世界主要国家和地区网络空间竞争的主要举措与政策建议

于 良
（中国科学技术发展战略研究院，北京 100038）

摘 要：网络空间战略的重要性已经得到世界主要国家和地区的高度重视。美国、德国、日本、英国等都制定了国家网络空间战略，维护和争取网络空间中的优势地位，特别是网络空间安全成为关注的热点。其中，发展数字经济、强化安全审查、进行国际合作、形成双边多边的网络安全合作协议和组织、培育网络安全市场、培训网络安全人才等做法对我国具有重要意义。

关键词：网络空间战略；网络安全；数字经济；网络安全人才
中图分类号：F273.1 **文献标识码**：A DOI：10.3772/j.issn.1009-8623.2018.11-12.006

围绕网络空间的竞争已经成为国家竞争的重要方面，世界主要国家和地区正通过加强数据监控、国际合作、市场培育以及人才培训等措施提升自身在网络空间领域的竞争力。例如，美国已经通过双边多边的网络空间协定和区域性组织逐步形成了以美国为主导的区域性网络空间体系。近期出现的美国《2019 年度国防授权法案》禁止政府和政府承包商使用华为和中兴通讯等中国科技公司的组件和服务，澳大利亚参议院通过了反外国干涉相关法案、禁止中兴和华为参加其 5G 网络建设等敏感事件都与其网络空间战略有关。

1 国家（地区）间竞争向网络空间延伸

当前，数字经济被认为是推动经济转型发展和效率提升的加速器。世界经济论坛研究指出，数字化程度每提高 10%，人均 GDP 增长 0.26%~0.5%。世界主要国家和地区加速推动向数字经济转型，英国在 2009 年就推行了“数字大不列颠”行动计划并陆续颁布相关法案政策，致力于数字经济的创新；欧盟在 2010 年将“数字欧洲计划”作为“欧盟 2020 年战略”的重要组成部分，以此推动数字经济和信息社会的发展。在世界主要国家和地区推动下，数字经济逐步成为经济的主体。据中国信息通信研究院的《G20 国家数字经济发展研究报告（2017 年）》统计，2016 年，美国数字经济规模全球领先，达到 10.8 万亿美元，占 GDP 的 58.3%[1]，日本、英国等国的数字经济占 GDP 比重都超过 40%，我国数字经济规模达到 3.4 万亿美元，占 GDP 的 30.3%。

随着数字经济的发展，网络空间在各国（地区）经济和战略博弈中的重要地位日益突出[2]。2017 年 12 月发布的美国《国家安全战略报告（2017）》指出：“经济和个人交易依赖于网络空间，财富的创造依赖于可靠、安全的互联网。”[3] 电气电子工程师学会（IEEE）提出人类社会、物理世界的二元结构正在转变为加入网络空间的三元结构。中国电子学会发布的《新一代人工智能发展白皮书（2017）》提出国家间竞争和博弈的重心逐

作者简介：于良（1978—），男，博士，副研究员，主要研究方向为科技规划与区域规划。
项目来源：科技部科技创新战略研究专项“新形势下推进产学研协同创新的重大问题研究”（ZLY201719）；“科技创新支撑经济新动能的成长方向和路径研究”（ZLY201703）。
收稿日期：2018–10–20

步从土地、人力、资本的数量质量转移至数字化发展水平，掌握网络空间核心竞争优势的国家和地区，将在围绕新一轮国际分工态势展开的博弈中抢先占据价值链制高点[4]。

2 世界主要国家和地区制定网络战略保障安全并提升影响力

世界主要国家和地区相继发布网络安全战略和网空间战略，如美国《确保网络空间安全的国家战略》（2003）、美国《网络空间国际战略》（2011）、德国《网络安全战略》（2011）、英国《国家网络安全战略》（2011）、日本《网络安全战略》（2013）、澳大利亚《网络安全战略》（2016）、澳大利亚《国际网络参与战略》（2017）等，覆盖网络犯罪、个人隐私信息、网络合作治理、关键基础设施安全等方面（见表1）。世界主要国家和地区网络战略的共性内容包括：保护关键信息基础设施，成立网络安全响应机构，成立网络安全委员会，加大网络安全技术研发、开展网络安全教育培训，发展国际伙伴合作并形成双边多边协议等。

表1 世界主要国家和地区网络战略要点

战略	要点
美国《确保网络空间安全的国家战略》	（1）建立国家网络安全反应系统；（2）建立一项减少网络安全威胁和脆弱性的国家项目；（3）建立一项网络安全预警和培训的国家项目；（4）确保政府各部门的网络安全；（5）进行国家安全与国际网络安全合作
美国《网络空间国际战略》	（1）通过制定国际标准、鼓励创新和开放市场，加强知识产权保护；（2）确保网络的安全、可靠和韧性；（3）深化执法合作并积极推出国际规则；（4）强化“网军”以应对21世纪的安全挑战；（5）建立有效且多方参与的国际互联网治理架构；（6）展开“网络援外”；（7）保障互联网自由
德国《网络安全战略》	（1）保护关键的信息基础设施；（2）保护公众和中小型企业信息系统安全；（3）加强公共领域系统安全；（4）建立国家网络响应中心；（5）成立国家网络安全协调委员会和国家网络响应中心（NCRC）；（6）控制网络空间犯罪；（7）在欧洲和全球范围内促进网络安全合作；（8）采用可靠和可信的信息技术；（9）推动联邦政府雇员在信息安全领域的职业拓展；（10）回应网络攻击方式[5]
日本《网络安全战略》	（1）改组内阁官房信息安全中心为网络安全中心；（2）完善国内关键基础设施的安全防护，改善日本政府机构及十大关键领域的网络安全防范网[6]；（3）扩大信息市场规模，提高日本网络安全专业人才的技术水平并发现和培养该领域内的杰出人才；（4）广泛开展国际合作，在与现有80多个国家网络安全合作的基础上增加3成
英国《国家网络安全战略》	（1）成立国家网络安全中心（NCSC）；（2）采取“国际行动”投资发展伙伴关系，通过与欧盟、北约和联合国的双边和多边协议加强网络安全[7]；（3）加大干预力度并投资，利用市场力量提高英国的网络安全标准，不断加强关键国家基础设施的网络安全；（4）利用产业界的能力，开发和应用主动式网络防御措施；（5）投资人才发展计划，解决英国网络安全技术短缺的问题；（6）成立两个新的网络创新中心，以推动先进网络产品和网络安全公司的发展；（7）拨款1.65亿英镑设立国防和网络创新基金，以支持国防和安全领域的创新采购[8]
澳大利亚《网络安全战略》	（1）构建政府、研究者和企业之间的国家网络合作关系；（2）以强有力的网络防御措施来更好地发现、阻止并应对威胁的发生，对风险进行预测；（3）增强全球化的责任感和影响力，营造安全、开放和自由的互联网环境，同时打击网络犯罪；（4）通过发展和改革，帮助澳大利亚的网络安全企业成长繁荣，支持本土网络安全专家发展；（5）建设一个网络智能国家，在大学里构建网络安全精英学术中心培养网络安全专家，并加强整个教育系统的科学、技术、工程、数学（STEM）技能培养。（6）成立网络威胁中心
澳大利亚《国际网络参与战略》	（1）启动“网络合作项目”（Cyber Cooperation Program），强力参与网络合作，有利于其发挥国际领导作用，重点支持在印太地区的实施；（2）澳大利亚政府成立工业界主导的非营利企业AustCyber（Australian Cyber Security Growth Network），进一步发展澳大利亚网络安全能力和市场需求，提高澳大利亚网络安全企业在全球市场的竞争力，为澳大利亚网络安全部门吸引国外直接投资；（3）主张多方参与论坛式的网络治理模式，反对政府控进行政治性审查

网络战略还是世界主要国家和地区提升国际影响力的重要途径。以澳大利亚为例，澳大利亚以网络空间战略为突破口，在主导区域经济、法律等方面建立国际机制。澳大利亚重视在太平洋岛屿国家中的影响力，建立了太平洋岛民网络安全组织（CSP）、太平洋网络运行网（PaCSON）以及协调解释太平洋国家的法律并优先考虑网络立法的太平洋岛国立法协调组织（PILON）。特别是，印尼是澳大利亚外交的重点，澳大利亚长期作为印尼最大的援助国，澳－印尼法律与安全部长理事会和援助成立的雅加达法律合作加强中心（JCLEC）等对网络法律制定产生了重要影响。

3　世界主要国家和地区实施网络空间战略的主要举措

世界主要国家和地区加强了对网络空间的治理，通过经济、政策等手段推动数据、安全、人才等方面发展。在全球统一的网络空间竞争规则尚未形成前，国际合作成为世界主要国家和地区网络空间战略的共同选择。

3.1　数据作为网络空间核心要素的作用凸显，积极强化对数据控制权的争夺

数据对网络空间的战略价值不亚于工业社会的石油，围绕掌控数据的新的大国竞争更加激烈。互联网数据中心预测，全球数据总量预计2020年达到4.5万EB（1EB约为10亿GB）。我国工业和信息化部预测，我国数据量年均增速超过50%，2020年数据总量在全球占比将达到20%。世界主要国家和地区纷纷制定法律法规对数据本地存储和跨国（地区）流动进行规范[9]。澳大利亚、韩国、希腊分别要求个人健康、金融、交通位置的关键产业数据在本地存储，俄罗斯、马来西亚等国家要求重要数据信息在本地存储。英国为保障数据流动的安全，出台《数据保留和调查权法案》，要求典型运营商和互联网企业进行数据留存。欧盟发布《通用数据保护条例》（GDPR）[10]，限制所有收集、处理、储存、管理欧盟公民个人数据的企业的权限[11]，主要针对美国的Facebook、Google等IT巨头采集和传输欧洲数据的行为。但由于美国在网络空间形成了明显的优势，世界其他主要国家和地区仍然难以单独对抗。

3.2　世界主要国家和地区网络安全战略实施高度重视国际合作，网络安全合作协议和组织成为构建国际空间格局的重要手段

网络安全的重要性不断提升[12]。达沃斯论坛发布的《2018年全球风险报告》显示，网络安全风险令世界经济每年损失5 000亿美元。世界主要国家和地区相继发布网络安全战略[13]，把国际合作作为保障网络安全的重要举措。美国《确保网络空间安全的国家战略》提出“国家安全与国际网络安全合作”；德国《网络安全战略》提出“在欧洲和全球范围内促进网络安全合作”；日本《网络安全战略》提出“广泛开展国际合作，在与现有80多个国家网络安全合作的基础上增加3成”；英国《国家网络安全战略》（2016）提出“采取‘国际行动’投资发展伙伴关系，通过与欧盟、北约和联合国的双边和多边协议加强网络安全”。

世界主要国家和地区与经济体之间形成了大量保护国家数据主权的双边多边网络合作协议和组织[14]。欧盟与美国签署跨境数据流动协议——欧美隐私盾协议（EU-US Privacy Shield）[15, 16]；欧盟28个成员国中有20个国家已经正式更新了其国内法，适用欧盟《通用数据保护条例》[17]；美国、墨西哥、日本、韩国等国家签署亚太经合组织（APEC）的跨境隐私规则（CBPRs）[18]；澳大利亚与太平洋岛屿国家建立了太平洋岛民网络安全组织等。美国已经通过美韩跨境数据流动规则、欧盟－美国隐私盾协议以及亚太经合组织跨境隐私规则等双边多边的网络空间协定，建立了美国主导的区域性网络空间体系，并将我国排斥在外。

3.3　网络安全市场逐步成为新经济增长点，世界主要国家和地区积极培训网络安全人才

培育网络安全市场成为世界主要国家和地区提升网络安全能力、保障数字经济增长的重要途径。英国通过国防和网络创新基金支持网络安全领域的创新采购；日本加大网络安全方面的采购，希望将市场规模扩大一倍以上；澳大利亚成立非营利企业AustCyber来为网络安全部门吸引国外直接投资。监管合规及数据隐私等规则对于推动网络安全市场的快速增长发挥着重要的作用。欧洲《通用数据保护条例》的罚款最高可达全球营业额的4%；美国

《数据安全和泄露通告法案》对未遵从者判处最高5年监禁。此外，全球企业受网络攻击和数据泄露等安全事件驱动加大网络安全的开支。咨询公司Gartner最新预测，2018年全球信息安全产品和服务支出将超过1 140亿美元，并将以每年7.8%的复合增长率增长，成为超过千亿美元市场的新经济增长点。

培训网络安全人才成为世界主要国家和地区实施网络安全战略的重要措施。美国咨询机构Cybersecurity Venture预测，到2021年全球网络安全领域的人才缺口将达到350万。英国在大学里设立专家课程并提出“网络安全学徒计划”[19]；日本建立信息安全从业人员相应的技术能力评定系统；澳大利亚构建大学网络安全精英学术中心，培养网络安全专家并提供工作机会。

4 政策建议

面对美国已经建立的区域性网络空间体系，我国需要提升在网络空间的竞争力，并通过双边多边国际合作提升中国在网络空间的影响力，保障我国在网络空间的国家安全,同时支撑数字经济的发展。

一是构建区域性网络空间合作体系，建设海外国际数据中心。在全球性网络空间合作体系难以形成的背景下，我国急需构建区域性网络空间合作体系来应对挑战。可考虑在金砖国家、亚太经合组织、东盟等区域性框架下提出对网络空间规则的整体性主张，在国际合作中扩大网络空间的合作；加强与欧日韩澳等国家和地区在网络安全产品和服务采购、数据跨界流动、网络安全人才培养等方面的合作。为满足我国企业在美国市场的数据跨国流动需求，可选择在签署了亚太经济合作组织跨境隐私保护规则的墨西哥、日本、韩国等国家建设国际数据中心。

二是完善数据本地存储和跨国流动规则，保护我国网络空间的数据主权。我国现有基于安全评估的网络安全政策还难以适应海量数据的监管需求。我国《网络安全法》规定个人信息和重要数据应当在境内存储。但是对于因业务需要确需向境外提供的数据，目前我国的监管规定缺乏实施流程和对数据滥用的救济机制。应借鉴欧盟的《通用数据保护条例》，对“个人信息和重要数据”的范围、用途、责任、救济、惩罚等方面进行更细致的规定，保护我国的数据主权。

三是加大政府采购力度，培育网络安全市场。与全球市场相比，我国的网络安全市场还处于发展安全硬件的初级阶段，安全服务比重较低，市场发展空间很大。我国应加大对网络安全产品和服务的政府采购力度，在金融、交通、医疗健康等重点领域形成自主可控的安全解决方案，培育形成一批网络安全领域的创新型领军企业，将现有网络安全市场扩大到千亿元人民币规模。

四是实施网络安全人才培训计划，弥补网络安全人才缺口。据中央网信办网络安全局和教育部高教司公布数据，目前我国信息安全专业人才总量不足10万，年培养规模在3万人左右，缺口高达95%。我国应设立每年培训10万～20万人规模的网络安全人才培训计划。重点支持企业和高等院校、职业学校等教育培训机构开展网络安全相关教育与培训，建立网络安全人员评价体系，建立在线网络安全培训平台。

五是建立灵活的数字经济监管框架，促进网络空间竞争。澳大利亚政府在网络空间战略中提出建立灵活的数字经济监管框架,明晰监管机构的权利，立法建立众包的股权融资框架；修改现有金融监管的优先领域，使其不妨碍创新和金融系统的竞争。我国应顺势建立促进数字经济的新监管体系，在支持“双创”融资、培训年轻人使用数字技术等方面进一步加强，提高我国在网络空间的竞争力。■

参考文献：

[1] 陈慧琴 . 数字经济驱动创新 转型升级开创未来 [N]. 上海证券报，2018-04-14（005）.

[2] 李鸿渊. 论网络主权与新的国家安全观 [J]. 行政与法，2008（8）：115-117.

[3] 王桂芳 . 网络安全是特朗普版国家安全战略报告的最大增量 [J]. 中国信息安全，2018（2）：41-43.

[4]《人民邮电》编辑部 . 共建智慧社会新时代，共创智能产业新动能 [N]. 人民邮电，2018-04-26.

[5] 张亚妮 , 傅鹏 .“壮年”维特之烦恼——德国网络安全战略浅析 [J]. 中国信息安全，2012（7）：48-51.

[6] 唐岚，张力 . 莫言网事风初起萧萧暗雨打窗声——透视国外网络安全战略 [J]. 信息安全与通信保密，2014

（11）：57-61.
[7] 沈逸，杨杨 .2016 年世界网络安全态势盘点 [J]. 汕头大学学报（人文社会科学版），2017，33（1）：23-33.
[8] 《中国教育网络》编辑部 . 终结黑客攻击的操作系统问世 [J]. 中国教育网络，2016（12）：51.
[9] 张衡，李兆雄 . 大数据本地存留与跨境流动问题研究 [J]. 信息安全与通信保密，2015（6）：65-69.
[10] 曾丽洁 . 欧洲企业对跨境流通数据资讯隐私权保护的自律模式 [J]. 武汉交通职业学院学报，2012（12）：21-27.
[11] 高明 . 欧盟跨境数据流动的法律探究 [J]. 法制与社会，2011（10 上）：20-23.
[12] 杨嵘均．论网络虚拟空间对国家安全治理界限的虚拟化延伸 [J]. 南京社会科学，2014（8）：87-94.
[13] 韩静雅 . 跨境数据流动国际规制的焦点问题分析 [J]. 河北法学，2016，34（10）：170-178.
[14] 何波，石月 . 跨境数据流动管理实践及对策建议研究 [J]. 互联网天地，2016（12）：29-32.
[15] 刘耀华，石月 . 欧美“隐私盾”协议及对我国网络数据保护的启示 [J]. 现代电信科技，2016，46（5）：12-16.
[16] European Parliament Approves EU-US. Umbrella Agreement [EB/OL].（2016-12-05）[2018-09-13]. http://www.natlawreview.com/article/european-parliament-approves-eu-us-umbrella-agreement.
[17] 王瑞 . 欧盟《通用数据保护条例》主要内容与影响分析 [J]. 金融会计，2018（8）：17-26.
[18] 耿晨 . 个人数据跨境流动的国际监管与合作制度研究 [D]. 上海华东政法大学，2014.
[19] 《中国教育网络》编辑部 . 英国政府公布网络安全学徒计划 [J] . 中国教育网络，2015（5）：6.

Major Initiatives for Cyberspace Competition in Major Countries and Regions in the World and Policy Recommendations

YU Liang
(China Academy of Science and Technology For Development, Beijing　100038)

Abstract: The importance of the cyberspace strategy has been highly valued by major countries and regions around the world. The United States, Germany, Japan, and the United Kingdom have all formulated national cyberspace strategies to maintain and strive for a dominant position in cyberspace. In particular, cyberspace security has become a hot spot of concern. Among them, developing digital economy, strengthening security review, forming international cooperation, forming bilateral and multilateral network security cooperation agreements and organizations, cultivating the network security market, training network security personnel and other practices are of great significance to China.

Key words: cyberspace strategy; network security; digital economy; cyberspace security talent