域名领土却是网络平台为遵守各国网络空间主权管理网络空间的主要方式。由于缺乏网络空间主权边界的国际规则,网络空间主权的行使范围模糊不清,地缘政治强力介入网络空间,网络空间碎片化严重,国家在网络空间的无序竞争导致网络安全遭受重大挑战,网络空间充斥着脱钩、监管、军事化、不信任和武器化。全球性网络巨头行使着准政府的权力,它们简单地采取基于域名方式与地理过滤方式管理其网络平台,加剧了网络空间的碎片化。无论是域名模式还是以物理存在为基础的分层划分网络空间及过境通行模式都难以在反映网络空间主权现实的同时去网络空间碎片化。将域名与物理存在相结合的模式可明晰复杂的网络空间主权与全球性的迷宫,在尊重国家主权的同时维护网络空间的全球性。当前中国应积极推动国际社会在网络空间的造法活动,可通过域名与物理存在相结合的模式明确网络空间各区域,在解决网络空间权力划分的基础上构建网络空间秩序,推动构建网络空间命运共同体,进行网络空间全球治理,确保网络空间造福人类社会,消除或降低其对国际安全与国家安全所产生的负面影响。

〔关键词〕网络空间主权;网络空间碎片化;域名制度;多利益攸关方模式;网络安全
DOI:10.3969/j.issn.1002-1698.2023.10.003

我们从未见过个人、公司、社区、政府和其他实体能够以如此即时、同期或无处不在的方式存在于民族国家边界内外的空间,[1]由互联网、电信网络、计算机系统、自动化控制系统、数字设备及其所承载的应用、服务和数据组成的网络空间正在全面改变人们的生产生活方式,深刻影响着人类社会历史发展进程。网络空间目前是国家竞争最为激烈的领域,一方面网络空间互联着人与人、人与物、物与物,推动着全球商业繁荣;另一方面物理世界的意识形态分歧、国家利益差异、安全问题同样投射在网络空间,网络空间走向分裂、封闭、脱钩。美国2023年3月发布的《国家网络安全战略》及在同年8月美国网络安全和基础设施安全局发布的《2024-2026财年网络安全战略计划》充分显示地缘政治已强力介入网络空间,技术与意识形态已经高度混杂在一起,美国将中国视为对其政府和私营机构网络最广泛、最活跃和最持久的威胁,且将使用所有的

作者简介:杨永红,法学博士,西南政法大学国际法学院教授、博士生导师。

〔*〕本文系国家社会科学基金西部项目"反外国金融制裁实施机制研究"(22XFX009)的阶段性成果。

治国手段应对各类网络安全威胁。[2]文件充斥着脱钩、监管、军事化、不信任和武器化的政策。网络空间的无序状态下没有国家是安全的,即使是网络空间最强大的国家亦面临着网络安全危机。[3]美国认为网络领域已经从一个辅助作战战区迅速演变成一个不断变化的战争领域,[4]成立了网络司令部,拥有网络任务部队。[5]中国深受网络攻击之害,政府网站每天都面临着海量网络攻击。[6]国家安全与国际安全岌岌可危,网络空间需要国际规则下的有序治理。尽管各国承认国际法适用于网络空间,但哪些规则适用于网络空间仍然模糊。历经多年的讨论后,仅就主权规则适用于网络空间与国际法适用于网络空间达成基本性共识,在网络空间主权的边界及网络空间法律地位等基本规则上均无合意。[7]建立网络空间秩序的进展极为缓慢。显然网络空间主权规则是网络空间秩序的基础性规则,明晰网络空间主权的边界无疑是重中之重。当前国家主要通过物理领土延伸主张网络空间主权,但通过该主张来划分网络空间主权范围在实践中缺乏可操作性。如果域名成为判断网络空间主权领域的标准之一,不仅极具可操作性,而且网络平台亦提供了一定的实践支撑。本文为明晰网络空间主权的边界,将首先从主权的本身及其动态发展展开研究,分别结合国家顶级域名与通用顶级域名的法律制度与相关实践分析国家在与域名连接的网络空间的权力,并从全球性网络平台的运行模式的角度来探讨网络空间主权对网络平台运行的实际影响,在此基础上比较不同的网络空间主权边界的学说,以解决网络空间主权的现实无序问题。

一、网络空间主权的成因

要明确网络空间主权的边界,显然要理清网络空间主权与传统主权间的关系,分析领土主权的发展历程,从网络空间主权的产生与发展进程窥视网络空间主权的本质特征。

(一)主权——受到限制的最高权力

主权并非自古有之,从该概念在国际关系中被明确为基本规范,尚不足4个世纪。这与漫长的人类社会发展的历史相比的确微不足道。但它的出现与普遍被接受,彻底改变了世界秩序的形态,进而塑造了国际关系的运行模式和行为体间的博弈类型,该概念不但塑造和限定着当今世界秩序的本质属性,也深刻影响着观察者与参与者的认识论与方法论立场。威斯特伐利亚主权体系下,世界由主权国家组成,在国家之上没有更高的权威。主权具有抽象无形的特征,它基于相互承认的领土划界,旨在使国家能够在领土界限以内进行管辖,对外独立于其他国家。由于主权意味着对内的最高统治权,对外独立于其他国家,主权国家都是相互平等而独立的,因此主权在国内建立了等级秩序,但在国际社会却要求无政府秩序。[8]

主权的概念是国际关系、国际法、政治理论、政治哲学和现代史的核心概念,[9]这导致主权的定义众多。但不管如何定义主权,无论从法律角度还是从政治角度,主权的核心含义都是一样的,都强调“领土内至高无上的权威”。[10]这些简单的字包含最复杂和最有争议的内涵,特别是网络空间主权问题为主权这一概念带来了前所未有的挑战。在国际社会的发展进程中,主权发展到今天有了很大的变化,它除了依然保持传统主权的本质内容外,其内涵在不断发展。第一,主权具有排他性,排除其他国家管辖。管辖权的排他性表示国家的基本国际法律地位,它不受其领土管辖范围之外的任何一个外国政府或实体的管辖,不管是行政方面,还是立法方面,还是外国司法方面或外国法律,除自己的国内法之外只受国际法的限制。第二,主权的平等既是权利也意味着义务。主权代表在其管辖范围内的最高权威,必然意味着相互之间尊重各自在其管辖范围之内的最高权力。因此,国与国之间都应当互相尊重各自的权利,都负有不妨碍别国在其管辖范围内行使管辖权的义务。于是主权平等原则为国际社会提供了有序、稳定和可预测的国际关系,被确认为建立联合国的基础,也被《联合国宪

章》与《关于各国依联合国宪章建立友好关系及合作之国际法原则之宣言》确定为国际法的基本原则。[11] 国家对内的主权权利反转成为国家主权责任,以确保个人福祉。“每一个国家都有保护人民免遭种族灭绝、战争罪、种族清洗和反人类罪的责任。国际社会必须使用适当的外交,人道主义和其他和平手段,帮助保护人民免遭上述暴行,并且在特殊情况下联合国安理会可以采取集体强制行动制止暴行以承担国际社会的保护的责任。”[12] 第三,主权既是绝对的又是相对的。一方面,主权代表一个国家的法律地位,或者作为一个主权国家特定实体的代表。这意味着,主权通常是一国在国际法上的合法身份。在另一方面,主权又赋予政治实体特别的权利、权力和义务,[13] 国家作为拥有权利、权力、义务和责任的具有国际法律人格的特定实体,主权代表了其在国际关系的体制框架内的地位,主权并不会明确规定具体包括什么权利。因此,主权作为法律地位而言,它是抽象的、绝对的;同时在实体内容上,它在本质上“包罗万象”,不仅指国家所拥有的权利的集合,还包括国家义务的集合,所以主权又是个相对的概念,随着时间的变迁而发展,为了适应新情况和紧急情形,它是一个在国际法框架内而不是来自国际法的一种酌情的自由。[14] 概言之,一方面,主权是绝对的,因为它代表着一国领土内最终和最高权力机构,享有独立于其他外部势力在一定领土范围以内的专属管辖权。另一方面,主权又是相对的,主权受到国际法和国内法的限制,例如在海洋法领域,领土主权受到了无害通过权与过境通行权的重大限制。第四,经济全球化导致部分经济主权权利由国家自愿通过条约向国际经济组织让渡,而且这些经济主权权利的让渡还伸展到非经济的其他领域,包括社会、文化、政治等方面。经济全球化是当今社会最深刻的变化之一,令国家彼此之间相互依存的经济关系已经达到了前所未有的广度和深度。随着科学技术的发展,世界范围内企业的发展不再依靠大工业生产和各种生产要素传统意义上的结合,而取决于各种科学技术、信息与知识的组合,[15] 于是以超地域性的高速发展的科学技术为物质基础,以资本与商品跨越边界的流动为特征,技术革命、资本扩张共同推动经济全球化的进程。[16] 通过提供一套最低标准的秩序,国际法促进了贸易、交通、信息的发展,带来了资本、商品、人员跨界流动的便利,全球化的进程也从经济扩张到了社会、文化、政治等多方面。同时,使得国际问题与国内问题的划分不再绝对,一些问题既是国际问题又是国内问题,一些原来的国内问题成为国际问题,也同时使一些原来的国际问题成为国内问题。第五,国际领域与主权领域的划分不再绝对。出现了介于二者之间的第三类区域,一国对该类区域不享有主权,仅享有部分主权权利,其他国家在此区域依然享有国际区域的部分权利。如专属经济区,沿海国享有勘探、开发、养护和管理此区域自然资源的主权权利和部分管辖权,其他国家在此区域依然享有航行自由、飞越自由及铺设海底电缆和管道的自由等在公海区域的权利,公海区域的规则在与该区域不相冲突的情况下同样适用于专属经济区。[17] 主权权利与主权相对独立的情况使主权变得极富弹性。第六,主权仍然构成全球化时代国际关系的基础。在全球化浪潮席卷而来、主权让渡成为常态的情况下,发展中国家更是担心大国利用全球化的影响干涉其内政,反而会更加强调主权平等和不干预内政等原则,极力保护自己国家的主权独立。国家仍然是国际社会的主体,它们依然对其领土和人民行使对内的主权,对外的主权也是真实存在的。无论全球化进程有多么广泛,以主权国家为基本架构的威斯特伐利亚体系在可预测的时间段内不会发生根本变动,国际法治依然会建立在主权的基础之上。这是客观事实。实际上,国际社会现在比以往任何时候都面临着一个悖论:国家看到自己在国际秩序中比以往任何时候都相互依存,但它们又继续以分散的方式进行决策。[18] 网络空间规则的发展进一步加剧了主权与全球性的矛盾,网

络空间主权、数据主权、技术主权成为主权的新兴内容。

(二)领土主权的动态发展

领土的边界随着人类社会科技发展发生了极大改变。自古典时代以来,人类的行动主要由两个领域主导:陆地和海洋。但随着 1904 年飞行器的出现,航空领域成为一种人类涉足的新场所。1957 年,“太空时代”的诞生开启了最后一个物理领域——外太空。当国家和个人开始发展进入海洋、空气和外层空间领域的技术能力时,这些领域中的每一个都存在着不受主权控制的有力论据,如海洋的流动性使得国家无法通过获得陆地领土的方式获得,空气空间的无形状态更被理所当然地视为人类的共同财产。然而,国家利益,如贸易和国家安全,再加上国家的技术能力,最终战胜了这些论点,并决定了这些领域目前的法律地位。从领土发展的过程来看,空气与海洋都曾被认为是一个整体,无法对其划界,被认为应该是由全人类共有的国际领域,不具备领土属于国家主权行使的对象的本质特征。这在很大程度上是因为当时人类缺乏实际控制空气空间与海洋的能力。然而,随着科技的发展,国家具备对空气空间与海洋行使主权的能力之时,领海与领空的概念得到广泛的接受。从领空与领海出现的历史来看,它们成为领土的关键在于国家是否有能力对其行使主权。这里的国家并非指少数国家,而是国际社会的各国。因为只有大多数国家能够有效控制并保卫的空间,国家才能真正对其行使主权,具备领土的条件。如外太空并未如同领空一样成为隶属于主权的客体,很大程度上是因为航天大国只是少数国家,大多数国家都缺乏前往外太空行使主权的能力,即使各国声称了主权,事实上也无力行使主权,这可能是各国未将外太空明确为领土的核心原因。从这一点来看,网络空间不会因其是一个难以划界的整体而否认其领土的性质,重要的是国家是否拥有对网络空间行使主权的能力。

由于科技的发展,国家领土扩张到海洋与空气空间的同时,国家在海洋领域创设了第三类区域,这一类区域既不是领土也不是国际领域,是介于二者之间的领域。国家在此区域并无主权,而是享有一定的主权权利,这类主权权利主要以开发自然资源的经济权利和与之相关的管辖权为特点。《联合国海洋法公约》明确了专属经济区与大陆架系沿海国享有主权权利的领域,其他国家则有航行自由、飞越自由、铺设海底电缆和管道的权利。[19]另外在海洋,领土主权受到了不少限制。无害通过制度、过境通行制度、群岛海道通行制度均不同程度地限制了领土主权,为领土主权设置了例外情形。《联合国海洋法公约》第三部分规定,只要“不损害沿海国的和平、良好秩序或安全”,“为了持续和迅速穿越领海”,船舶可“无害”通过领海。《联合国海洋法公约》禁止在船只无害通过时起落或接载飞机以及任何携带武器的演习等,潜艇和其他水下航行器无害通过时必须在水面上航行并展示其旗帜。但《联合国海洋法公约》同时又允许沿海国在其领海的特定区域暂时暂停外国船只的无害通过,只要这种暂停对保护其安全至关重要。另外在用于国际航行的海峡中,《联合国海洋法公约》规定了“过境通行权”,“仅为使船舶和飞机在公海或专属经济区的一部分与公海或专属经济区的另一部分之间的海峡持续迅速过境而享有的航行和飞越自由”。在“过境通行”期间,船舶和飞机可以正常运作模式过境,不允许沿岸国暂停过境通行。[20]《联合国海洋法公约》谨慎地平衡了一个国家的安全需求与世界对商业和贸易海洋航行自由的需求。这种平衡正是网络空间新领域所需要的。

领土边界的不断扩张与领土主权相关规则动态发展的进程表明,基于国家实际控制在领土的核心地位,加之网络空间与人类社会全方位的联系,网络空间或将成为国家最重要的疆域。[21]

(三)从自由乌托邦到国家主权领域

网络空间是计算机技术和信息技术相结合的产物,是科技创造的一个全新领域。从一开始

科技巨头就展开了与国家对该区域的管辖权力博弈。在互联网时代的早期,网络空间被一些人视为思维的新家园、无政府无疆界的虚拟世界。互联网治理出现了渴望在世界各地遵循一套规则的世界主义理想。[22]该学说以互联网公司进行网络治理为基础,将互联网视为一个整体,通过在全球互联网普遍实施统一的规则来进行监管。[23]互联网公司被凯特·克洛尼克称为"新总督",称互联网治理为"在线平台模式自治"。[24]哈佛大学教授戈德史密斯指出,网络空间由人和物组成,因此国家可以对其领土上的人和物行使权力,并规范其活动。[25]网络空间自治观点忽视了网络空间无法脱离物理存在的基础事实,忘记了这些"新总督"都受国家管辖。互联网很快被证明既不是一个全球公地,也不是一个虚拟或无主权的领域。网络空间一方面附着于基础设施与人,具有明显的物理化特征;另一方面其最基本的技术架构是一个分布式的网状结构,即通过打破信息流通中心节点的存在,实现每个节点之间权利和义务的对等,表现为一个开放的全球系统,没有物理的国界和地域限制,用户可以匿名的方式将信息在瞬时从一个终端发送至另一个终端,实现全球范围内的互联互通。网络空间既有形又无形、既属地又虚拟、既地域又全球的特征,使网络空间能否成为新领土充满了争议。

从网络空间的物理结构来看,网络空间连接的基础设施是现实空间有形存在的,通常存在于国家的领土之上。而网络空间连接的不仅是计算机,更重要的是人。使用者的数据成为网络空间的内容层,使用者通常位于一国的领土之上,而且从事网络空间活动的程序员、技术人员和计算机工程师通常受其所在领土国的主权管辖。[26]因此,信息基础设施与数据均与领土有着直接的联系,数据却难以附着于领土,但它不能脱离信息基础设施与人,无法脱离物理存在而单独存在。国家只要能够控制其边界内网络的物理组成部分,就可以对互联网进行有效管辖。[27]"世界各地、海底、空中的每一个信息和电信网络的每一个组件都受制于专有利益,无论是私营公司还是主权政府,或者两者都有。每一根铜线、光纤电缆、微波中继塔、卫星转发器或互联网路由器都是由合法的实体生产或安装的,它们不仅保持对该实物资产的所有权,而且希望得到主权当局的保护。"[28]于是网络空间的治理模式很快转向了传统的监管模式,包括通过国内法和基于主权的国际法。[29]

杰克·戈德史密斯和蒂姆·吴教授在2008年针对以国家为中心的治理体系迅速被转移到网络空间提出了三种解释。第一,终端用户通常选择当地语言和文化内容。尽管互联网在世界范围内具有较大的影响力,早期英语网站居主导地位,但随着时间的推移,互联网的使用和内容在许多方面变得更加狭隘,因此具有地域性。第二,科学技术的发展使国家能够对互联网实施控制,如防火墙和封闭网络。尽管互联网有完全无边界运作的技术能力,但由于国家的安全控制,互联网已经被碎片化。第三,各国已经认识到关于规范国家安全、知识产权、合同执行、诽谤、诈骗、赌博以及言论审查等相关法律在网络空间适用的必要性。[30]上述解释当然能够部分说明国家对网络空间行使主权的可行性与必要性。本质上,国家对网络空间行使主权的核心在于网络空间的重大价值与国家拥有实际控制的能力。

早期的互联网思想家期望互联网能够脱离主权的控制,现在被视为不切实际的乌托邦梦想。国家只要能够控制其边界内网络的物理组成部分,就可以对互联网进行实际控制。[31]随着互联网的爆发性成长,过去十年来,各国已陆续在网络空间行使主权。今天,几乎所有人都承认,互联网不是一个法外之地,相反,国家拥有大量富有成效的工具控制互联网,而且国家日益倾向使用这些工具,越来越多的国家颁布法律对网络空间进行监管。事实上,经过数十年的实践,目前的核心问题已经从国家可否主张其对网络空间的主权转为怎么行使网络空间主权的问题。[32]

二、国家域名与网络空间主权

网络空间是虚拟的现实空间,是电子通信(特别是通过互联网)发生的环境,是使我们能够利用互联网实现各种计算机设备之间通信的虚拟领域。[33]国际标准化组织将网络空间定义为互联网上的人、软件和服务通过与之相连的技术设备和网络进行交互而产生的复杂环境,这种交互不以任何物理形式存在。[34]互联网被描述为许多单独但相互连接的电子通信网络。它是一个分组交换网络,通过将消息分解成较小的寻址分组来分发消息,这些分组沿着独立的路线到达目的地,在那里,它们被重新组装成原始消息。独立的路由器确保"被寻址的数据包在饱和的信道周围流动",而不受中央控制。这个系统不仅提高了效率,还提供了一个更安全的通信系统。如果一个节点坏了,网络就会围绕它重新路由。根据任何给定时间的需求,数据包在最有效的路径上传输,导致没有可预测的传输路径,也没有办法禁止数据包在特定状态的开放网络上传输。不同的计算机和网络能够相互通信,因为它们都被传输控制协议/互联网协议(TCP/IP)设计为使用相同的通用语言。它的存在和发挥作用是因为若干独立的计算机和计算机网络运营商决定使用通用数据传输协议与其他计算机交换通信和信息。互联网没有集中的存储位置、控制点或通信通道,单个实体控制互联网上传递的所有信息在技术上是不可行的。[35]因此,互联网被认为是去中心化的一个技术体系,而域名是独立计算机相互发现的地址,并使全球互联互通,不同域名所连接的网络空间在处于不同的国家管辖的同时,组成了一个全球性网络空间。

(一)国家顶级域名的产生与发展

域名制度于1983年在美国诞生的时候,仅有通用顶级域名(gTLD)。最初的目的是没有地理联系,也没有地理限制。最初的五个"通用"域名中的三个——.com,.edu 和.org 是在20世纪80年代设计的,没有按地理位置定义的注册资格要求;任何符合域名用途描述的人都可以在这些域名上注册域名。[36]而另外两个通用原始域名.gov 和.mil 实际上是有领土注册要求,因为它们被交给了美国总务管理局和美国国防部,并分别由美国政府和美国军方使用。[37]1985年诞生的.us,.uk,.il 是最初的国家顶级域名(ccTLD,亦指国家域名、国家代码顶级域名等)。ccTLD 由国际标准化组织的两个字母的国家代码组成,与通用顶级域名不同,ccTLD"对应于一个国家、地区或其他地理位置",[38]至少从名称而言具备地域性。ccTLD 与通用顶级域名的不同并不是因为技术差异,而是因为参与互联网早期管理的人员将这些域名空间专门用于不同的国家及地区。[39]

从1985年到1993年,互联网域名制度的创始人普斯特尔(Jon Postel)以先到先得的方式授予个人或实体 ccTLD,并不需要申请者与该域名有领土联系。[40]但随着越来越多的国家接入互联网,国家和私人实体开始充分发挥国家顶级域名的社会经济潜力。ccTLD 的代理实体的数目从1990年的46个增加到1993年的108个,2002年时共有243个国家及地区代码顶级域名。[41]20世纪90年代中期,几乎所有现有 ccTLD 都有了代理实体,包括那些互联网接入非常有限的国家。[42]1994年3月起,获取国家顶级域名开始较为系统,要求代理实体必须有一名指定的经理来监督域名空间,且行政联系人必须居住在该国。因为管理者是国家和全球互联网社区的"受托人",所以管理者必须对所有申请域名的人公平。此外,管理者必须在为网站域名运行的服务方面做得"令人满意",并且"重要利益相关方"必须同意授权是适当的,[43]还要求 ccTLD 服务器须在所请求的域名国的领土上。[44]

1998年11月,美国商务部和互联网名称与数字地址分配机构(Internet Corporation for Assigned Names and Numbers,以下简称 ICANN)就域名系统(DNS)管理的转让达成协议后,域名制度的管理模式转变为多利益攸关方模式。政府成为互联网域名管理中重要的利益攸关方。ccTLD 的管理

从私人手中转为由 ICANN 中政府咨询委员会(Governmental Advisory Committee)负责。[45]政府咨询委员会在 2000 年即提出政府对其 ccTLD 有最终决策权,[46]但当时并未得到 ICANN 的支持。尽管 ICANN 并不愿交出 ccTLD 注册权,但国家在争夺中占据了上风。2003 年在日内瓦和 2005 年在突尼斯举行的关于信息社会世界首脑会议讨论了 ccTLD 的决策权,其最后文件与政府咨询委员会指向相同。2005 年 11 月 18 日《突尼斯信息社会议程》第 63 段认为:国家不应参与有关另一个国家的国家顶级域名的决策,各国以不同方式表达和定义的关于影响其国家顶级域名的决定的合法利益,需要通过灵活和改进的框架与机制得到尊重、维护和解决。[47]这明确显示了国家在 ccTLD 域名权上的排他性。事实上,2005 年 9 月 30 日的草案更进一步,它称"每个政府都对其各自的国家及地区代码顶级域名拥有主权"。[48]由于美国政府对根区资源的控制,美国政府亦不得不回应其他国家的主权关切。在 2005 年信息社会世界首脑会议期间发表的一份声明中,美国重申其打算保留"其在授权更改或修改权威根区文件方面的历史性作用",但也承认政府在管理其 ccTLD 方面有合法的公共政策和主权关切。[49]

正是由于根服务器受到 ICANN 与美国的管理,一些人主张国家对 ccTLD 的控制受到了一定的限制,因此国家对 ccTLD 的权力不是最高的,故不属于主权性质。[50]还有学者认为国家对 ccTLD 提出主权主张的最现实和最实际的理由是,一个主权国家(美国)对所有 ccTLD 拥有最终控制权,而其他国家需要通过维护主权来制衡这种控制。由于美国对根区资源的控制是基于历史的偶然,而不是互联网治理的固有或永久特征,主权主张是对这种偶然情况的合理反应。一旦偶然性消除,即美国商务部 2016 年 1 月已将控制权移交给 ICANN,那么主权主张的主要驱动因素随之消除。[51]而另外的意见认为,关于 ccTLD 管理的基本思想是,ccTLD 与各自的国家之间存在真正的联系,因此,一个国家可以对自己的 ccTLD 行使完全管辖权,故 ccTLD 可成为国家在网络空间的领土。[52]

(二)国家顶级域名的法律地位

如前所述,国家顶级域名的法律地位存在争议,它是意味着该国的主权范围,还是仅仅意味着该国的财产,抑或国际公共资源,在 21 世纪初期 ICANN 与国家争夺此类域名的管理权时,学术界的争议最为激烈。随着国家对此类域名获得了管控权,关于其法律地位的争论并未尘埃落定,仍然缺乏法律文件加以明确。[53]

首先,ccTLD 属于无形财产。尽管 ICANN 强调域名为服务,但不少法院明确其为无形财产。在 Kremen v. Cohen 一案中,美国第九巡回上诉法院认为,域名是无形财产,因为它是一种能够精确定义的利益,能够独立占有或控制,能够产生合法的排他性要求。[54]印度最高法院在 Satyam Infoway 案中认为,域名可以被承认为知识产权,并受商标法管辖。[55]在英国 OBG 有限公司诉艾伦案中,法院表示域名可如版权或商标一样是无形财产,并指出这是一项宝贵的权利。[56]加拿大安大略省高等法院的一项裁决确认,.ca 的域名是个人财产,因此受相关个人财产的规则的约束。[57]在一个涉及德国域名争议的案件中,欧洲人权法院声称,"占有"的概念不仅限于有形商品的所有权,还适用于域名等无形商品。该法院表示,注册商和注册人之间的合同赋予域名持有人一项不受限制的权利,即从其产生的收入中受益,将权利出售给他人,并禁止他人使用该域名。因此,使用相关域名的专有权具有经济价值。考虑到上述标准,这一权利因此构成了"占有"。[58]弗吉尼亚州巡回法院在 NSI v. Umbro 案中提出了同样的论点,之后弗吉尼亚州最高法院推翻了判决。[59]在瑞典的一个案件中,法院认定瑞典域名 piratebay. se 和 thepiratebay. se 应被视为无形财产并可以被没收。[60]

法院的定性并不总是一致的。一些美国法院认为,域名是财产还是服务的问题对案件的结果

无关紧要。NSI v. Umbro 案是域名系服务的著名案例。[61]“域名注册是注册商和注册人之间服务合同的产物”。[62]弗吉尼亚州最高法院认为,注册人拥有的任何合同权利,即使涉及财产,在没有域名注册服务的情况下都不会存在,服务合同也不能被扣押。法院称,如果允许扣押域名,任何服务合同都将是可扣押的。虽然法院讨论了域名的产权与服务的关系,但最终得出结论,确定域名是否为知识产权不会影响案件的结果。[63]因此,法院没有对域名的产权状况作出肯定的判决。在 Dorer v. Arel 案中,美国法院在没有对域名的法律地位作出任何结论的情况下,决定根据. com 注册的争议解决政策来解决域名争议。[64]

在洛克希德·马丁公司诉网络解决方案公司案中,法院裁定. com 的注册商提供了服务,指出 NSI 作为. com 的管理者与美国邮政局的角色几乎没有区别:当互联网用户输入域名组合时,NSI 将域名组合转换为注册人的 IP 地址,并将信息或命令路由到相应的计算机。NSI 提供域名组合,就像邮政服务提供街道地址一样。[65]该法院的推理遭到了批评,被认为其对 DNS 技术功能的无知促成结论的不正确。[66]然而,在关于域名作为财产或服务的争论中,ICANN 和注册机构几乎总是反对将域名作为财产,强调它们提供的是服务。[67]确实,ICANN 及注册机构提供互联网接入和名称解析服务器等服务,以实现其作为互联网地址的功能,这些服务本身确实毫无价值,但它们一旦被锚定在全球唯一和排他性的域名注册中,即具有了财产价值。[68]所以,域名功能涉及财产和服务,承认其提供服务不一定会必然破坏注册域名本身的财产地位。正如土地可以是财产但并不排斥其领土主权一样,即使域名具备财产地位,也并不与国家对 ccTLD 主张主权相排斥。

其次,国家对 ccTLD 有最终的决策权,即拥有对内主权。由于 ccTLD 最初来自科学家的私人安排,从一开始并未成为国家主权声称的对象,但随着互联网日益深入影响到一国政治、经济、文化、社会等方方面面,ccTLD 原本与特定国家或地区对应的本质成为国家对 ccTLD 的主权主张的现实基础。尽管有人列明了国家对其主张主权的各类瑕疵,认为对 ccTLD 的主权主张没有法律、政治或逻辑依据,但如同国家主权向海洋、天空的扩张,其核心基础事实上不在理论上或逻辑上,而是来自国家的实践与国家的合意。

在国家对 ccTLD 的域名管理方面,ccTLD 从 ICANN 转移至国家后,ccTLD 的注册条件不再是统一的,注册条件最终取决于对应国家与地区的政策。每个 ccTLD 的要求各不相同。如加拿大对 ccTLD 注册资格有严格的领土限制,只有当个人和实体是加拿大公民或永久居民,根据加拿大法律成立或注册的公司、信托和合伙企业,加拿大政党、工会、教育机构,以及其他加拿大机构时,他们才能在. ca 上注册域名。[69]法国亦有效地控制着其域名登记处,要求紧密的领土联系。[70]欧盟根据欧洲议会和理事会第 733/2002 号条例[71]创建了自己的 ccTLD——. eu,根据第 874/2004 号条例(EC),[72]欧盟委员会通过了管理. eu 的公共政策规则。[73]因此,欧盟对其 ccTLD 的管理拥有完全管辖权,[74]并据此曾拒绝 ICANN 访问其根区域文件。[75]爱尔兰共和国的 ccTLD 则是一个注册资格要求限制较少的顶级域名,但它仍然要求与其国家保持密切的联系。根据爱尔兰的注册和命名政策声明,. ie 是爱尔兰的在线地址,因此,所有. ie 域名持有者必须位于爱尔兰岛,或者与爱尔兰岛有真正的联系。为了证明一个人或实体的总部在爱尔兰,申请自然人可以使用其爱尔兰驾照或护照,实体可以使用诸如爱尔兰注册企业编号或增值税编号之类的文件。仅基于与爱尔兰的“真实联系”注册域名,申请人必须证明潜在域名持有人与爱尔兰岛上的消费者或企业进行了交易,或明确打算与爱尔兰岛上的消费者或公司进行交易。[76]还有一些 ccTLD 更为开放,附加更少的领土限制。例如,图瓦卢的. tv 域名注册是完全开放的,并受

益于图瓦卢的两个字母代码与“电视”的缩写重合,使得这个小岛屿国家的虚拟“领土”远远超出了其物理边界。[77]一些过去有限制性注册资格要求的国家为了吸引更多的人和实体注册其域名,获得更多的收入,放宽了其注册要求,向外国注册人开放其 ccTLD,这些国家包括比利时(2000 年)、瑞典(2003 年)、斯洛文尼亚(2005 年)、葡萄牙(2012 年)和芬兰(2016 年)。[78]

尽管 ccTLD 起源于一个几乎不受国家控制的领域,但不管是注册域名条件严格与否,最终还是取决于对应政府的政策,任何对 ccTLD 的政策变动都需要获得对应的政府的授权。互联网域名系统可以由一些计算机和网络科学家管理的日子早已一去不复返了。[79]目前正是由于政府决定他们的 ccTLD 将如何运作,导致各国的注册条件千差万别。[80]而这些差异正好体现了主权行使的结果。无论是 ICANN 或任何一个其他国家均不能对他国的域名行使更高的权力。

再次,国家对相应域名的主权不受其他国家或实体的限制,拥有对外的独立主权。正如《突尼斯信息社会议程》所规定的,国家不参与其他国家的域名管理与决策,在其排除其他国家的权力方面并无争议。有争议的在于 ICANN 是否对国家域名拥有超越对应国家的权力。过去 ICANN 是国家域名管理的技术和行政当局,国家的监管措施须符合 ICANN 制定的政策和原则,以避免再次授权,早期政府在监管本国域名管理方面显然受到了限制。[81]目前 ICANN 已退出了在国家顶级域名上的管理,保持着与国家顶级域名管理者的合作关系,[82]如其管理着根服务器。显然,国家对 ccTLD 有一定的管理瑕疵,但 ICANN 对国家在 ccTLD 的权力缺乏限制工具。国家与 ICANN 之间曾因域名管理发生过冲突,如美国司法部 2001 年在未经 ICANN 批准的情况下,修改了. us 根区域文件中的信息。美国司法部通过技术上强制重新授权,迫使美国国家域名注册职能的法律权力从威瑞信(Verisign)转移到纽斯塔(Neustar)。[83]2001 年多米尼加自行重新指定了注册商,在新注册商管理多米尼加域名注册数年后,ICANN 才在 2007 年认可了该事实。[84]无疑,国家在二者的冲突中占据了上风,尽管 ICANN 似乎为国家提供技术上的指导,但国家对 ccTLD 有最终决策权,ICANN 无权限制国家管理其域名。

威思特诉伊朗伊斯兰共和国和 ICANN 一案中,原告辩称 ccTLD 是财产,并试图夺取伊朗的. ir 域名以获得赔偿。ICANN 在此案中否认国家顶级域名的财产性质,它认为:ccTLD 不是财产;即使 ccTLD 是财产,它们在哥伦比亚特区法院也不可扣押;即使它们是可扣押的,ICANN 也不能单方面转让它们;即使 ICANN 可以转让它们,这样做也会对互联网造成严重破坏;被告不拥有 ccTLD;即使被告拥有 ccTLD,《外国主权豁免法》也适用,ICANN 不能将其移交。[85]法院未肯定 ICANN 关于国家顶级域名并非财产的观点,但同意其不可扣押,一旦扣押可能会给互联网带来灾难性结果。[86]而在 2021 年 6 月 22 日,美国宣布对 36 个伊朗媒体域名进行了“扣押”,其中包括伊朗英文电视台(presstv. com)、伊朗世界新闻卫视(alalamtv. net)等,理由是这些域名的持有者“违反了美国的制裁措施”并“传播以美国为目标的虚假消息”。[87]威瑞信公司执行了该扣押,被扣网站将域名 presstv. com 迁移至 presstv. ir 才恢复了服务。[88]区别在于伊朗英文电视台网站不是 ccTLD,而是美国公司注册的通用顶级域名,在美国管辖范围内,表明美国并不认为伊朗对 presstv. com 的域名享有主权,但. ir 则不同,伊朗对其的主权使得美国法院认为扣押将导致互联网灾难性结果,否决扣押没收他国 ccTLD。

最后,域名国对域名网站的运行行使排他监管权。在实践中,网络平台运行者通过注册一国域名网站接受该国监管,域名国对域名的主权扩展至域名网站运行的排他监管权。例如,谷歌除 google. com 外在全球有着约 190 个当地网站,[89]以适应不同国家与地区对于网络平台的监管要求。而域名国监管失败使网络滥用问题日益严

重。由于国家及地区代码顶级域名注册政策取决于相应国家,有少数国家为了增加财政收入或其他原因,在域名注册上几乎不作限制,免费向任何人开放,但却缺乏对网站的监管能力,导致大量域名网站滥用问题。如新西兰的托克劳地区域名.tk 是最容易申请到的免费域名,曾经一度超过中国成为域名注册最多的 ccTLD,但它也是发起网络钓鱼攻击的第一大国家域名网站。[90] 2023 年 3 月 3 日,梅塔平台(Meta Platforms,Ins.)在美国法院对.tk 域名注册商提起诉讼,指控其侵犯网络占有权和商标权,新域名注册被叫停。[91]

(三)互联网企业的国家域名管理

全球性互联网企业通过在各国与地区注册 ccTLD 并运行对应网站,保证了对该国网络空间主权的尊重。全球性网站注册 ccTLD 以符合各国监管要求,如谷歌为符合各国的监管政策,在世界各地均拥有当地域名,其在执行当地监管要求时,多以基于域名的方法以避免其执行活动对他国主权造成影响。基于域名的方法根据用于访问搜索引擎的 ccTLD 来定制搜索结果。这意味着将删除特定搜索结果的效果限制在搜索引擎服务的一个或多个“特定国家”版本。谷歌的全球隐私顾问在对欧盟法院解释其基于域名的方式时称:“我们的搜索服务的国家版本是从每个国家的相关 ccTLD 提供的,比如法国的 google.fr 和意大利的 google.it。我们积极将欧洲用户从谷歌网站重定向到适当的 ccTLD,欧洲用户绝大多数使用这些服务。只有不到 5% 的欧洲用户使用 google.com,我们认为旅行者在其中占了很大一部分。”[92] 他们认为,目前基于域名的方法在实现这一目标方面相当有效,因为绝大多数用户(95%)坚持他们的“特定国家”版本。2012 年,马克斯·莫斯利向汉堡地区法院提起诉讼,要求谷歌不要在网络上提供某些照片。汉堡法院再次确定英国高等法院此前的认定,即这些照片侵犯了原告隐私权。[93] 莫斯利先生在汉堡法院获得的禁令仅限于德国“google.de”域名搜索。[94] 在 Foundem 案中,谷歌被指控滥用其主导市场力量,以不公平竞争的方式影响搜索结果。经过一年多的调查,谷歌提出了几项承诺,以解决委员会提出的竞争问题,但这些承诺仅限于“谷歌欧洲经济区搜索域”。[95] 谷歌作出的基于域名方式的承诺似乎让欧盟委员会很满意。[96]

国家顶级域名从一开始虽然由个人与私人实体进行管理,但随着互联网的迅速发展,国家将国家顶级域名纳入了主权管辖范围,并迅速借本国域名对相应的网络平台及连接的网络空间进行监管,使得全球性网络平台为尊重各国的网络空间主权而使用相应国家域名网站,显示国家域名成为各国行使网络空间主权的重要方式。

三、通用顶级域名与网络空间主权

相对于国家域名与国家主权的紧密联系,通用顶级域名的注册与管理呈现出明显的国际性,尽管在实践中,通用顶级域名网站运行者所在国家系网站的主要控制者,但不同国家对其连接的网络空间进行管辖的局面显然难以与领土主权的排他性相融合。

(一)通用顶级域名由国际组织管理

ccTLD 仅占所有域名的 40%,通用顶级域名更受注册人的欢迎。[97] 此类域名由 ICANN 负责管理,它们不与特定国家产生联系。[98].com 属于注册最多的通用顶级域名,另外还有表示企业的.net 及.firm,表示非营利组织的.org,表示销售公司的.store,突出网络活动组织的.web,突出文化、娱乐活动的.arts,突出消遣、娱乐活动的.rec,提供信息服务的.info,表示个人网站的.nom 等。基于历史原因,.edu,.gov,.mil 均由美国使用与控制,域名不由 ICANN 管理。由于通用顶级域名以行业特征为域名,故有人把域名体系划分为国内域与功能域。也有不少人将其划分为国内域与国际域。[99] 从管理机构来看,通用顶级域名系统由国际非政府组织 ICANN 管理,具有国际性。ICANN 指定注册局负责通用顶级域名的注册与管理。注册局是负责维护在某一顶级域名下注册的域名数据库的公司。目前,位于美国弗吉尼

亚州的威瑞信股份有限公司受 ICANN 委托作为注册局负责管理与维护. com 的域名数据库。虽然 ICANN 主要是互联网名称空间的政策制定者和协调者,但注册局和注册商的职能更具技术性。注册局和注册商又被称为“DNS 运营商”,因为他们直接对 DNS 进行更改,例如添加或删除域名。

ICANN 的核心使命是“确保互联网唯一标识符系统的稳定和安全运行”,特别是“协调制定和实施有关在通用顶级域中注册二级域名的政策”,同时促进 DNS 根名称服务器系统的运行和发展的协调。[100] ICANN 章程规定,ICANN 不得在其使命之外对在使用互联网唯一标识符的服务或此类服务所携带或提供的内容中施加规则和限制。[101] 登记滥用和使用滥用之间有一个传统的区别。前者“与注册商和注册局开展的核心域名相关活动有关”,而后者“涉及注册人在创建域名后对其域名的处理——注册人将域名用于的目的和/或注册人在其上运营的服务”。前者完全在 ICANN 的职权范围内,后者则被认为属于对网站运行的监管活动,不在 ICANN 章程规定的职权范围内。

随着 ICANN 新的顶级域计划的实施,互联网域名系统的通用顶级域名单从 22 个增加到数千个,2013 年 ICANN 制定了一系列权利保护措施,要求所有新的顶级域名注册机构提供多重保障,包括法律权利异议程序、商标索赔等预防措施、统一快速暂停程序、授权后争议解决程序和公共利益承诺争议解决程序等措施。授权后争议解决程序和公共利益承诺争议解决程序被怀疑可能对注册局与注册商施加技术中介责任。授权后争议解决程序使商标所有者能够对恶意行为、意图从侵权域名的系统注册中获利或以其他方式将通用顶级域名用于不当目的的注册运营商提出异议。尽管被批评商标所有人对注册经营者的经营方式提出索赔的权利可能会被推断为中介责任,但授权后争议解决程序已通过提供免责声明列表来防止中介责任。涉及商标法律权利异议的争议将由世界知识产权组织处理。[102] 申请的通用域名字符串违反了国际法原则公认的普遍接受的道德和公共秩序法律规范,则涉及公共利益承诺争议解决程序,该程序允许第三方对被视为违反“国际法关于道德和公共秩序的一般原则”或对广义社区有害的通用域名申请质疑,由 ICANN 进行管理。[103] 为实施这些额外的保障措施,ICANN 修改了其与域名注册局和注册商的标准协议,要求域名注册局和注册商遵守“所有适用法律”,并采取补救措施,如暂停域名等。[104] 尽管采取了以上措施,但由于受到 ICANN 职权所限,仍然缺乏普遍接受的关于如何处理使用滥用的框架。例如著名的反知识产权法的网络平台海盗湾即拥有通用顶级域名和国家顶级域名,在其持续侵犯知识产权的情况下,仅国家顶级域名国采取了没收域名的措施。2015 年 5 月 19 日,瑞典法院裁决扣押海盗湾的. se 域名。海盗湾即恢复使用了 piratebay. org。尽管海盗湾几乎输掉了每一场法律战,但他们的. com 和. org 域名都没有被没收。[105] 虽然很大程度上是因为他们的注册商在德国和澳大利亚,[106] 但同时表明了通用顶级域名滥用问题缺乏有效的解决工具。目前域名滥用最为严重的系通用顶级域名. live,域名滥用排名前 10 中有 8 个系通用顶级域名。[107]

(二)国家对通用顶级域名的监管

ICANN 缺乏国家所拥有的法律功能,在管理通用顶级域名的监管活动方面依赖国家进行管理。对域名的扣押与没收等强制措施上,ICANN 要求注册商须持有国家司法机构的裁决。由于缺乏国际法律工具,对于内容方面的滥用,DNS 运营商的做法差异很大。使用滥用包括两个方面:一是与 DNS 的安全性和稳定性密切相关的技术滥用(如网络钓鱼、恶意软件分发等);二是滥用内容(如虐待儿童、侵犯知识产权等)。注册局和注册商在规模、活动、治理结构方面非常多样化。此外,国家顶级域名和通用顶级域名之间在与国家法律、当局的关系方面的根本区别,

导致在 DNS 层面收到关于滥用的直接请求或行动命令时,特别是当它们来自跨境时,会采取非常不同的方法。出于法律确定性和法律责任的考虑,DNS 运营商倾向于简单地遵守权威决定,即只服从甚至要求其所在国法律实体的命令,很大程度上是担心接受外国法院的命令会鼓励政府以不可预测的方式行使域外权力。然而,国内法院关于通用顶级域名的裁决可能意味着将一个特定国家的立法强加给世界各地的注册人和用户,这会赋予许多 DNS 运营商所在的国家强大的权力。由于全球 58% 的通用顶级域名注册商是美国公司,[108]而注册域名最多的. com 的注册局在美国弗吉尼亚州,这使得在大多数情况下,特别是在执法方面,都处于美国的管辖之下。[109]基于美国案例较多,美国积累了足够的判例法,影响并塑造了通用顶级域名争议的解决规则。[110]无疑,美国对通用顶级域名享有巨大的影响力。

与国家顶级域名相似,通用顶级域名仍然具备知识产权的性质,但前者因对应国家与地区行使主权监管政策各异,后者则是国际组织通过多利益攸关方模式对其进行管辖,在 ICANN 职权范围以外,注册商、注册局所属国对域名享有管辖权,这似乎很类似于公海与公空亦或外层空间、国际海底区域,在缺乏国际规则的时候,国籍国拥有管辖权。这表明由于国际非政府组织的权力有限,即使被视为全球公域的域名管理,实质上还是需要国家权力的介入,而且仰仗的是少数大国,主要是美国的国家权力。有时候亦会因注册商与注册局的国籍国不同,出现管辖权冲突。

(三)通用顶级域名网络空间运行的多方管辖

尽管在域名方面,ICANN 与注册局及注册商国籍国拥有管辖权,但在域名运行上,ICANN 与注册商国籍国的管辖有限。域名运行地国通常享有完整的管辖权,即国家将其对物理存在的管辖权扩展到网络空间。然而目前国家基于主权的不仅可以是基于属地的,亦可以基于属人的,这将导致国家行使域外管辖权,出现国家网络空间管辖权的冲突。数据作为网络空间的内容层的珍贵价值使其成为国家争夺的重要资产。越来越多的国家要求互联网企业将数据中心设置在本地,主张数据主权,这使得美国难以控制全球数据。2018 年美国通过的《澄清海外数据合法使用法》(Clarifying Lawful Overseas Use of Data Act,以下简称《澄清法》)规定美国可通过控制者的属人管辖对位于域外数据实现管辖权,[111]美国企业在全球互联网行业的市场份额转变为美国数据主权的域外扩张。[112]与传统的域外立法管辖权受到执法管辖权极大限制不同,因美国互联网企业在全球数据上的主导地位使得美国可以在其领土上毫不费力地对域外数据行使执法管辖权。以属地为基础的数据主权与美国域外数据管辖权发生了激烈冲突。按照《澄清法》,美国的网络巨头须将在欧盟运行时收集的欧盟人员的数据保存在位于美国的服务器,但欧盟监管机构表示,在美国处理和存储欧盟个人数据违反了欧盟《通用数据保护条例》。[113]2023 年 5 月,梅塔平台因将脸书欧盟用户的个人数据转移到美国的服务器而违反了欧盟隐私法,被欧盟监管机构处以破纪录的 12 亿欧元罚款。[114]而该问题的根源在于美欧间关于数据获取规定的“法律冲突”,亦显示网络空间的多方管辖问题。

因此,通用顶级域名不仅受到 ICANN 管理,还受到注册局与注册商国管辖,在禁止域名滥用方面其网站内容亦会受到前三者的管辖,但域名网站的运行更多的是来自该域名拥有者、域名所在地国的管理。如欧盟《通用数据保护条例》第 3 条第 1 段便明确规定,在欧盟内部设立的数据控制者或处理者对个人数据的处理应适用该条例,还要求非欧盟数据控制者任命一名驻欧盟代表或设立分支机构以便保证欧盟的监管规则得以适用。[115]中国网络监管法规适用于在中华人民共和国境内建设、运营、维护和使用网络以及网络安全的监督管理。[116]法国政府的文件称“对位于其领土内的信息系统行使管辖权”,并在脚注中补充道,“通过覆盖国家领土的电子通

信网络或从归属于法国的 IP 地址操作或处理的连接对象/……/和内容”。[117]可以看到,通用顶级域名连接的网络空间的管辖权主要取决于其运行地的法律。通用顶级域名本身具有国际性,而与之相联系的网络空间仍然受到网络空间主权的影响,因运行地的差别适用不同国家法律。

四、全球性网络平台的实践

2000 年还没有脸书或其他社交媒体,谷歌只是一家小型初创公司。到 2010 年,互联网已经成为全球商业、金融和安全的核心基础设施。在过去的二十年里,网络平台已经成为我们生活中不可或缺的一部分,一些网络平台获得的主导地位,对国家权力、个人权利、社会和经济产生了巨大影响。它创造了新的强大的社会力量,挑战了政治稳定。作为回应,各国纷纷主张控制网络空间,网络空间主权同样影响着这些网络平台全球运行。在线网络空间管理权高度集中在少数数字平台上,这些平台与全球数亿用户中的绝大多数不在同一管辖范围内,[118]它们管理的网络平台受到不同国家网络主权的影响。一方面技术公司受到国家的监管,但另一方面技术公司又是国家在网络空间的管理者,国家执法机构的代理人。[119]通过颁布平台管理条例、处罚平台上的违反规则用户、执行国家法律等行为,网络平台实际已经成为准立法者、准裁判者与准执法者。[120]欧洲法院将谷歌视为类行政机构。[121]欧盟出台了一系列立法,限制网络平台行使网络空间准立法者与执法者的权力。目前全球性网络平台在网络空间执行各国法律的手段主要有两类,一类是基于域名进行监管,另一类是通过地理过滤的监管模式。这两种方法的主要好处是,国家会将其视为全球性网络巨头对该国网络空间主权的尊重,它们最大限度地减少了对其他国家主权的可能干扰。除这两类之外,还有受到广泛争议的全球网络执行方式。

(一)基于域名的方法

正如本文第二部分所述,谷歌适用基于域名的方法管理其在世界各国与地区的网络平台运行。它根据用于访问搜索引擎的 ccTLD 来定制搜索结果。为了服务当地用户,遵守当地的法律,谷歌除 google. com 外,在全球有着约 190 个当地网站,[122]使其能够按照各自国家及地区的法律、裁决及命令运行谷歌搜索引擎。谷歌基于域名执行各国及地区的监管规则,并试图说服欧盟、加拿大的法院,采取基于域名的方法来执行这些法院的裁决。[123]

(二)地理过滤的方法

最初,许多互联网公司使用地理地位工具来定位广告。[124]2004 年雅虎在受到美国起诉威胁后,该公司停止了在线赌场广告的运营,通过地理过滤将该措施仅限于美国领土。[125]地理过滤意味着使用软件来识别用户的地理位置。[126]这意味着无论使用哪个域名网站,用户的地理位置决定了用户获得的网页信息内容。地理位置工具可以保证不影响地理范围之外的法律适用与监管政策。[127]地理过滤工具的使用似乎提供了重要的好处。它使国家当局能够对外国行为行使管辖权,同时将其影响(至少在很大程度上)限制在自己的国家领土上。[128]地理过滤和基于域名的方法可协同工作,只有居住在监管国境内的互联网用户才会受到其实施的影响。如位于欧洲的网民访问 google. com,网站会自动重定向到他们自己所在国家域名网站的搜索引擎。在 M. et Mme X et M. Y v. Google France 一案中,尽管谷歌辩称其目前基于域名的方法应该被视为足够,但法院指出“谷歌法国公司……将禁令限制在 google. fr 上的链接是徒劳的,因为它并没有证明从法国领土链接到谷歌搜索引擎的其他域名扩展是不可能的”。法院称,“鉴于谷歌辩称,法院不能对 google. fr 以外的不针对法国公众的网站发布禁令,鉴于应由(谷歌)证明其运营的网站上出现的照片在被视为构成刑事犯罪的地区没有构成影响……”[129]这些陈述表明,法院拒绝了谷歌提出的基于域名的方式,但基于查询位置来源(而不是基于域名)的地理过滤就足够

满足法院的要求了。[130]

相对于域名管辖而言,地理过滤法进一步提高了执行的有效性。[131]然而,该方法也被批评者称,任何愿意投入一点时间和金钱的人通常都可以绕过它们重定位搜索,故地理过滤工具也不能保证是完全有效的。

(三)全球执行方式

与上述两类模式并存的是富有争议的全球执行模式。与物理领土的域外管辖一样,立法与司法域外管辖适用的是宽松许可原则。只要符合合理原则,立法与司法域外管辖权只要和被管辖事件建立了真实的联系,即被广泛接受为合法的。然而,执法管辖权仍被限制在本土,域外执行权需征得执行地国家的同意。[132]如脸书为遵守美国域外数据管辖的规定,将在欧盟内收集的数据转移到美国的服务器,因未经欧盟同意遭到欧盟的巨额罚款。[133]只有获得欧盟的同意(欧美间的安全港协议与后来的隐私盾协议及最新"欧盟 - 美国数据隐私框架")才可能避免域外执行带来的冲突。

在 Equustek Solutions Inc. v. Jack 一案中,加拿大法院指出,谷歌仅从 google. ca 中删除搜索结果不足以为原告提供有效救济。法院认为,"尽管谷歌在每个国家都有一个默认搜索的网站,但用户可以覆盖该默认搜索并访问其他国家的谷歌网站。为了有效,即使在加拿大,谷歌也必须屏蔽其所有网站上的搜索结果。"[134]欧盟法院在"谷歌西班牙被遗忘权案"中亦作出类似裁决。欧盟法院认为仅仅在谷歌西班牙的网页删除信息是不够充分的,谷歌作为搜索引擎的运营商有义务保证被遗忘权得以有效保护,即使在相关信息合法存在的网页上也须删除此信息。[135]这意味着欧盟法适用于包括 google. com 在内的全球性网页,表明欧盟以有效性为根据要求全球执行欧盟法。[136]

无论加拿大法院还是西班牙法院裁决谷歌全球执行其判决尚不侵犯他国主权,但如果他们未获得同意强制域外执行则可能侵犯了相关网站所在国的主权。如前所述,未经同意的域外执行侵犯一国的主权的规制同样适用于网络空间。谷歌数次对域外管辖提出异议,如其在欧盟法院提出因为 google. com 系国际领域,西班牙法院的裁决不能适用于 google. com,[137]还在加拿大法院主张加拿大将其裁决适用 google. com 侵犯了美国的主权,[138]甚至向美国加州地区法院提起诉讼,要求法院免除其遵守加拿大法院裁决谷歌从 google. com 搜索结果中删除某些网页的义务。[139]美国法院对谷歌的支持亦同样回应了全球执行方式与域外执行一样需要获得被执行地国的同意,否则全球适用方式无法得以实现。

有意思的是,欧盟法院在 2019 年 9 月 24 日否认了欧盟数据保护规则的全球适用,欧盟法院裁定,"被遗忘权"并不要求搜索引擎运营商在其所有域名上的搜索结果删除相关信息,而是在与所有成员国对应的搜索引擎版本上删除相关信息。必要时,采取措施,在满足法律要求的同时,有效防止或至少阻止互联网用户试图绕过搜索访问限制。[140]这意味着欧盟更倾向于适用基于域名的方式与地理过滤方式而非全球执行模式。

由于地理定位的改进,地理封锁可以更准确地发挥作用,并在更狭窄的地区和特定位置进行操作。足够可靠的工具的成本已经降低到互联网运营商可接受价格。[141]许多动机促使互联网运营商对用户进行地理定位;位置信息可以用于收集营销和其他目的的统计数据,提供本地化内容,支持网络安全措施,划分市场以进行价格区别,以及实现其他目的。渐渐地,地理位置不再是一个选择的问题,而是互联网法律合规的必要条件。随着地理定位工具的改进,各国在根据行为的影响规范互联网行为方面变得不那么犹豫;他们现在正在用基于消费地的监管取代基于行为来源的监管。因此,出于销售税、版权使用费、游戏许可证和个人数据保护等理由,各国现在根据互联网平台的客户所在地来规范互联网平台的行为,这意味着各国法律要求互联网平台对用户进行地理定位。[142]为了遵守国家法律,使用地

理屏蔽可能是必要的,甚至是必不可少的手段。[143]随着越来越多的义务要求互联网公司对用户进行地理定位的出现,用户获得信息的通道受到越来越多的限制,位于不同地理位置的用户对相同事项可能获得不一样的信息,互联网的碎片化已然发生。互联网搜索引擎已经在用户不知情的情况下根据国家的要求过滤了结果。信息通道虽然因此有一定阻碍,但互联网仍然保持全球互连。

从上述三种模式的实践来看,本国域名网站由本国监管并适用本国法律已经毫无争议;基于地理位置的过滤方式则通过技术手段强制位于该国领土的用户获得符合该国法律的信息通道;而强制全球适用或在非本国管辖的域名网站适用该国法律将构成域外适用,可能引发国家间法律适用冲突。全球性科技公司已经广泛适用域名方式与地理位置过滤方式,基于用户的 IP 地址,或将全球性网站转入本国域名网站,[144]或根据地理位置过滤执行该 IP 地址所在国的法律,使得域名连接网络空间物理领土化。[145]这不仅明确显示了网络监管以域名和地理位置两个标准来进行,同时显示网络空间主权直接影响着全球性网络平台的运行模式。因此,一些专家认为网络空间已经出现巴尔干化的分裂状态。然而互联网依然全球相连,巴尔干化对信息连通性和经济利益造成的损害将使大多数国家望而却步。[146]显然网络空间碎片化与整体性、主权与全球公域并存系必然,但亟需制定相关国际规则以防止网络空间碎片化加深,这包括网络空间全球治理以及调整网络空间主权与网络空间全球公域的国际规则。

五、网络空间主权边界标准

领土主权通常以领土边界为限,网络空间在国家声称主权的声明中却并无明确的边界,这使得网络空间主权行使的边界相对模糊,网络空间碎片化日趋严重,网络空间被担心巴尔干化,网络空间主权的无序状态与网络空间全球治理局限性使网络空间全球性面临挑战。

(一)以域名为网络空间主权边界

通过域名判断一国领土极为方便并极具可操作性,由前文来看,国家域名下的网站通常代表着该国的主权,特别是政府网站成为一国网络领土的明确象征。在网络攻击事件中,一国政府网站常因为国家间争端被黑客攻击。如 2022 年 1 月,乌克兰的政府网站被攻击破坏;[147]中国政府网站也被经常性攻击。[148]然而,占据互联网网站 60% 的通用顶级域名网站并无国家域名显示,但仍然受到国家管辖,常常出现多个国家对通用顶级域名网站连接的网络空间享有管辖权,且 ICANN 亦对通用顶级域名及网站运行享有管辖权,此类域名下网络空间的法律地位很难通过域名本身进行明确。对于通用域名网站而言,复杂的多方管辖使得大多数用户无法了解哪个国家或哪个实体在对该网络行使管辖权。就目前而言,仅以域名来判断一国网络空间主权并不现实。

(二)分层划分网络空间主权边界

在网络空间问题上备受瞩目的《塔林手册 2.0》将网络空间划分为基础设施、逻辑、基础资源、数据,以及社会 5 个层面,针对这 5 个层面分别探讨了主权的适用。网络基础设施层与社会层毫无疑问因其实际存在于领土上应受国家主权管辖,逻辑层是一种网络设备之间的信息流交换,其中包含相互之间的协议、通行的应用以及用于交换的基本数据,对于逻辑层国家可以通过某些网络协议进行管理,对于基础资源层(电子频率及根域名资源)则采取“全球公域”的思路,在这一层面抑制国家主权的适用性。[149]《塔林手册 2.0》称国家通过物理层、逻辑层、社会层实现了网络空间的主权。[150]这种划分将网络空间分层化,使得网络空间主权边界主要以物理领土边界为准。由于网络设备与个人通常位于不同的物理领土,这使得网络空间主权领域相互交叉,令网络空间主权边界极为复杂与模糊。这种分层化的方式使得网络空间的不同层面属于不同领域,网络空间各层面法律地位各异的状态令

网络空间主权边界如迷宫一样复杂,难以改变网络空间碎片化的趋势。由于目前分层划界仅系部分国家的实践与学者的论述,缺乏分层划界的规则,这将加剧各国对网络空间监管的扩张,加深国家间互不信任、网络安全恶化及网络空间的军事化和武器化。

尽管分层划界对于大部分用户而言过于复杂,但目前在无明确划分边界的情况下,由于有实践的支持,故具有现实意义。这一现实提出了关于最有效的治理模式的问题。分层治理必然存在分层之间的协调治理,需要在国家主权与全球性之间进行平衡。目前网络空间全球治理在多边治理与多方利益相关者主义之间的争议上勾勒出一幅相当复杂的网络空间治理图景。网络空间的基础资源层中的根域名资源被视为全球公共产品,通过国际非政府组织 ICANN 以多利益攸关方模式进行管理。而联合国大会在探索网络国际治理更多元的模式。联合国大会裁军与国际安全委员会(第一委员会)根据联合国秘书长的指令于 2004 年建立联合国信息安全政府专家组(UN Group of Governmental Experts on Developmentsin the Field of Information and Telecommunications in the Context of International Security),服务于联合国建立一个“开放、安全、稳定、无障碍及和平的信息通讯技术环境”。该联合国专家组是由国家主导,在协商一致的基础上编写关于网络空间安全的报告,提交给联合国大会作为下一届专家组的工作基础。目前,该机制下已经组织了六届专家组,发布了四份共识报告。[151]在政府专家组编写报告的同时,另一个多利益攸关方模式亦同时展开。2005 年联大组织召开的突尼斯会议通过的《突尼斯信息社会议程》对互联网多利益攸关方治理模式进行了具体阐释,要求联大组织召开新的多利益攸关方政策对话论坛,联大因此在 2006 年组织联合国互联网治理论坛,建立了由来自五个联合国区域集团的政府、私营部门、民间社会、学术和技术社区的 50 ~ 55 名成员组成的多利益攸关方咨询专家组。该论坛旨在将来自不同利益攸关者群体的人们平等地聚集在一起,讨论与互联网相关的公共政策问题,促进不同机构、群体之间的相关交流,提出建议,加快发展中国家互联网建设等,但并无谈判结果,只是通知和激励公共和私营部门的决策者,有助于就如何最大限度地利用互联网机会、应对出现的风险和挑战达成共识。[152]在 2018 年,联大建立了名为“从国际安全角度看信息和电信领域的发展”的开放式工作组,并邀请所有联合国会员国参加,该工作组组织了多利益攸关方协商会议,与联合国政府专家工作组共同推动全面的网络空间国际法律的形成。[153]然而这些活动仅承认了网络主权的存在与网络空间需要全球治理,但并未推出关于网络空间主权与全球公域分层治理及相关协调规则。

(三)过境通行模式

一些学者尝试将国际海洋法的划界模式借用于网络空间。与网络空间类似,海洋对国家的发展有着重大影响,而海洋的流动性、整体性与陆地领土存在着明显冲突,使海洋国际规则需要突破陆地领土与国际区域划分的传统规则。《联合国海洋法公约》把海洋划分为领土、国际区域(公海)、第三类区域、人类共同继承财产等不同性质的区域。由于海洋的整体性与其在国际航运中的重要地位,主权在海洋领土区域受到了重大限制,如外国船舶与飞机在群岛水域的群岛海道通行权、外国船舶与飞机在用于国际航行海峡中领海的过境通行权、外国船舶在领海的无害通过权均无需领土主权国的同意。[154]而在国家陆地主权延伸区域的大陆架,沿海国仅享有主权权利,沿海国 200 海里以外的外大陆架的划定受到联合国大陆架界限委员会划界建议的限制,且与公海重叠,沿海国主权权利受到其他国家的权利与自由的限制。[155]可以看到主权在不同领域调整的灵活性,它甚至可以与国际区域融合创造出新区域的现实。网络空间必然以其特性创造新兴区域与新兴规则,改变目前领土、第三类区域、国际区域、人类共同继承财产的划分。有学者提

出网络空间的公共和自由访问部分就像连接硬件所在主权领土的国际海峡,适用过境通行制度,而网络空间中受密码保护的私人或公用网络应被视为内水,在这里国家有完全的领土主权。[156]该理论认为,在国际海峡中,不止一个国家的领海重叠。过境通行制度允许所有船舶和飞机航行和飞越自由,其唯一目的是使船舶和飞机在公海或专属经济区的一部分与公海或专属经济区的另一部分之间的海峡持续迅速过境。一旦信息被发送到网络空间,在最终到达之前,几乎不可能判断它何时从一个主权国家传递到另一个主权国家。尽管每台计算机、服务器、光纤电缆和电线等都位于受其他监管框架约束的某个地方,但数据包在互联网上传播的路径在很大程度上超出了用户的控制,并且可能在从发送者到接收者的过程中经过许多不同的主权管辖区。“过境通行”允许电子以正常运行模式过境他国的网络空间。[157]如果按照物理存在延伸网络主权的字面含义来解释,那么某个特定的网络空间都将有若干个国家行使主权,主张过境通行制度适用于网络空间可使国家在保证网络空间信息自由流动的同时,又让国家可以分别在其网络空间进行监管;由于用于国际航行的海峡两端连接着公海及专属经济区,过境通行适用于连接着公共网络空间的国家网络空间。[158]该理论尝试用过境通行来解释网民进入全球网络的自由,能够符合网络空间既有主权又相互连接的现实,但却未解释网络空间的全球公域与网络空间主权的边界,亦难以解释当域外用户通过位于域外的设备前往一国域名网站时受到该国监管的情形。可以看到,通过物理设备主张网络空间主权时错综复杂的主权交叉的情况。

(四)域名与物理设置结合分界模式

网络空间无疑如同大海一样,是相互连接在一起的整体,信息像海水一样自由流动,然而维持信息自由流动部分根域名资源系全球公共产品,如同国际海底区域一样由国际组织进行管理。或许我们不用把网络空间限制于用于国际航行的海峡,可以将网络空间视为汪洋大海,那里目前各国均声称基于其对领土上的物理存在与人员的主权延伸到网络空间,如同海洋的主权及主权权利来自陆地(即陆地统治海洋原则),网络空间的主权来自物理空间,同样可以如同海洋有着主权区域、第三类区域、国际区域、全球公域等不同性质的区域的划分。网络空间主权也如同海洋主权一样受到重大限制,就像外国船舶可以过境通行、无害通过、自由航行一样。目前国家对网络空间主权系物理领土上的物理存在的延伸,实际上与海洋划界中的“陆地统治海洋”、空气空间的划界取决于陆地与海洋有着类似逻辑。但是否应划分内网、领网、专属网、国际网、全球公域等区域则需要国家合意。尽管在实践中域名并未成为国家主张网络空间主权的标准,但事实上国家域名网站已由域名国行使排他管辖权,且域名是最为简单且清晰的判断网络归属的方式。基于操作简单宣示效果清晰明了,这样的方式在领土主权与管辖的宣示上极为常见,船舶上的旗帜、航空器上的字母均在难以划界的海洋与天空中起到国籍宣示的效果。因此,笔者将二者相结合提出域名与物理设置相结合模式,可使网络空间的主权边界清晰明了,亦使国家能够对域名网站下的网络空间进行实际控制,可大幅度减少网络安全隐患。

如同《联合国海洋法公约》《国际民用航空公约》明确海洋与空气空间的主权领域,网络空间的主权边界亦需要条约来明确。条约可将域名与物理设施地相结合,明确采用国家域名严格领土登记制度,将注册人国籍与服务器位于领土范围内作为硬性登记条件,以杜绝“方便域名”导致缺乏监管所带来的网络安全问题。此类网络空间属于领网,在向全球开放的同时,不管是运营者还是进入该网站的用户均将受到域名国的管辖。尽管有人认为网络的自由进出不是领网的本质,然而,领网的自由进出事实上是由国家控制的,因为它可以随时被国家关闭,[159]因此,其自由出入是在国家默许同意的前提下,而

同意显然是行使主权的一种方式,而在特殊情况下,国家自然有权进行中断,这与无害通过权可在特定条件下中断是类似的。[160]

而在通用顶级域名网站的管辖方面则根据注册人与服务器所在地明确该国为主要管辖权国。而注册商、注册局所属国可以行使部分管辖权,ICANN 亦享有部分管辖权。基于通用顶级域名的复杂性,同时还需规定例外情形。例外一为因历史原因实际成为一国网站的.edu,.gov,.mil,此类网站可作为例外情形与国家顶级域名网站一样成为领网。另一类例外属于国际组织的域名网站,可将其视为国际网络空间,豁免于该国际组织及其服务器所在地国的管辖,其运行应由该组织自行负责并承担相应的法律责任,由 ICANN 就域名进行维护与管理。还需设置一个解决网络空间国际争端的国际实体或赋权现有国际组织(如国际电信组织)设立的专门机构。另外还需明确内网的范围包括那些未接入互联网的局域网与那些面向特定群体需要用户名与密码并受一国主权管辖的网络空间,并使其区别于领网,明确此类网络空间需要明示同意才能进入。而根域名资源与电子频率等则通过条约明确为全球公域,由专门的国际组织或国际非政府组织进行管理。

正是由于网络空间全球连通,为国家、实体及个人提供了前所未有的获取其他国家领土上信息和物体的机会。网络空间使它们摆脱了以前可能阻碍访问的许多地理和物理限制,一方面它极大地降低了信息通信成本,深刻地改变了人类社会的方方面面,成为造福人类的重要新渠道。另一方面,因为它的全球性使网络攻击的成本很低且发现肇事者的难度极大,网络安全问题突出。如前文所述,主权具备最高性的同时,也是受限制的,网络空间主权也同样受到限制。网络空间的全球性是网络空间的主要特质,网络空间主权受到网络空间全球性的限制,主权规则在网络空间的适用不能将网络空间巴尔干化。国际社会还应通过条约明确网络空间全球性对主权的具体限制,在明确领网、国家管辖网、国际网络空间等不同领域的同时,确保网络空间主权及管辖权的行使不影响全球用户在所有领域的全球连通,使网络空间继续发挥造福人类重要渠道的作用。因此有必要在条约中明确国家行使网络空间主权的同时,确保网络空间的全球连通,换言之,需开放网络空间,使信息自由流动,仅在例外的情况下可以限制网络空间的自由进出。就当前的实践来看,例外的情况主要集中在国家安全与人权隐私及商业秘密等。[161]通过例外安排实现信息自由流动与国家安全、公共利益有机统一。[162]

由于缺乏明确网络空间法律地位的国际法与协调和指导国家行动的有效机制,导致国际社会无法减少摩擦和主权控制的扩散。联合国尽管为建立这样一个机制提供了合理场所,但尚需主要网络大国对此承担起领导责任,承认所有国家的利益并不一致,并明确网络空间主权的边界,以最大限度地减少对全球连通性的损害。[163]中国作为网络空间的新兴国家,一贯主张网络空间的主权,认为网络空间主权系国家领土主权的延伸,并积极在网络空间打造命运共同体,反对网络霸权。要实现该目标,中国应大力鼓励中国科技公司在网络信息科技的技术突破,支持中国企业经营国际域名网站,削弱美国网络霸权,同时要坚持网络空间主权原则,并利用好中国互联网企业与学术界,积极加入网络空间国际造法,努力在联合国框架下推动创立一个能够取代“美国治理”的国际网络空间治理机制,促使网络空间中的全球公域真正成为人类共同财产。

六、结　论

当前网络空间高度融入人类社会的各个方面,对于国家有着难以估量的影响,各国极为重视网络空间的权力,而且有能力通过有效的技术及其领土上的信息基础设施与相关人员对网络空间进行实际控制。各国以不同的理由在不同程度上对网络空间进行监管。尽管国家对其国

家域名及其连接的网络空间能够行使排他的主权,但在通用顶级域名方面,由 ICANN 以多利益攸关方模式对域名进行管理,通常由注册局、注册商所在国在域名的没收及扣押上享有管辖权,而对其所连接的网络空间的日常监管则取决于网站运行者所在国。全球性网络平台尊重国家的网络空间主权,简单地通过基于域名方式和地理过滤方式,拒绝全球适用模式,保证在不同地域适用该地域的国内法。网络空间主权的普遍接受和缺乏相应的国际规则导致网络空间碎片化严重,充斥着脱钩、监管、军事化、不信任和武器化,影响并威胁网络空间互联互通所带来的巨大利益。无论是域名模式还是以物理存在为基础的分层划分网络空间及过境通行模式都难以在反映现实的同时促进网络空间的全球性。接受网络空间主权存在的现实,将域名与物理存在相结合,明确网络空间的不同区域可能使复杂的网络空间主权与全球性的迷宫清晰化,并大幅提高网络安全、降低碎片化程度。如同国家通过了相当长的时间达成《联合国海洋法公约》一样,国家亦需要时日达成网络空间国际条约。当前中国作为网络新兴国家应致力于让互联网更好造福人类,积极推动国际社会携手进行国际造法,通过条约明确网络空间的区域划分,在尊重网络主权的同时,促进国家与国际组织及其他利益攸关方积极合作以保证网络空间全球性与安全,共同构建更加公平合理、开放包容、安全稳定、富有生机活力的网络空间。要承认所有国家的利益并不一致,未来的网络空间国际条约应破除国家行为对互联网全球连通的障碍,以最大限度地减少对全球连通性的损害,减少网络空间中侵犯主权干涉他国内政等国际不法行为,降低网络滥用行为,提高网络安全,发挥网络空间所带来的优势,造福人类社会,为构建网络空间命运共同体提供规则支撑。

注释:

〔1〕Georgios I. Zekos, "State Cyberspace Jurisdiction and Personal Cyberspace Jurisdiction", *International Journal of Law and Information Technology*, Vol. 15, No. 1, 2007, pp. 1 – 37.

〔2〕National Cybersecurity Strategy, MAR 2023, https://www.whitehouse.gov/wp – content/uploads/2023/03/National – Cybersecurity – Strategy – 2023.pdf.

〔3〕美国国防部在 2024 财年投入网络空间行动 135 亿美元,比去年的 75 亿美元增加了近一倍,详见 https://www.whitehouse.gov/wp – content/uploads/2023/03/budget _ fy2024.pdf;2022 年美国国土安全局宣布拨款四年 10 亿美元资助各州应对网络安全,2023 年美国国土安全局宣布增加拨款 3.749 亿美元资助各州应对勒索软件的不断攻击,详见 DHS Announces Additional $374.9 Million in Funding to Boost State, Local Cybersecurity, https://www.dhs.gov/news/2023/08/07/dhs – announces – additional – 3749 – million – funding – boost – state – local – cybersecurity#: ~ : text = WASHINGTON% 20% E2% 80% 93% 20Today% 2C% 20the% 20Department% 20of% 20Homeland% 20Security, threats% 20to% 20their% 20critical% 20infrastructure% 20and% 20public% 20safety。

〔4〕Report of Cyberspace Solarium Commission, March 2020, https://www.solarium.gov/.

〔5〕U. S. Army Cyber Command, https://www.arcyber.army.mil/About/About – Army – Cyber/.

〔6〕〔148〕《外交部:中国政府部门每天都遭受海量网络攻击,大多源自美国》,观察者网, https://www.guancha.cn/politics/2023_07_14_700917.shtml。

〔7〕〔151〕"Incremental Progress or Circular Motion? – The UN Group of Governmental Experts (UNGGE) Report 2021", June 12, 2021, https://policycommons.net/artifacts/1901072/incremental – progress – or – circular – motion/2652249/.

〔8〕Tanja E. Aalberts, *Constructing Sovereignty Between Political and Law*, New York: Routledge, 2012, p. 20.

〔9〕Melea Lewis, Charles Sampford and Ramesh Thakur, "Introduction", *Re – Envisioning Sovereignty, The End of Westphalia?* ed. by Trudy Jacobsen, Charles Sampford and Ramesh Thakur, Ashgate Publishing Ltd, 2008, p. 1.

〔10〕Yang Yonghong, *Sovereignty in China's Perspective*, Peterlang, 2017, p. 12.

〔11〕Helmut Steinberger, "Sovereignty", *Encyclopedia of Dispute Installment 10*, Elsevier, 1987, pp. 397 – 418.

〔12〕2005 World Summit Outcome, paras. 138 – 139, https://www.ilo.org/wcmsp5/groups/public/ – – – dgreports/ – – – integration/documents/meetingdocument/wcms_079439.pdf.

〔13〕Martti Koskenniemi, "The Future of Statehood", *Harvard International Law Journal*, Vol. 32, 1991, pp. 397 – 410; Wouter Werner, "From Justus Hostis to Rogue State", *International Journal for the Semiotics of Law*, Vol. 3, 2004, pp. 74 – 92.

〔14〕Luzius Wildhaber, "Sovereignty and International Law", in

Structure and Process of International Law: Essays in Legal Philosophy Doctrine and Theory, eds. by R. S. J. MacDonald and D. M. Johnston, The Hague: Martinus Nijhoff, 1983, p. 441.

〔15〕〔德〕狄特玛尔·布洛克:《全球化时代的经济与国家——从民族的国民经济到全球化的世界经济》,张世鹏、殷叙彝编译:《全球化时代的资本主义》,北京:中央编译出版社,1998年,第100-117页。

〔16〕〔美〕阿兰·伯努瓦:《面向全球化》,王列、杨雪冬编译:《全球化与世界》,北京:中央编译出版社,1998年,第2页;〔英〕菲利普·桑斯:《无法无天的世界——当代国际法的产生与破灭》,单文华等译,北京:人民出版社,2011年,第1-21页。

〔17〕《联合国海洋法公约》第58条第2项规定:第八十八至第一一五条以及其他国际法有关规则,只要与本部分不相抵触,均适用于专属经济区。另参见杨永红:《从北极日出号案析沿海国在专属经济区的执法权》,《武大国际法评论》2017年第3期。

〔18〕Akbar Adibi, Homayoun Habibi, "The Challenge of the Economic Independence and the Sovereignty of States: A Review of the Problem of Legitimacy of Economic Sanctions in the Reality of the International Legal Order", *Russian Law Journal*, Vol. 5, 2017, p. 113.

〔19〕〔155〕《联合国海洋法公约》第76、77、78条。

〔20〕〔154〕《联合国海洋法公约》第17、38、53条。

〔21〕Andrew Liaropoulos, "Exploring the Complexity of Cyberspace Governance: State Sovereignty, Multi - stakeholderism, and Power Politics", *Journal of Information Warfare*, Vol. 15, 2016, pp. 14 - 26.

〔22〕Jack Goldsmith, "The Failure of Internet Freedom", Knight First Amendment Institute, 3 (June 13, 2018).

〔23〕Fergus Hanson, "Internet Freedom: The Role of the U. S. State Department", Brookings, October 25, 2012, https://www.brookings.edu/research/internet - freedom - the - role - of - the - u - s - state - department.

〔24〕Kate Klonick, "The New Governors: The People, Rules, and Processes Governing Online Speech", *Harvard Law Review*, Vol. 131, 2018, p. 1598.

〔25〕Jack L. Goldsmith, "The Internet and the Abiding Significance of Territorial Sovereignty", *Indiana Journal of Global Legal Studies*, Vol. 5, No. 2, 1998, p. 475.

〔26〕Michael N. Schmitt, ed., "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations", 2017, pp. 15 - 16.

〔27〕〔30〕〔31〕Jack Goldsmith, Tim Wu, *Who Controls the Internet? Illusions of a Borderless World*, Oxford University Press, 2006, pp. 50 - 58, 68, 50 - 58.

〔28〕Sean Kanuck, "Sovereign Discourse on Cyber Conflict Under International Law", *Texas Law Review*, Vol. 88, 2010, pp. 1571, 1585 - 1590.

〔29〕〔32〕Sean Watts, Theodore Richard, "Baseline Territorial Sovereignty and Cyberspace", *Lewis & Clark Law Review*, Vol. 22, 2018, pp. 771 - 840.

〔33〕Vasudha Krishnamurthy, "Cyber - Attacks in Outer Space: A Study", *Supremo Amicus*, Vol. 20, 2020, pp. 584 - 595.

〔34〕Kristen E. Eichensehr, "The Cyber - Law of Nations", *Georgetown Law Journal*, Vol. 103, 2015, pp. 317 - 325.

〔35〕Elizabeth C. Hanson, *The Information Revolution and World Politics*, Lanham: Rowman & Littlefield, 2008, pp. 57 - 61.

〔36〕〔70〕〔110〕Marketa Trimble, "Territorialization of the Internet Domain Name System", *Pepperdine Law Review*, Vol. 45, No. 4, April 2018, pp. 623 - 684.

〔37〕"Federal Management Regulation; Internet GOV Domain", Government Publishing Office, https://www.gpo.gov/fdsys/pkg/FR - 2003 - 03 - 28/html/03 - 7413.htm.

〔38〕"FAQs", ICANN, https://www.icann.org/resources/pages/faqs - 2014 - 01 - 21 - en. See also Marketa Trimble, "Targeting Factors and Conflict of Laws on the Internet", *Review of Litigation*, Vol. 40, No. 1, 2020, pp. 1 - 60.

〔39〕〔50〕〔79〕〔81〕Marc Watkins, "Government Regulation of the Dot - ca Domain Name Space", *University of Ottawa Law & Technology Journal*, Vol. 2, No. 1, 2005, pp. 145 - 172.

〔40〕〔45〕Peter K. Yu, "The Origins of ccTLD Policymaking", *Cardozo Journal of International and Comparative Law*, Vol. 12, 2004, p. 387.

〔41〕"Intellectual Property on the Internet: A Survey of Issues", WIPO, 2002, p. 60.

〔42〕Milton L. Mueller, *Ruling The Root: Internet Governance and the Taming of Cyberspace*, MIT Press, 2002, pp. 39 - 40.

〔43〕〔44〕Jon Postel, "Domain Name System Structure and Delegation", Network Working Group, Request for Comment, No. 1591, 1994.

〔46〕GAC原则(2000年)第5.1部分规定:相关政府或公共机构最终代表ccTLD授权的国家或地区人民的利益。因此,相关政府或公共机构的职责是确保ccTLD的管理符合公众利益,同时考虑到公共政策和相关法律法规的问题。5.2部分规定:政府或公共当局对公共政策目标负有责任,例如:透明度和非歧视性做法;为各类用户提供更多的选择、更低的价格和更好的服务;尊重个人隐私;消费者保护问题。考虑到保护这些利益的责任,政府或公共当局对其各自的ccTLD保持最终政策权威,并应确保其运作符合国内公共政策目标、法律法规、国际法和适用的国际公约。See Dwi Elfrida Martina Simanungkalit, "Evaluating Governance and Market of Country Code Top - Level Domain (ccTLD): Lessons for Indonesia's ccTLD. id", 2013, https://scholarworks.umass.edu/cppa_capstones/25/。

〔47〕Document: WSIS - 05/TUNIS/DOC/6 (Rev - 1) - E, https://ininet.org/document - wsis - 05tunisdoc6rev - 1 - e.html.

〔48〕Document: WSIS - Il/PC - 3/DT/10 (Rev. 4) - E, https://www.itu.int/net/wsis/docs2/pc3/working/dt10rev4 - zh.pdf.

〔49〕National Telecommunications and Information Administration, "U. S. Principles on the Internet's Domain Name and Addressing System", https://www. ntia. gov/sites/default/files/publications/usdnsprinciples_06302005_0. pdf.

〔51〕〔66〕〔67〕〔68〕Milton L. Mueller, Farzaneh Badiei, "Governing Internet Territory: ICANN, Sovereignty Claims, Property Rights and Country Code Top - Level Domains", *Columbia Science and Technology Law Review*, Vol. 18, No. 2, Spring 2017, pp. 435 - 491.

〔52〕Robert Uerpmann - Wittzack, "Principles of International Internet Law", *German Law Journal*, No. 11, November 2010, pp. 1245 - 1263; Marketa Trimble, "Territorialization of the Internet Domain Name System", *Pepperdine Law Review*, Vol. 45, No. 4, April 2018, pp. 623 - 684; Gregory R. Hagen, "Sovereign Domains and Property Claims", *International Journal of Law and Information Technology*, Vol. 11, No. 1, 2003, pp. 1 - 39.

〔53〕Marketa Trimble, "Territorialization of the Internet Domain Name System", *Pepperdine Law Review*, Vol. 45, No. 4, April 2018, pp. 623 - 684; Milton L. Mueller and Farzaneh Badiei, "Governing Internet Territory: ICANN, Sovereignty Claims, Property Rights and Country Code Top - Level Domains", *Columbia Science and Technology Law Review*, Vol. 18, No. 2, Spring 2017, pp. 435 - 491; Marc Watkins, "Government Regulation of the Dot - ca Domain Name Space", *University of Ottawa Law & Technology Journal*, Vol. 2, No. 1, 2005, pp. 145 - 172.

〔54〕Kremen v. Cohen, 325 F. 3d 1035 (9th Cir. 2003).

〔55〕Satyam Infoway Ltd. v. Sifynet Solutions Pvt. Ltd., (2004) 2 S. C. R. 465.

〔56〕OBG Limited v. Allan, [2007] UKHL 21.

〔57〕Mold. ca Inc. v. Moldservices. ca Inc., (2013) (Ont. Sup. Ct. of J.) No. CV - 13 - 480391.

〔58〕Paeffgen Gmb H v. Germany, 8 - 9 Eur. Ct. H. R. (2007).

〔59〕〔61〕〔62〕〔63〕Network Solutions, Inc. v. Umbro International, Inc., 529 S. E. 2d 80 (Va. 2000).

〔60〕Stockholms Tingsrätt, Avdelning 5 DOM (DELDOM), https://Internetstiftelsen. se/docs/Stockholms - TR - B - 6463 - 13 - Deldom - 2015 - 05 - 19_avidentifierad. pdf.

〔64〕Dorer v. Arel, 60 F. Supp. 2d 558, 561 (E. D. Va. 1999).

〔65〕Lockheed Martin Corp. v. Network Solutions, Inc., 194 F. 3d 980 (9th Cir. 1999).

〔69〕Canadian Presence Requirements For Registrants, Version 1. 3. CIRA, https://static. cira. ca/policy/canadian - presence - requirements - for - registrants. pdf.

〔71〕Regulation (EC) No 733/2002 of the European Parliament and of the Council of 22 April 2002 on the implementation of the . eu Top Level Domain (Text with EEA relevance).

〔72〕Commission Regulation 874/2004 of 28 April 2004, O. J. 2004 L 162/40, last modified by Commission Regulation 560/2009 of 26 June 2009, O. J. 2009 L 166/3.

〔73〕Commission, "Call for Expressions of Interest for the Selection of the . eu TLD Registry", Notice of 3 September 2002. O. J. 2002 C 208/6.

〔74〕Robert Uerpmann - Wittzack, "Principles of International Internet Law", *German Law Journal*, Vol. 11, No. 11, November 2010, pp. 1245 - 1263.

〔75〕Gregory R. Hagen, "Sovereign Domains and Property Claims", *International Journal of Law and Information Technology*, Vol. 11, No. 1, 2003, pp. 1 - 39.

〔76〕"Registration and Naming in the. IE Namespace", IE Domain Registry, § 2, p. 4, 2018, https://www. iedr. ie/uploads/IEDR - RegistrationNaming - . IE - Namespace. pdf.

〔77〕"The Domain Name Industry Brief", Vol. 16, N0. 4, 2019, https://dnib. com/media/downloads/reports/pdfs/2019/domain - name - report - 2019Q3. pdf.

〔78〕〔141〕Marketa Trimble, "Targeting Factors and Conflict of Laws on the Internet", *Review of Litigation*, Vol. 40, No. 1, Fall 2020, pp. 1 - 60.

〔80〕Ashley La Bolle, "Why are ccTLDs so complicated?", July 18, 2017, https://www. epag. de/why - are - cctlds - so - complicated/.

〔82〕ICANN, "Resources for Country Code Managers", https://www. icann. org/resources/pages/cctlds - 21 - 2012 - 02 - 25 - en.

〔83〕ICANN, "Redelegation of . us Country - Code Top - Level Domain", https://www. icann. org/fr/announcements/details/redelegation - of - us - country - code - top - level - domain - 19 - 11 - 2001 - en.

〔84〕"IANA Report on Redelegation of the . DM Top - Level Domain", https://www. iana. org/reports/2007/dm - report - 31jul2007. html.

〔85〕〔86〕Weinstein v. Islamic Republic of Iran, No. 14 - 7193 (D. C. Cir. 2016).

〔87〕"United States Seizes Websites Used by the Iranian Islamic Radio and Television Union and Kata'ib Hizballah", https://www. justice. gov/opa/pr/united - states - seizes - websites - used - iranian - islamic - radio - and - television - union - and - kata - ib.

〔88〕"U. S. seizes websites used by Iranian news outlets", http://www. xinhuanet. com/english/2021 - 06/23/c_1310023367. htm.

〔89〕〔122〕Google, https://www. google. com/supported_domains.

〔90〕〔97〕"The Domain Name Industry Brief", Vol. 17, No. 1, March 2020, https://www. verisign. com/assets/domain - name - report - Q42019. pdf.

〔91〕Alfonso Maruccia, "Meta is suing Freenom, cybercrimi-

nals' favorite domain registrar", https://www.techspot.com/news/97856-meta-suing-freenom-cybercriminals-favorite-domain-registrar.html.

〔92〕Peter Fleischer, "Response to the Questionnaire addressed to Search Engines by the Article 29 Working Party regarding the implementation of the CJEU judgment on the 'right to be forgotten'", https://storage.googleapis.com/transparencyreport/faqs/eu-privacy/Article%2029%20Questionnaire%202014-07-31.pdf.

〔93〕Max Mosley v. News Group Newspapers Ltd., [2008] EWHC 1777 (QB), http://www.bailii.org/ew/cases/EWHC/QB/2008/1777.html.

〔94〕Case 324 O 264/11[2014], at paras 61 and 69, http://openjur.de/u/674344.html.

〔95〕Case COMP/C-3/39.740, Foundem and others v. Google, 2013, http://ec.europa.eu/competition/elojade/isef/case_details.cfm? proc_code=1_39740.

〔96〕Joaquín Almunia, "Statement on the Google investigation", February 5, 2014, http://europa.eu/rapid/pressrelease_SPEECH-14-93_en.htm.

〔98〕〔127〕Yulia A. Timofeeva, "Establishing Legal Order in the Digital World: Local Laws and Internet Content Regulation", *Journal of International Commercial Law and Technology*, Vol. 1, No. 1, 2006, pp. 41-51.

〔99〕Dan Hunter, "Cyberspace as Place and the Tragedy of the Digital Anticomons", *California Law Review*, Vol. 91, 2003, pp. 439, 447-452.

〔100〕"Domains & Jurisdiction Program, Operational Approaches Norms, Criteria, Mechanisms", April 2019, https://www.internetjurisdiction.net/uploads/pdfs/Papers/Domains-Jurisdiction-Program-Operational-Approaches.pdf.

〔101〕"Bylaws for Internet Corporation for Assigned Names and Numbers | A California Nonprofit Public-Benefit Corporation", Article 1.

〔102〕Hong Xue, "Caveats of intermediary liability in the Domain Name System: a review of the ICANN new gTLD right protection measures", in *Intellectual Property Perspectives on the Regulation of New Technologies*, ed. by Tana Pistorius, Edward Elgar Publishing, 2018, p. 35.

〔103〕ICANN, "About Public Interest Commitments Dispute Resolution Procedure (PICDRP)", https://www.icann.org/resources/pages/picdrp-2013-10-31-en.

〔104〕〔109〕Caroline Bricteux, "Regulating Online Content through the Internet Architecture: The Case of ICANN's new gTLDs", *Jipitec*, 7 (2017) 3, https://www.jipitec.eu/issues/jipitec-7-3-2016/4512.

〔105〕〔106〕〔108〕〔144〕Francis Augusto Medeiros, "Is .com International: The .com gTLD: An Analysis of Its Global Nature through the Prism of Jurisdiction", *International Journal of Law and Information Technology*, Vol. 21, No. 3, Autumn 2013, pp. 269-312.

〔107〕"The 10 Most Abused Top Level Domains", July 8, 2023, https://www.spamhaus.org/statistics/tlds/.

〔111〕"Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act", White Paper, April 2019.

〔112〕洪延青:《美国快速通过 CLOUD 法案 明确数据主权战略》,《中国信息安全》2018 年第 4 期。

〔113〕2020 年 7 月欧盟法院以美欧数据跨境流动的"隐私盾协议"未提供充分隐私保护违反了《欧盟基本权利宪章》的规定为由裁决该协议无效,此后至美欧再次达成协议前美国公司向美国储存欧盟人员数据的行为即违反欧盟法。

〔114〕〔133〕Hanna Ziady, "Meta slapped with record $1.3 billion EU fine over data privacy", CNN, https://edition.cnn.com/2023/05/22/tech/meta-facebook-data-privacy-eu-fine/index.html.

〔115〕General Data Protection Regulation, Art. 27(1).

〔116〕《网络安全法》第 2 条、《数据安全法》第 2 条。

〔117〕Ministere Des Armees (2019) op. cit., p. 6.

〔118〕Dongsheng Zang, "Revolt against the U.S. Hegemony: Judicial Divergence in Cyberspace", *Wisconsin International Law Journal*, Vol. 39, No. 1, January 2022, pp. 1-70.

〔119〕〔132〕杨永红:《美国域外数据管辖权研究》,《法商研究》2022 年第 2 期。

〔120〕〔146〕〔161〕〔162〕James Andrew Lewis, "Sovereignty and the Evolution of Internet Ideology", October 30, 2020, https://www.csis.org/analysis/sovereignty-and-evolution-internet-ideology.

〔121〕Google Spain SL v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, CJEU, Case C-131/12, May 13, 2014.

〔123〕Google Inc. v. Equustek Solutions Inc., 2017 SCC 34. [2017]1 S.C.R. 824, Supreme Court of Canada, June 28, 2017; Case C-131/12, Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, CJEU, Case C-131/12, May 13, 2014.

〔124〕Jack Goldsmith, "Unilateral Regulation of the Internet: A Modest Defence", *European Journal of International Law*, No. 11, 2000, pp. 135-148.

〔125〕Matt Richtel, "Web Engines Plan to End Online Ads For Gambling", *The New York Times*, https://www.nytimes.com/2004/04/05/business/web-engines-plan-to-end-online-ads-for-gambling.html.

〔126〕Dan Jerker B. Svantesson, *Extraterritoriality in Data Privacy Law*, Ex Tuto Publishing, 2013, p. 173; Svantesson, Dan Jerker B, "Delineating the Reach of Internet Intermediaries' Content Bloc-

king – ‘ccTLD Blocking’, ‘Strict Geo – location Blocking’, or a ‘Country Lens Approach’?”, *SCRIPTed: A Journal of Law, Technology & Society*, Vol. 11, No. 2, September 2014, pp. 161 – 168.

〔128〕Dan Jerker B Svantesson, “Delineating the Reach of Internet Intermediaries’ Content Blocking – ‘ccTLD Blocking’, ‘Strict Geo – location Blocking’, or a ‘Country Lens Approach’?”, *SCRIPTed: A Journal of Law, Technology & Society*, Vol. 11, No. 2, September 2014, pp. 164 – 165.

〔129〕Tribunal de Grande Instance de Paris, Ordonnance de référé du 16 Septembre 2014, M. et Mme X et M. Y/Google France, http://www.legalis.net/spip.php?page=jurisprudence – decision&id_article=4291.

〔130〕〔131〕Brendan Van Alsenoy, Marieke Koekkoek, “Internet and Jurisdiction after Google Spain: the Extra – Territorial Reach of the EU’s ‘Right to Be Forgotten’”, *International Data Privacy Law*, Vol. 5, No. 2, May 2015.

〔134〕Equustek Solutions Inc. et al. v. Jack et al., (2015) 373 B. C. A. C. 240 (CA).

〔135〕〔137〕Case C – 131/12, Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, CJEU, May 13, 2014.

〔136〕Article 29 Data Protection Working Party, “Guidelines on the implementation of the Court of Justice of the European Union judgment on ‘Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González’ C – 131/12”, 2014, WP225, https://ec.europa.eu/newsroom/article29/items/667236/en.

〔138〕Google Inc. v. Equustek Solutions Inc., [2017] 1 S. C. R. 824, 826 (Can.).

〔139〕Google LLC v. Equustek Solutions Inc., et al., Case No. 5:17 – cv – 04207 – EJD., United States District Court, N. D. California, November 2, 2017.

〔140〕Case C – 507/17, Google Inc. v. Commission nationale de l’informatique et des libertés, ECLI: EU: C: 2019: 772, paras. 63 – 64 (Sept. 24, 2019).

〔142〕Regulation (EU) 2017/1128 of the European Parliament and of the Council of 14 June 2017 on cross – border portability of online content services in the internal market, 2017 O. J. (L 168) 1, 98.

〔143〕Marketa Trimble, “Copyright and Geoblocking: The Consequences of Eliminating Geoblocking”, *Boston University Journal of Science & Technology Law*, Vol. 25, No. 2, 2019, pp. 476, 486.

〔145〕《重定向和 Google 搜索》, https://developers.google.cn/search/docs/crawling – indexing/301 – redirects?hl=zh – cn。

〔147〕David E. Sanger, “Microsoft Warns of Destructive Cyberattack on Ukrainian Computer Networks”, *The New York Times*, 2022, https://www.nytimes.com/2022/01/16/us/politics/microsoft – ukraine – cyberattack.html.

〔149〕〔美〕迈克尔·施密特、丽斯·维芙尔:《网络行动国际法塔林手册 2.0 版》, 黄志雄等译, 北京: 社会科学文献出版社, 2018 年, 第 5 页。

〔150〕TaLlinn Manual 2.0 on International Law Applicable To Cyber Operations (Michael N. Schmitt ed., 2017), at 12, 14.

〔152〕《关于 IGF》, https://intgovforum.org/zh – hans/about。

〔153〕鲁传颖、杨乐:《论联合国信息安全政府专家组在网络空间规范制定进程中的运作机制》,《全球传媒学刊》2020 年第 1 期。

〔156〕〔157〕〔158〕Danielle Higson, “Applying the Law of Neutrality While Transiting the Seas of Cyberspace”, *National Security Law Brief*, Vol. 6, No. 2, Spring 2016, pp. 1 – 36.

〔159〕Rachel Pannett, “Indian state shuts down Internet for millions to prevent cheating on teachers’ exam”, The Washington Post, September 29, 2021, https://www.washingtonpost.com/world/2021/09/29/india – exam – cheating – internet – shutdown/.

〔160〕《联合国海洋法公约》第 25 条。

〔163〕《网络空间国际合作战略》第三章, 外交部网, http://new.fmprc.gov.cn/web/wjb_673085/zzjg_673183/jks_674633/zclc_674645/qt_674659/201703/t20170301_7669140.shtml。

〔责任编辑:邹秋淑〕