网络空间安全国际指数研究

吕 欣

摘要：随着信息技术的不断发展，网络空间安全已经成为国家安全的重要组成部分，成为了展开国际竞争的重要领域。本文研究建立了网络空间安全国际指数，选取 7 个国家（地区），综合衡量建设情况指标、运行能力指标、安全态势指标 3 个方面，细分 12 个 3 级指标，对各国（地区）的网络安全态势进行了分析评估。评估结果旨在为我国的网络空间安全有关工作提供借鉴和启示。

网络空间安全的竞争压力凸显

习近平总书记提出，没有网络安全就没有国家安全。随着互联网的普及和发展，网络安全在国家安全中的地位愈加突显，除了传统的军事、经济、金融方面的较量，网络资源已经成为各国争夺的重要战略资源，网络安全威胁也成为各国政府面临的重要挑战。在当前国际背景下，世界各国普遍将加快信息科技创新、提升网络空间竞争能力作为促进经济发展和提升综合国力的重要战略举措,并逐步推出各自的网络空间安全战略。

近年来，一些国家和国际组织相继推出了网络安全评价相关的研究成果，用于各个国家（或地区）信息化进程与网络安全状况的比较分析。国际电信联盟（ITU）和ABI Research公司联合研究并提出了全球网络安全指数，该指数用于衡量各国的网络安全工作情况；美国弗吉尼亚州马可研究所于2015年2月推出了网络空间就绪度指标（Cyber Readiness Index），调查了125个国家网络安全基本要素的成熟度；软件联盟（BSA）于2015年1月提出了基于五大主要领域、25项标准的欧盟网络安全指示板（EU Cyber security Dashboard），给欧盟成员国的政府官员提供了评估其国家政策的标准；国际标准化组织也发布了信息安全管理测量标准（ISO/IEC 27004:2009），从方针策略、信息安全、风险管理、控制目标、控制措施、过程和规程等多维度测度信息安全；澳大利亚战略政策研究所（ASPI）发布了2014年与2015年的亚太地区网络成熟度报告。

本文通过研究制定网络空间安全国际指数，对部分国家的网络空间发展状况与安全保障能力进行评价，实现对部分国家的信息化程度与网络安全保障能力的评估分析；通过评价结果的分析,对网络空间安全保障能力和水平进行比较;最后根据评价实践和分析结果对我国网络安全工作给出了几点启示。

评价指标体系介绍

本报告选取2013—2015年7个国家（区域）网络安全相关数据建立指标体系，对部分国家（区域）的网络安全保障情况进行评价，具体指标包括：网络安全战略规划指标、网络安全法律法规指标、网络安全标准体系指标、网络安全人才培养指标、网络安全信息共享指标、网络安全组织结构指标、公共安全意识指标、产业规模指标、R&D投入指标、网络治理参与指标、网络应急处置指标、关键基础设施战略规划指标。具体的评价过程如下。

1）指标确定

组织专家进行内部讨论，对国际公开资料以定性定量方法进行评估，确定网络空间安全国际指数的主要指标。

2）权重评估

召集专家对各项指标的重要性进行评价，进而确定各项指标在指标体系中的权重。

3）量化计算

对各国家（区域）的网络安全保障情况进行量化并计算各项指标的得分。总分即为各项指标评分的加权平均数，并转化为百分制。指标体系如表1所示。

表 1 网络空间安全国际指数指标体系

一级指标	二级指标	三级指标
建设情况指标	宏观管理指标	ZB01 网络安全战略规划指标
		ZB02 网络安全法律法规指标
		ZB03 网络安全标准体系指标
		ZB04 网络安全人才培养指标
		ZB05 网络安全信息共享指标
		ZB06 网络安全组织结构指标
		ZB07 公众网络安全意识指标
	技术产业指标	ZB08 产业规模指标
		ZB09 R&D 投入指标
运行能力指标	网络治理指标	ZB10 网络治理参与指标
		ZB11 网络应急处置指标
安全态势指标	网络态势指标	ZB12 关键信息基础设施战略规划指标

该指标体系包括12个3级指标，既综合反映各国家（区域）网络空间安全保障体系的建设情况，又突出技术产业、关键信息基础设施等对网络空间安全的重要意义。指标的选取主要基于2方面的考虑：一方面，这些指标的数据来源可靠，一般来自于各国家（区域）的官方文件，具有权威性与准确性；另一方面，这12个指标是各国家（区域）网络安全保障状况的综合反映，可体现各个国家（区域）在网络安全方面作出的努力与取得的成果。

评价结果分析

1）总体情况分析

2013—2015年，部分国家（区域）网络空间安全指数排名及得分情况如表2所示，这7个国家（区域）二级指标得分情况如图1和图2所示，美国、日本、德国与欧盟网络空间安全指

数情况如图3所示，英国、法国与俄罗斯网络空间安全指数情况如图4所示。

表 2 部分国家（区域）网络安全保障指标评价排名（截至 2015 年）

排名	国家（区域）	网络空间安全国际指数指标体系				总分
		建设情况指标		运行能力指标	安全态势指标	
		宏观管理	技术产业	网络治理	网络态势	
1	美国	89.78	81.21	87.84	85.33	86.04
2	德国	84.78	76.26	82.08	81.83	81.24
3	欧盟	84.54	72.96	83.75	83.67	81.23
4	英国	86.95	70.47	82.59	81.50	80.38
5	日本	83.23	83.00	80.83	72.50	79.89
6	法国	78.78	72.15	80.17	69.00	75.03
7	俄罗斯	76.29	60.08	80.83	68.17	71.34

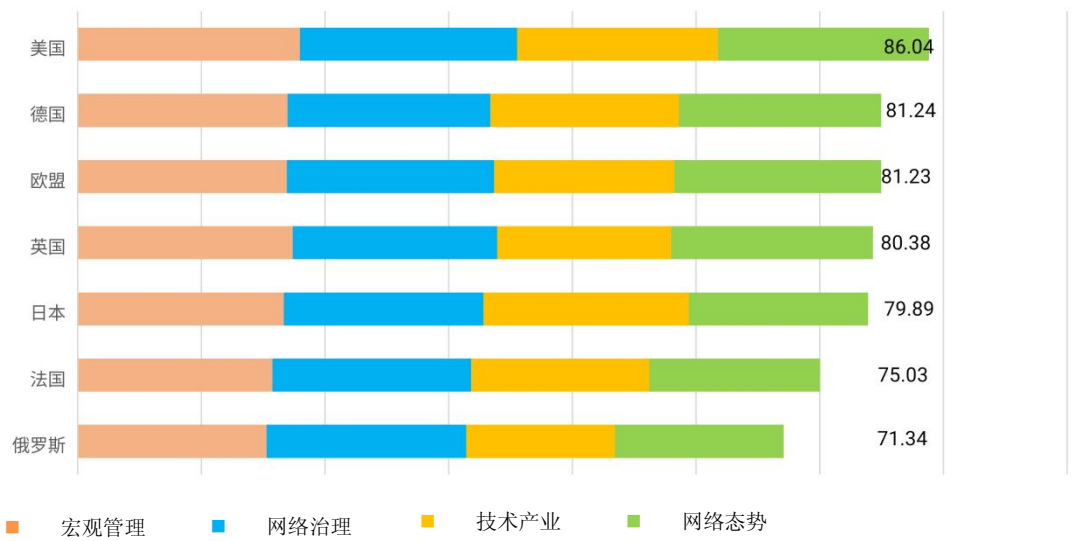

图 1 部分国家（区域）网络安全保障指标得分情况（截至 2015 年）

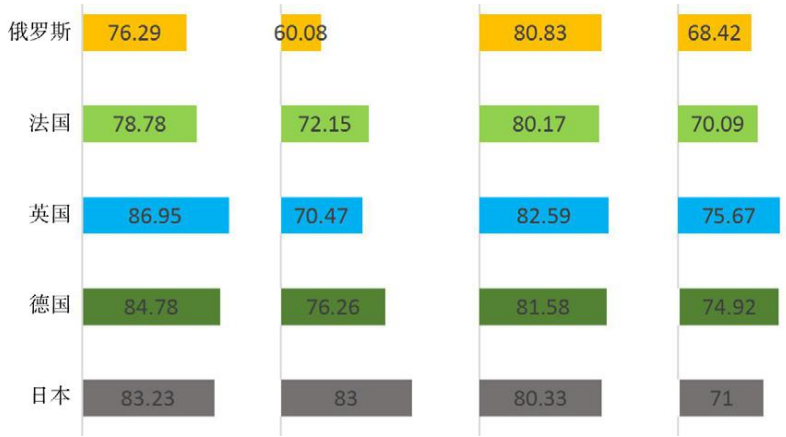

图 2 部分国家（区域）二级指标得分情况（截至 2015 年）

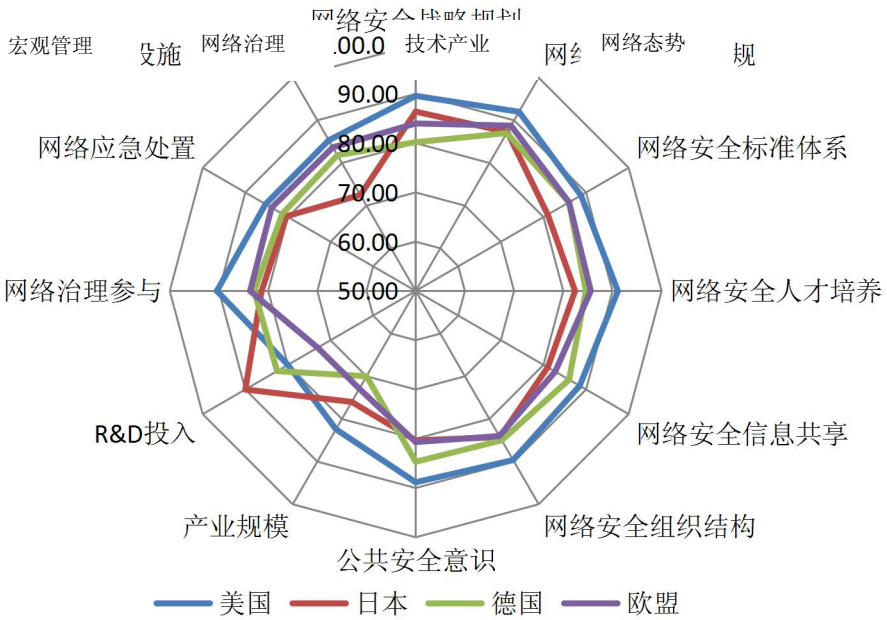

图 3 部分国家（区域）网络安全保障指标得分情况 1

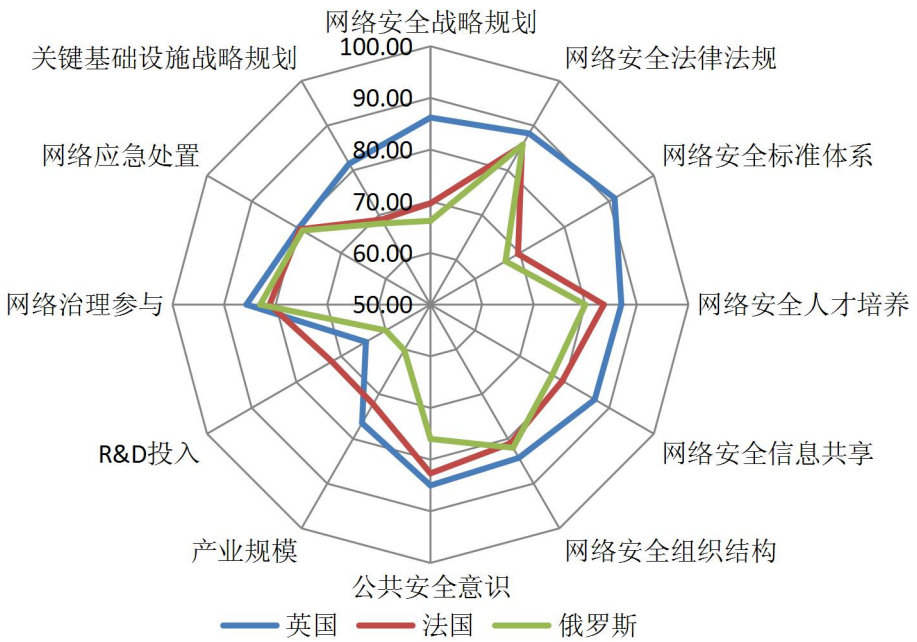

图 4 部分国家（区域）网络安全保障指标得分情况 2

如图3所示：①2013—2015年美国的网络安全保障体系建设在部分国家（区域）中占据相对优势，其各个3级指标得分均处于较高水平且总体较为均衡；②日本依托其较高的技术产业研发投入与较为完善的网络空间战略规划紧跟其后，位列第二，但在网络安全标准体系建设和信息共享方面还有较大发展空间；③德国在各个领域均有较好表现且发展相对均衡，位列第三；④欧盟的网络态势建设相对不足，但在宏观管理方面表现较好，位列第四。如图4所示：①英国与法国在网络态势建设方面存在较大的发展空间，此外，在网络安全信息共享与网络应急处置等方面也与领先国家存在一定差距；②俄罗斯在网络安全法律法规和网络空间国际方面的工作取得明显成绩，但在网络安全保障的其他方面较美日等国家仍有一定发展空间，从而处于相对较低的位置。

从2级指标得分情况来看，①部分国家（区域）在技术产业指标、宏观管理指标方面的表现整体较好。其中，各国家（区域）在宏观管理指标得分相差较小，说明部分国家（区域）对网络安全保障宏观管理方面均给予一定的重视并采取相应措施；各国家（区域）的技术产业指标得分差距较大，美国与日本的技术产业居于世界领先水平，德国、欧盟、法国与英国处于第2梯队，俄罗斯还有一定的距离需要追赶。②部分国家（区域）在网络治理与网络态势方面的得分相对较低，其中网络应急处置工作有待加强。

2）分项指标比较

美国等7个国家（区域）在网络安全保障方面均取得一定的成绩，下文将分别从12个分项

指标加以分析，总结7个国家（区域）在网络安全保障方面的工作。

（1）宏观管理指标

①网络安全战略规划

在网络安全战略规划方面，7个国家（区域）均出台了相关的战略，将网络安全纳入各国（区域）的战略重点，并不断完善配套政策和相关报告。

网络空间安全战略实施。美国以2011年发布的《网络空间安全国际战略》和《网络空间安全行动战略》为指导框架，发布相关条令规范“网络战”的具体内涵，建立必要的框架体系以及配套机制，并逐年发布《情报界全球威胁评估报告》[1]，实现从以技术为中心的军事层面向国际层面转移，从针对传统威胁向针对非传统性数字威胁过渡。

政策实施情况有效评估。日本2013年发布了以创建“领先世界的强大而有活力的网络空间”为宗旨、以实现“网络安全立国”为目标的《网络安全战略》，在强化国家基本职能的同时，制定必要的法律法规保障网络安全，发布网络安全政策年度报告来评估网络安全领域的建设成果，有效评估网络安全态势以及政策实施情况[2]。

网络安全领域精准聚焦。德国以打造一个具有国际竞争力的“数字强国”为目的，联合推出《数字议程2014—2017》，确定了网络安全战略的十大关键领域，使其网络安全战略的实施更具针对性和有效性[3]。

②网络安全法律法规

网络安全法律法规作为维护网络安全的重要手段之一，在7个国家（区域）均有所涉及，对网络安全的监管力度均进一步增强。

法律覆盖范围不断扩大。美国网络空间安全的相关法律具有较为广泛的覆盖面，其法律法规体系较为完备。2013—2015年，每年均提出重要的网络安全法案条例讨论并通过，在法理层面将网络安全放到了重要的战略地位，对政府部门角色定位、网络安全人员评估以及监控系统立法改革作了相应的规范。联邦政府以及各州政府均积极推动与网络安全相关的法律建设，不断完善优化网络安全法律体系，推进网络安全的法治化建设[4]。日本近年来不断加强立法，制定了《个人信息保护法》、《禁止不正当接入法》、《电子契约法》和《特定秘密保护法》等专门法规[2]，与此同时，日本设立配套行动部门，如全国性的网络攻击分析中心和国家网络安全中心、网络安全战略本部、网络犯罪中心等机构，提高了对网络犯罪的分析能力，健全了网络犯罪的应急处置机制。

组织机构职能逐渐明确。欧盟已经出台了网络安全、数字网集成服务、个人信息保护等诸多方面的法律，并且不断修订使得现有法律适应新技术发展的要求。在加大对网络攻击犯罪严惩力度的同时，专门制定了金融网络安全相关法规，此外，设立网络犯罪的相关组织机

构，进一步明确各个部门的职能。

执法机制逐步健全。英国在网络犯罪检举、通信监控、隐私条例等方面制定了相关法律法规，发布的《欧盟网络与信息系统安全指令》强调在关键国家基础设施领域进行网络与信息安全合作[5]。在执法机制方面，成立了国家预防网络犯罪署（NCCU）和警察部队，开展打击网络犯罪方面的培训，建立专职的网络领域的专家队伍[3]。

③网络安全标准体系

在网络安全标准体系方面，7个国家（区域）的发展不太均衡，但在本国标准体系的覆盖范围以及国际标准体系制定的参与方面均给予一定程度的重视。

标准体系影响力不断扩大。英国近年来采取了一系列的网络安全标准体系，其中英国标准ISO 27000:2005已经成为世界上应用最广泛与典型的信息安全管理标准，具有较大的国际影响力，此外，英国标准协会（BSI）对各项标准定期展开专项评估，不断优化和更新标准体系，设立标准的专业队伍，逐渐成为集各大互补性业务于一体的国际标准服务提供商，不断将本国网络空间标准推向国际化[6]。日本近年来一方面重视对现有标准体系的完善和优化，另一方面积极参与同国际标准化相关的活动和会议，在国际标准化制定上提出自己的观点。

信息安全标准及时优化。美国在2013—2015年相继发布了智能电网网络安全、政府敏感数据保护以及云计算安全方面的文件，不断更新现有的信息安全标准，以适应法律变动和网络发展的客观要求，积极参与同国际网络空间标准相关的会议和论坛，加强对话与合作，不断完善本国的网络标准体系。

标准体系框架逐渐建立。德国的联邦信息安全局发布了电子邮件准则，为电子服务领域提供了具有功能性、互操作性和安全性的总体框架。同时德国是国际标准组织下属SC27的成员之一，在国际标准的制定中具有一定的影响力[7]。

④网络安全人才培养

在网络安全人才培养方面，7个国家（区域）的整体发展水平较高，各具独特的人才培养途径以及方法。对于人才培养均具有一定的战略规划以及部署。

人才队伍不断壮大。美国在2015年制定网络安全人才培养长期计划，形成一套以夏令营为基础的网络安全人才培养体系。2013—2015年，美国通过开设网络挑战赛等方式选拔各类优秀人才，并宣布将网络安全部队扩编5倍[4]。日本主要通过官产学合作方式，培养维护网络安全的人才队伍。近年来，日本实施了“信息安全人才培养计划”、“黑客大赛SECCON”等人才队伍建设专项计划，建立了网络安全技能国家资格认证制度，并在政府各部门成立网络攻击特别搜查队、CSIRT等专业网络安全维护人才队伍[2]。

人才培养模式逐步优化。英国通过行业协会与技术公司的合作，开展相关的网络安全人

才培养，同时通过大量的开放式在线课程优化人才培养体系。同时，建立网络人才储备库和学术卓越中心，吸纳优秀专业人才，提高网络安全的防御能力[8]。德国的人才培养计划注重于强调教育的重要性，通过数字化论坛、数字化学习战略、职业教育和训练的数字化媒介来提升教育领域的发展效率，提供安全的数字化学习环境，同时通过推动“信息技术安全研究”科研项目来带动网络安全人才的培养[3]。

人才培养领域逐渐扩大。法国将网络安全培训纳入高等教育，产学研相结合，支持产业基地的建设，并且组织大型的网络安全人才招聘。俄罗斯通过《2014—2020年信息技术产业发展战略及2025年远景规划》以及《2018年信息技术产业发展规划》提出加大IT人才培训力度，减少人才流失，将人才储备和培养作为一个重点方向。同时俄军方也将信息安全防护干部的培训列入部分高、中级军事院校的培训体系，将网络安全人才培养扩展至军事层面[9]。

⑤网络安全信息共享

在网络安全信息共享指标层面，各国均建立起了不同层级的共享平台。总的来看，美国、英国和德国处于领先地位，欧盟和日本较为完善，而法国和俄罗斯信息共享建设的情况较为一般。美国、英国和德国的优势在于它们形成了全国性的信息共享机制，实现了跨行业、跨区域的信息一体化[10]。而法国和俄罗斯的全国性系统共享机制作用较小，信息一体化进程较慢。

着力发展政府与企业间信息共享。英国于2013年正式成立“网络安全信息共享合作机制”（CISP），搭建起一套政府和企业间的信息共享合作方式[11]；美国于2015年出台《网络空间安全信息共享法》，进一步提高其网络空间信息开放度[4]。

积极参与构建国际间信息共享平台。德国建立了全球网络态势感知系统，旨在提供全球网络攻击概况。美国与日本在战略同盟的基础上深化网络安全的信息交流。英国也与美日韩等各国共同进行了网络安全问题的专题研讨。

⑥网络安全组织结构

在网络安全组织管理指标层面，7个国家（区域）都形成了较为完善的网络安全组织结构。其中美国占据着相对领先的地位，其他国家的发展水平较为均衡。美国的优势在于其设立了合理的专门安全管理责任机构，定期对责任人进行网络安全教育和技能考核，同时还具有更加完善的组织机构协同联动机制。其他6个国家（区域）的组织间协同联动机制建设力度有待加强。

建立专职责任机构，制定内部管理条例。欧盟国家分别在欧盟框架下成立了计算机应急响应小组（CERT）；法国建立了网络与信息安全局（ANSSI）；英国设立了网络安全办公室（OCS）全权负责信息网络安全战略的规划和实施[12]。

构建组织间协同联动机制，发展多层有序的管理组织。美国于2009年成立网络空间司令部，作为守护美国网络安全的核心组织，协调全国的网络安全事务[4]。日本2015年开始着手建立一支一体化网络安全服务的网络空间防卫队，综合调配各方政府力量，同时吸纳民间组织的力量。

⑦公众安全意识

在公共安全意识指标层面，7个国家（区域）的状况存在一定差异，发展不均衡。美国拥有最佳的公共安全意识状态；英国、德国、法国、欧盟和日本也在国内形成了较强的网络空间公共安全意识；而俄罗斯的公共安全意识建设情况相对较弱[13]。

积极组织宣传教育，引导民众保护个人信息安全。欧盟通过发起“加强网络安全日”、“欧洲网络安全月”、“欧洲网络安全挑战赛”等活动来提升欧盟成员国公民的网络安全意识。德联邦信息安全部(BSI)建立为个人用户提供网络安全信息的网站，积极参与欧盟组织的提升安全意识的活动[14]。

全面提供建议指导，保卫私营企业数据安全。英国政府将650万英镑的计划资金用于网络安全教育，出台了《保证网络安全10个步骤》等一系列帮助大中小型企业应对和管理网络安全风险的文件，并发布了“安全上网”计划，为小型企业和公众提供广泛建议[8]。

（2）技术产业指标

①产业规模

在产业规模指标层面，7个国家（区域）的发展水平差异较大，数字产业规模、电子商务规模、电子政务发展水平和国内ICT基础设施建设水平是产业规模的衡量标准。美国的发展水平最为完善，优势在于国内软件企业、计算机服务产业在全世界拥有强大的影响力，美国软件企业在世界500强企业中所占数量超过300家，数字产业规模、电子商务规模在2015年也跃居世界第一。英国、德国、法国和日本的数字产业规模、电子商务规模和电子政务发展水平基本稳居世界前列，国内ICT基础设施建设水平较高，分别位居世界第4、第14、第17和第11。

②R&D投入

在R&D投入指标层面，7个国家（区域）对于R&D投入的重视程度存在一定差异，表现在R&D投入金额和其占GDP比例不同。其中日本处在绝对的领先地位，从2013年的1630亿美元到2015年的1645.9亿美元，在这3年一直蝉联R＆D投入金额世界排名的第3名，同时占GDP的比例基本维持在3.4%，远高于其他国家（区域）。美国和德国的R&D投入力度很大，投入资金连年提升，分别达到4968.4亿美元和1074.2亿美元，并在这3年一直蝉联R＆D投入金额世界排名的第1名和第4名。法国和欧盟的R&D投入程度一般，法国每年的R&D投入总额均占同年GDP总量的2.3%左右，在2015年其总额达到了592亿美元。英国的R&D投入只占2015年GDP总量的1.8%。

（3）网络治理指标

①网络治理参与

在网络治理参与指标层面，7个国家（区域）均较为完善。其中，美国和英国完善程度最高。美国和英国的优势在于积极参与地区和国际组织的网络合作与协调，并在制定跨国或国际组织的网络安全专项规则或法规的过程中发挥主导作用。相对而言，日本、法国和俄罗斯的不足之处在于对于国际网络安全专项规则制定以及国际互联网安全治理执法行动的参与度不高[15]。

成立国际网络治理机构，为国际合作提供制度保障。美国与日本、北约等国家和组织构建了网络安全伙伴关系，与韩国针对朝鲜形成了遏制网络威胁的一体化战略[16]。日本主动性强，在《日美防卫合作指针》的基础上，与美国、意大利、以色列等国在网络安全治理上展开了频繁的合作[17]。英国成立了国际网络安全保护联盟和全球网络安全中心，来促进各国网络安全治理合作。

积极开展多边研讨会，落实国际立法、司法和执法工作。法国积极参与欧盟、北约、欧洲安全与合作组织、联合国等地区或国际组织网络安全策略的制定[18]。欧盟各国共同制定了《欧盟数据总规》，为国际间网络治理提供了制度保障[19]。

②网络应急处置

截至2015年，7个国家（区域）的发展程度相对均衡，基本都建立起相应的网络应急处置机制，并且积极寻求国际合作，定期开展网络安全演习。

美国发展较为完善，有着较为成熟的黑客攻击预防机制和较为强大的网络反恐能力。美国在计算机安全应急响应方面，由美国国土安全部运营的US-CERT和由卡内基梅隆大学运营的CERT Coordination Center，有效支撑了全美范围内网络安全应急处置工作。2015年与北约举办的“锁定盾牌2015”是几场网络危机处理演习活动中规模最大的，并且从2015年开始，美国着力打造全球首个网络战场预警与防御系统。欧盟紧随美国，欧洲网络信息安全局(ENISA)发布了《CERT队伍建设指导文件》，并且在ENISA的组织下，各成员国积极参与网络安全演习，包括网络欧洲系列演习、北约组织的演习等。德国也建立了较完善的网络应急处置机制，包括CERT、CERT-BUND、IT情况监测中心、IT应急响应中心和网络响应中心等机构[8]。

日本积极与美国和欧盟加强沟通与合作，参与国际网络安全演习和国际网络安全对话，正在形成一套日趋成熟的网络危机应急机制。同时英国也积

极开展国际合作演习，与美国联合举办了跨大西洋联合演习，牵头与其他8个欧洲国家组织了国际网络犯罪演习等。法国国防及国家安全总秘书处（SGDSN）每年开展4次主要网络安全演习，主要针对政府部门与私营合作伙伴之间的信息共享对接安全，其目标明确、方案完备。

（4）网络态势指标

关键信息基础设施战略规划指标：

在关键基础设施安全指标保障层面，7个国家（区域）的发展水平存在不平衡的状况，一些国家（区域）的优势在于其关键基础设施的专项网络安全战略及其目标、路线、实施主体和路径较为全面和明确。

美国所具有的强大的网络安全基础设施得益于它先进的网络技术与团队。2013年美国成立网络部队，包含保护美国重要基础设施的网络部队、协助海外部队策划并执行网络袭击的“进攻性”部队，以及保护国防部内部网络的“防卫性”部队。同时国防部的系统升级为具有自我修复功能的云架构。美国政府还开展对于网络安全基础设施的投入与建设，如2013年奥巴马发布的《提升关键基础设施网络安全》行政令，2014年通过的《网络空间安全框架》都是有力举措[4]。英国建立了完善的关键基础设施的专项战略及配套政策，设立了国家基础设施保护中心（CPNI），同时，推进关于保护国家关键基础设施的研究，发布了《网络安全与英国关键国家基础设施报告》等。

德国2003年发布了鉴别关键基础设施方法和保护方法，随后发布一系列专项文件，并适时对相关战略和方法进行评估和优化。11欧盟2013年以前发布了《关键基础设施保护欧洲规划》和《欧洲关键基础设施指令》2个关键政策文件。在ENISA的组织下，欧盟各成员国在泛欧网络安全演习中开展针对关键基础设施的演练，ENISA在演习的基础上发布报告，对关键基础设施的保护方法进行评估与更新[7]。

对我国网络安全工作的几点启示

根据网络空间安全国际指数的评价结果，部分国家（区域）均对网络空间安全给予高度重视，出台相应政策并贯彻实施。在总结归纳部分国家（区域）宝贵经验的基础上，对完善我国网络安全保障体系有以下几点启示：

1）健全网络安全战略体系和管理制度

我国的网络安全治理体系已初步完善，但仍需要在以下方面进行完善：①逐步完善我国网络安全战略体系，做到指导方针与具体措施、战略规划与配套政策相结合，构建常规性的战略规划评估机制；②加快推进我国网络安全法律法规建设，形成以宪法为核心、以法律为主干的多层次网络安全法律体系，做到依法治网，保护我国各类网络行为主体的合法权益；③积极打造多层级的网络信息共享机制，建立主体清晰、权责明确的联动机制，在推进跨部门、跨行业信息共享的基础上实现全国性的网络信息一体化；④多措并举增强社会公众网络安全意识，普及网络安全的基础知识和技术，动员媒体、企业、高校、民众共同营造健康网络环境。

2）科学布局我国信息安全技术产业

①整合产业链条，打造整体优势。在持续推进杀毒、入侵防范等中游产业发展的同时，加大对关键芯片安全、操作系统安全、基础密码算法等上游核心技术产业和下游信息安全服务业的扶持力度，形成协同发展优势。充分发挥主管部门和行业协会作用，打造确保信息安全的产业联盟。②做好产业服务，规范行业管理。出台产业配套政策，支持优势企业“走出去”做大做强，形成一批具有国际竞争力的信息安全企业。发挥国家级专业孵化器职能，鼓励创业和促进中小企业发展，做好服务工作，壮大产业基石。加强行业监管，规范市场秩序，赢造公平的竞争环境，避免企业间的恶性竞争。③加大财政投入，鼓励社会投资。国家增加财政拨款，建立信息安全产业发展基金。采用项目贴息贷款、补助、奖励等方式滚动使用，用于信息安全关键技术、重点产品开发和产业化生产，创造良好的融资环境。鼓励风险投资，允许通过多种渠道筹集资金，建立信息安全产业风险投资基金，以此带动社会资本对信息安全产业的投资。

3）重视国际合作、协作与交流

①着眼于统筹国内国际2个大局，积极拓宽网络与信息安全国际合作渠道，建立多层次的双边和多边合作机制，建立高层互访、安全对话、学术交流和信息共享等平台和制度，逐步形成各国参与、普遍受益的网络与信息安全格局。②借助G20、上合组织等国际机构，与美国、欧盟、俄罗斯等国家和地区建立双边、多边合作关系，通过签订备忘录、研讨会等形式，在信息安全立法、标准制定、人才培养、情报共享、打击犯罪、应急演练、公共基础设施保护等方面，加强协

作与交流，创造有利于保障我国信息安全的国际环境，提升我国在国际信息安全领域的影响力和主动权。③积极参与网络安全国际规则制定。在充分尊重各国主权和社会政治制度的基础上加强立法、执法的合作，共同打击网络违法犯罪行为，打击网络恐怖活动。加强信息安全技术标准化领域的合作交流，积极参与国际信息安全技术标准的制订。

总　结

随着信息与通信技术在社会各个领域的深化应用，网络空间成为传统的军事、经济、金融方面之外国际间较量的新领域。网络资源已经成为各国争夺的重要战略资源，网络安全威胁也成为各国政府面临的新挑战。当前，我国正处于信息化发展的新时期。大数据发展、政府数据开放共享以及智慧城市建设深化推进，成为促进经济社会发展的重要驱动力量。但同时，网络技术的广泛渗透、数据的高速汇聚、智能技术的应用延伸，给网络安全工作也带了前所未有的挑战。

本文选取了部分国家（地区）作为研究案例，综合整理了各国（地区）截至2015年的网络安全保障建设方面的数据，分析度量了宏观管理、技术产业、网络治理、网络态势4个方面的12项网络安全治理指标情况，并通过特定权重和量化计算方法，研究评估了各国网络安全状况。最后，从宏观管理、技术产业、国际合作等方面提出了对我国网络安全工作的启示。

参考文献

[1] Homeland Security. Cybersecurity[OL].[2016-07-02]. https://www.dhs.gov/topic/cybersecurity

[2] 李婧, 刘洪梅, 刘阳子.国外主要国家网络安全战略综述[J]. 中国信息安全,2012(7):34-37

[3] ENISA (European Union Agency for Network and Information Security). Germany- “Digital Agenda 2014-2017”[EB/OL]. (2014-08-20)[2016-07-05]. https://www.enisa.europa.eu/about-enisa/structure-organization/national-liaison-office/news-from-the-member-states/digital-agenda-2014-2017- adopted-by-federal-cabinet-on-20-august-2014

[4] 刘勃然.21 世纪初美国网络安全战略探析[D]. 长春: 吉林大学,2013

[5] 由鲜举, 田素梅.2014 年《英国网络安全战略》进展和未来计划[J]. 中国信息安全,2015(10):83-86

[6] 李晓飞. 试析英国的网络安全治理[D]. 北京: 外交学院, 2014

[7] GOV.UK. UK cyber security strategy: Statement on progress 2 years on[EB/OL]. (2013-12-12)[2016-07-10]. https://www.gov.uk/government/speeches/uk-cyber-security-strategy-statement-on-progress-2-years-on

[8] 张彬彬. 英国网络安全现状研究[J]. 中国信息安全,2014(12):98-100

[9] 郝晓伟, 陈侠, 杨彦超. 俄罗斯互联网治理工作评析[J]. 当代世界,2014(6):70-73

[10] 王星. 英国网络安全人才队伍建设体制研究[J]. 中国信息安全,2015 (11):101-103

[11] GOV.UK. Cyber essentials scheme: Overview[EB/OL]. (2014-04-07)[2016-07-12]. https://www.gov.uk/government/publications/cyber-essentials-scheme-overview.

[12] 雷小兵, 黎文珠.《欧盟网络安全战略》解析与启示[J]. 信息安全与通信保密,2013(11):52-59

[13] 李广乾, 谢丽娜. 全球化背景的网络安全新思维: 他国镜鉴及其下一步[J]. 改革, 2014(8):19-28

[14] 饶晔, 刘润生, 张丽娟. 智库建言德国网络安全研究战略[J]. 科学中国人,2014(10):19-22

[15] 李淑华. 俄罗斯加强网络审查状况分析[J]. 俄罗斯东欧中亚研究,2015(6):64-70

[16] 陈明奇, 姜禾, 张娟, 廖方宇. 大数据时代的美国信息网络安全新战略分析[J]. 信息网络安全,2012(8):32-35

[17] 杨冠天. 日本网络安全战略探析[D]. 长春: 吉林大学,2015

［18］刘权，方琳琳．法国信息系统防御和安全战略[J]．中国信息安全,2011(10):66-70

［19］周秋君．欧盟网络安全战略解析[J]．欧洲研究,2015(3):60-78

作者：吕欣，国家信息中心博士后工作站处长、研究员