美日网络安全合作机制论析 *

江天骄

【内容摘要】 由于网络安全领域缺乏明确的国际法规则约束，加之网络技术的相关特点，导致网络黑客、窃密、大规模网络攻击等网络安全事件频发。在此背景下，美国和日本围绕网络安全进行了长期深入合作，并取得了一定成效。美日同盟向网络空间延伸是美国的传统同盟体系向网络空间扩展的典型案例，或将对全球网络空间战略稳定带来较为复杂的影响。从美日网络安全合作的发展历程来看，美国在合作中处于引领地位，而日本则对美国提出的相关理念和战略行动具有较高的认同度，并快速学习进而转化为自身的网络安全战略。从具体合作机制看，美日两国启动了多层次的网络安全对话合作机制，从宏观战略和微观政策上规划与落实网络安全合作，聚焦民用网络安全、军事网络安全和国际规则合作三大领域。然而，在当前国际社会难以就界定网络攻击达成普遍共识的情况下，美日两国通过主观性较强的判定标准，并机械地套用传统安保体系来应对重大网络安全事件，容易引发误判甚至导致冲突升级。

【关键词】 美日同盟　网络安全　共同防御　灰色地带　国际规则

【作者简介】 江天骄，复旦大学发展研究院讲师，复旦大学网络空间国际治理研究基地兼职研究员（上海　邮编：200433）

【中图分类号】 D815.5　D871.22　**【文献标识码】** A

【文章编号】 1006-1568-(2020)06-0127-19

【DOI 编号】 10.13851/j.cnki.gjzw.202006007

* 本文系国家社科基金重大项目“总体国家安全观视野下的网络治理体系研究”（17ZDA106）和教育部青年基金项目“全球网络空间的战略稳定性研究”（19YJCGJW004）的阶段性成果。感谢王蕾、陈云轩以及匿名评审专家对本文写作和修改提出的宝贵意见。

2019 年，美日两国确认网络攻击适用于《美日安保条约》，标志着美日同盟从物理空间全面向网络空间延伸。这是以美国为核心的传统同盟体系向网络空间扩展的典型案例。其主要有三个特点，一是在合作模式上，美国发挥引领作用，日本对美国提出的网络安全相关理念和行动战略都具有较高的认同度，并快速学习转化为自身的网络安全战略。特别是自 2010 年以来，美日双方都陆续推出了国家网络安全战略和网络空间国际合作战略，并建立网络部队，加强政策话语体系的融通和网络攻防能力建设的协调。二是在合作机制化程度上，美、日两国以新版《美日防卫合作指针》和《美日安保条约》作为法律依托，通过首脑对话、安保磋商、网络对话等磋商机制，实现了从政治、经济到军事、安全的全方位“无缝合作”。三是在合作效果上，两国政府不仅明确表达了深化合作的意愿，而且这种以传统军事同盟向网络空间扩展的合作方式将对地区乃至世界其他国家产生示范效应，由此可能加剧网络空间的“巴尔干化”[①]，并形成多个政治乃至军事集团，从而对全球网络空间战略稳定产生较为复杂的影响。[②]

值得注意的是，美日网络安全合作深刻反映出美日同盟背后的张力。尽管两国政府在网络空间这一新兴领域的明确合作意愿以及大量合作实践为美日同盟进一步深化注入了新的动力，但双方应对网络安全挑战的战略目标及政策偏好仍然存在结构性差异。美国主要试图整合包括日本在内的全球盟友资源，以有效遏制甚至挫败所谓“修正主义国家”试图颠覆全球网络空间秩序与美国霸权的行为。而日本则更注重从两国网络安全合作中得到安全承诺与集体防卫自由，借助网络空间行为的模糊性与不确定性为本国军事行动松绑。这种差异将使双方在维护网络安全的责任划分、合作的紧密程度等方面展开博弈，也使双方在更具进攻性的网络行动方面协调一致，从而对全球网络空间的战略稳定造成冲击。本文拟梳理美日网络安全合作的发展历程与核心内容，进而分析两国开展网络安全合作的方式及其特点，并研判其对全

① Marshall Van Alstyne and Erik Brynjolfsson, “Could the Internet Balkanize Science?” *Science*, Vol. 274, No. 5292, November 1996, pp. 1479-1480.

② 周宏仁：《网络空间的崛起与战略稳定》，《国际展望》2019 年第 3 期，第 21—34 页。

球网络空间战略稳定可能造成的影响。

一、美日网络安全合作历程与现状

美日两国在网络安全政策方面的契合度较高，具体表现为日本对美国提出的网络安全相关概念及其主张的快速学习、认同并转化为自身的网络安全战略。这为双方持续深化的网络安全合作奠定了坚实基础。除此之外，双方还通过建立多层次的对话和协调机制，持续推进在民用网络安全、军用网络安全和国际规则领域的合作。

（一）美日网络安全合作历程

早在 21 世纪初，日本就充分认识到信息技术对摆脱经济停滞、提升国际竞争力的重要作用。而这一认知与美国克林顿政府时期提出的“信息高速公路”计划以及“知识经济”所取得的巨大成功密切相关。2000 年日本内阁设立 IT 战略本部，由时任首相森喜郎担任本部长。同时，美日两国在 2000 年前后都出台了一系列针对信息安全和网络通信基础设施防护的国内法律文件。[①] 然而，随着网络相关技术的不断发展，网络空间逐步成为国家间政治、经济乃至军事竞争的焦点。尤其是在 2010 年前后，一系列重大网络安全事件的集中爆发已经完全超出了传统信息安全的范畴。起初，西方国家纷纷指责俄罗斯对爱沙尼亚和格鲁吉亚发动网络攻击，谋求地缘优势。随后，美国监听全球的“棱镜”项目不仅很快被曝光，而且还伙同以色列对伊朗的铀浓缩设施发动“震网”病毒攻击。几乎在同一时期，网络平台还成为中东地区国家政局普遍动荡的重要推手。在这一重要背景下，美国奥巴马政府将网络空间安全威胁视为最严重的国家经济和安全挑战之一，并迅速设立了网

① U.S. Congress, “S.982-National Information Infrastructure Protection Act of 1996, the 104th Congress (1995-1996),” June 29, 1995, https://www.congress.gov/bill/104th-congress/senate-bill/982?r=17&s=1; U.S. Congress, “S.1993-Government Information Security Act, the 106th Congress (1999-2000),” November 19, 1999, https://www.congress.gov/bill/106th-congress/senate-bill/1993; U.S. Congress, “H.R.3844-Federal Information Security Management Act of 2002, the 107th Congress (2001-2002),” March 5, 2002, https://www.congress.gov/bill/107th-congress/house-bill/3844; and Prime Minister of Japan and His Cabinet, “Basic Act on the Formation of an Advanced Information and Telecommunications Network Society, Act No. 144 of December 6, 2000,” December 6, 2000, https://japan.kantei.go.jp/it/it_basiclaw/it_basiclaw.html.

络司令部。美国一方面强调对关键基础设施的保护，强化网络攻防能力建设；另一方面在网络空间积极推行所谓“互联网自由”战略，旨在建立“开放、互通、安全、可靠”的全球网络空间，并积极与盟友和伙伴组建“意愿联盟”，构筑网络空间的“集体防御”机制。①

正是在网络安全国际形势和美国网络安全战略的影响下，日本才逐步形成了目前的网络安全战略。在 2011 年度的《防卫白皮书》中，日本首次将网络攻击列为其面临的首要安全威胁，并建立了网络空间防卫队。② 2013 年，日本发布了第一份《网络安全战略》以及《网络安全国际合作方针》，跳出了聚焦于信息安全技术的传统框架，强调应对网络安全带来的综合性挑战。③ 2014 年，日本出台《网络安全基本法》并正式组建与陆、海、空、天并列的网络防卫队。2015 年，日本发布第二版《网络安全战略》，增加了“确保自由、公平和安全的网络空间”的愿景、目标，与美国的网络安全战略主张高度契合。④ 2018 年，日本又推出了新版《网络安全战略》，在继承此前相关愿景、目标和基本原则的基础上，进一步阐明了具体行动计划、体制机制建设和国际合作战略。⑤

（二）美日网络安全合作机制

在日本积极向美国借鉴并逐步确立新时期网络安全战略的同时，美日两国网络安全合作的机制化进程也日益深化。尤其是在安倍晋三第二次执政后，美日两国通过领导人峰会将网络议题磋商提升至政府首脑级别，使双边网络安全合作机制的发展进入快车道。由外交部长、国防部长参加的“美日安保磋商委员会”（“2+2”）会议，明确将网络安全议题纳入其中，并对

① *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*, Washington, D.C.: White House, May 2011, https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

② *Defense of Japan 2011*, Tokyo: Japanese Defense Ministry, August, 2011, https://www.mod.go.jp/e/publ/w_paper/2011.html.

③ *International Strategy on Cybersecurity Cooperation*, Tokyo: Information Security Policy Council, October 2, 2013, https://www.kantei.go.jp/jp/singi/it2/dai63/siryou9-2.pdf.

④ *Cybersecurity Strategy*, Tokyo: Information Security Policy Council, September 4, 2015, https://www.nisc.go.jp/eng/pdf/cs-strategy-en.pdf.

⑤ *Cybersecurity Strategy*, Information Security Policy Council, July 27, 2018, https://www.nisc.go.jp/eng/pdf/cs-senryaku2018-en.pdf.

后续的美日网络安全合作起到整体的政策设计、评估和协调作用。[①] 在这一部长级磋商机制之下，还包括三个司局级工作组专门负责特定领域的网络安全合作。其中，美日网络安全对话已举行过七次，旨在通过定期交换网络威胁情报，协调政府间网络安全政策，保护关键基础设施。[②] 此外，两国防务部门之间还成立了“网络防御政策工作组”（Cyber Defense Policy Working Group, CDPWG），聚焦于网络防御政策磋商、网络军事能力建设以及双边演习和推演等。[③] 另外，美日网络经济政策会谈主要围绕双方数字经济合作展开，同时部分涉及如何就保障商业网络安全问题加强合作。[④] 总体上，美日网络安全合作既包括宏观层面的战略对话，也包括微观层面的具体合作措施（见图 1）。

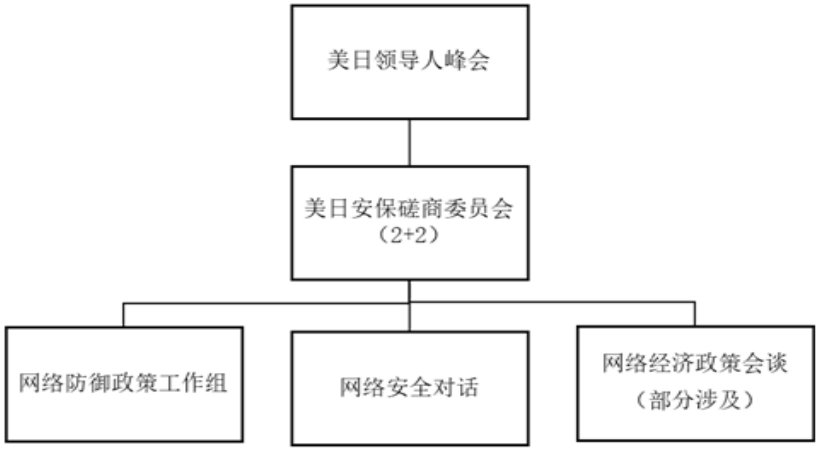

图 1　美日网络安全合作机制层次示意图

资料来源：作者自制。

① Japanese Foreign Ministry, “Joint Statement of the Security Consultative Committee: Toward a Deeper and Broader U.S.-Japan Alliance: Building on 50 Years of Partnership,” June 21, 2011, https://www.mofa.go.jp/region/n-america/us/security/pdfs/ joint1106_01.pdf.

② Japanese Defense Ministry, “Joint Statement of the Security Consultative Committee: Toward a More Robust Alliance and Greater Shared Responsibilities,” October 3, 2013, https://www.mod.go.jp/e/d_act/us/pdf/JointStatement2013.pdf, p. 4.

③ Japanese Defense Ministry, “Joint Statement of the U.S.-Japan Cyber Defense Policy Working Group,” May 30, 2015, https://www.mod.go.jp/j/press/news/2015/05/30a_1.pdf.

④ U.S. Department of State, “First Director-General Level U.S.-Japan Dialogue on the Internet Economy,” November 1, 2010, https://2009-2017.state.gov/r/pa/prs/ps/2010/11/150264.htm.

在宏观层面主要以美日领导人峰会以及美日安全磋商委员会会议为代表，为双方的网络安全合作定下基调；而在落实相关技术性问题时，双方又借助网络安全对话、网络防御政策工作组以及网络经济政策会谈等常态化磋商机制加以推进。从具体合作内容和战略目标看，日本学者曾把施行《美日防卫合作指针》、共同保护海底光缆和共享网络情报作为三大合作领域。[①] 而事实上随着双边合作的不断推进，相关合作机制既包括保障商业网络安全、防护关键基础设施、协调政府间网络安全政策等偏向民用领域的安全合作，又涵盖网络部队建设、网络空间联合行动以及防御政策磋商等偏向军事领域的合作。两者相辅相成，构成了全方位的网络安全合作体系。此外，由于网络空间缺乏公认的国际规范和行动原则，探讨国际法如何适用于网络空间也是美日两国网络安全合作的重要内容。在此基础上，美日同盟向网络空间延伸将对美国全球同盟体系产生示范效应，并谋求为全球网络空间建章立制。

二、美日在民用网络安全领域的合作机制

在民用网络安全领域，自开启网络安全对话以来，美日两国即强调合作的首要任务在于促进各自的网络安全保障能力建设。网络安全保障能力主要是应对网络安全风险的能力，即在真正的网络攻击发生之前评估网络安全风险，并通过网络安全技术的应用等提升信息系统的稳健性和恢复力，从而防范安全风险的发生，增强网络攻击出现时的应对能力并使损失最小化。

（一）以安全威胁信息共享推动民用网络安全合作

2017 年以来，美日两国分别为提升各自的网络安全保障能力进行了积极努力。例如，美国国土安全部在 2018 年发布网络安全战略，其核心内容在于为联邦政府按照一定流程评估和应对网络安全风险提供指导。[②] 在同一年发布的日本网络安全战略中，日本政府则将网络安全责任体系和风险管理

① 土屋大洋：『日米サイバーセキュリティ協力の課題』、笹川平和财团、2016 年 3 月、https://www.spf.org/topics/WG1_report_Tsuchiya.pdf。

② *Cybersecurity Strategy* Washington, D.C.: Department of Homeland Security, May 15, 2018, https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf.

确定为保障网络安全的关键路径。[①] 在此基础上，网络安全保障能力建设成为两国间对话机制关注的重点。2019 年美日安保磋商发布的联合声明强调，尽管双方将在网络威慑和响应能力等方面加强合作，但提升各自对信息系统和关键基础设施的保护仍是两国政府的优先目标。[②]

具体而言，共享有关网络安全威胁和风险的信息是美日两国提升各自网络安全保障能力的重要内容。对于网络安全风险的防控来说，掌握充分的网络安全威胁信息是评估风险、发布预警并做出相关决策的基础。信息共享可助力更及时和充分地获知并预判网络安全风险。自首次网络安全对话以来，美日两国都强调交流和共享与网络风险相关的信息的重要性。[③] 为此，2017 年 5 月，日本内阁网络安全中心宣布将加入美国国土安全部的“自动指标共享”（Automated Indicator Sharing）项目。该项目旨在促进网络安全威胁指标在公共部门和私营部门之间的流动，以强化并逐步整合各部门提前防范网络攻击的能力。[④] 这一合作意味着美日双方将在跨国、跨部门的范围内共享有关网络安全威胁的信息，从而迈出了网络安全信息实时共享的关键一步。

（二）以最佳实践优化政府及产业网络安全保障体系

网络安全保障能力建设方面的最佳实践是双方民用领域合作的重点，网络安全保障的核心在于信息系统的运行者及相关部门为预判和应对网络安全风险而提出一系列应对方案并予以落实。受各国战略文化、决策方式不同等因素影响，管控网络安全风险的具体路径和方式存在一定差异。例如，在私营部门对网络安全的管控方面，只有 55％的日本公司进行网络安全风险评估，而美国约为 80％；只有 27％的日本公司设有首席信息安全官，而美国公司为 78%。[⑤] 与美国不同，在日本，将网络安全整合到公司治理中是一

① *Cybersecurity Strategy* Tokyo: National Center of Incident Readiness and Strategy for Cybersecurity, July 27, 2018, https://www.nisc.go.jp/eng/pdf/cs-senryaku2018-en.pdf.

② Japanese Foreign Ministry, “Joint Statement of the Security Consultative Committee,” April 19, 2019, https://www.mofa.go.jp/files/000470738.pdf.

③ Ministry of Foreign Affairs, Japan, “Joint Statement of Japan-US Cyber Dialogue,” May 10, 2013, https://www.mofa.go.jp/region/page22e_000001.html.

④ Japanese Foreign Department, “Automated Indicator Sharing (AIS),” https://www.dhs.gov/cisa/automated-indicator-sharing-ais.

⑤ 「企業の CISO や CSIRT に関する実態調査 2017 年調査報告書」、情報処理推進機構 IPA、2017 年 4 月 13 日、https://www.ipa.go.jp/files/000058850.pdf。

个相对较新的概念，只有约 1/5 的日本企业会将网络安全视为提升自身竞争力的重要因素。[①] 绝大部分日本企业高管不仅缺乏关于网络安全的专业知识和经验，而且将网络安全相关投入视为巨大的成本而非投资，不愿将相对有限的预算投入到风控、运营和技术部门。[②]

美日两国在网络安全合作中认识到这一点，并指出加强网络安全风险管控的必要性。[③] 这不仅有助于增强双方在共同制定网络安全保障方案时的默契，也将帮助美日两国完善各自网络安全保障方案。尤其是在 2017 年勒索病毒（WannaCry）席卷全球的背景下，美日两国开始进一步反思其国内网络安全治理架构，并为私营部门提出改善网络安全和应对紧急事态的最佳实践方案。其中，日本经济产业省和信息处理推进机构（Information-Technology Promotion Agency, IPA）共同为企业修订的“网络安全管理指南”，明确将美国国家标准技术研究所（National Institute of Standards and Technology, NIST）制定的网络安全框架作为参照标准，要求企业建立以首席信息官制度为代表的应对网络安全风险管理架构，增强企业从网络攻击中快速恢复的弹性，优化对关键资产的网络保护，定期进行网络风险评估，并加强供应链安全审核。[④] 在此基础上，美、日两国在合作中尤其注重构建全政府（whole-of-government）的网络安全战略。两国的国家网络安全战略都强调，面对复杂的网络安全挑战，需要以跨部门、跨领域的综合手段予以应对。有效的网络风险防控体系应以覆盖所有政府部门乃至私营部门为目标。两国一致认为，应合作维护各自的全政府网络安全保障体系。[⑤]

以信息共享和实践交流为引导，各自建立全政府的网络安全保障体系是美日应对民用领域网络安全挑战的积极尝试。长期以来，日本在网络安全风

① 「平成 28 年度　企業のサイバーセキュリティ対策に関する調査報告書」、ニュートン・コンサルティング株式会社、2017 年 3 月、https://www.nisc.go.jp/inquiry/pdf/kigyoutaisaku_honbun.pdf。

②「サイバーセキュリティ経営ガイドライン Ver 2.0」、経済産業省、2017 年 11 月、https://www.meti.go.jp/press/2017/11/20171116003/20171116003-1.pdf。

③ U.S. Department of State, “Joint Statement of the Japan-U.S. Cyber Dialogue,” July 24, 2017, https://www.state.gov/joint-statement-of-the-japan-u-s-cyber-dialogue/.

④ 「サイバーセキュリティ経営ガイドライン Ver 2.0」。

⑤ Japanese Foreign Ministry, “Joint Statement of Japan-US Cyber Dialogue.”

险保障方面的一个主要短板在于资源投入较为有限。[①] 同时，与较早开始关注网络安全建设的美国不同，日本政府是在受到一系列国内外事件影响后，直到 2010 年前后才开始启动有关网络安全事务的整体战略规划，对网络安全风险防控的经验相对不足。在此情况下，尽管军事上依赖与美国的联合防御能在一定程度上弥补日本的能力欠缺，但联合防御的覆盖范围有限，且成本较高，难以全面、及时应对民用领域日益增长而又复杂的网络安全风险。因此，对日本而言，根本性解决方案是突出跨部门、跨领域协调，建立全政府的网络安全保障体系。此外，美日两国的网络安全保障能力处于不均衡的状态，美日在当前的合作中以保护者和被保护者的角色出现，从而制约了两国共同探索网络安全保障方案的空间。从这个意义上说，促进各自网络安全保障能力建设将为美日两国开展更为广泛的网络安全合作奠定重要的基础。

三、美日在军事网络安全领域的合作机制

除强化民用领域的网络安全保障能力建设外，美日通过双方军事合作来应对潜在或现实的网络攻击。在 2013 年的美日安保磋商中，双方明确将共同应对军事领域的网络威胁作为修订《美日防卫合作指针》的目标之一。[②] 2015 年发布的新版《美日防卫合作指针》明确提出两国将合作保护对双方军队具有重要意义的关键信息基础设施与服务的安全，并规划了共享网络空间军事情报和开展联合军事行动的路径。[③] 其中，网络威慑、共同防御和应对“灰色地带”挑战 [④] 构成了美日网络军事安全合作的主要内容。网络威慑主要针对大规模网络攻击；共同防御既为网络威慑提供技术支撑，又是威

① James Andrew Lewis, “U.S.-Japan Cooperation in Cybersecurity,” Center for Strategic and International Studies, November 2015, https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/151105_Lewis_USJapanCyber_Web.pdf.

② Japanese Defense Ministry, “Joint Statement of the Security Consultative Committee: Toward a More Robust Alliance and Greater Shared Responsibilities,” October 3, 2013, https://www.mod.go.jp/e/d_act/us/pdf/JointStatement2013.pdf.

③ Japanese Foreign Ministry, “The Guidelines for Japan-U.S. Defense Cooperation,” April 27, 2015, https://www.mofa.go.jp/files/000078188.pdf.

④ 戴正、洪邮生：《美国学界对“灰色地带”挑战的认知》，《国际展望》2019 年第 4 期，第 79—97 页。

慑失效后的最后防线，是对网络威慑的补充；应对“灰色地带”挑战则针对难以被有效威慑和防御的恶意网络活动，采取更加积极主动的军事行动。三者相辅相成，构成一体化的军事网络安全协同体系。

（一）以政策宣示强化网络威慑战略

美日同盟的一项重要支撑是美国长期为日本提供核保护伞，并实施延伸核威慑。自 2011 年美国国防部将网络空间作为美军第五大“行动领域”以来，美国的延伸威慑战略正向网络空间拓展。[①] 美日安保磋商及网络安全对话也多次论及如何构建网络空间的延伸威慑。与核威慑不同，网络威慑和反击更为复杂，关于核领域的延伸威慑能否有效应用于网络空间存在很大争议。[②] 针对网络攻击采取报复措施的公开承诺将有助于提升网络威慑的可信度，因此，新版《美日防卫合作指针》指出，当发生威胁日本国家安全的严重网络攻击事件时，两国政府将密切磋商并采取适当行动予以积极应对。[③] 两国有关反击措施的表态从政治上强化了网络威慑。

在此基础上，2019 年的美日安保磋商联合声明进一步表示，在特定情况下，网络攻击将被视为在《美日安全保障条约》第 5 条界定范围内的武装攻击。[④] 根据这一条款，在日本境内对于两国中的任意一方发起的武装攻击将被视为危及和平与安全，两国对此将采取实际行动予以应对。[⑤] 新版《美日防卫合作指针》提出，在发生针对日本和驻日美军的网络袭击时，由日本承担主要应对责任，美国则提供妥善支持，与之不同的是，此次联合声明明确了一旦网络攻击被认定为武装攻击，美国将担负起军事应对的主要责任。

① 川口貴久『サイバー空間における安全保障の現状と課題』、日本国際問題研究所、http://www2.jiia.or.jp/pdf/resarch/H25_Global_Commons/03-kawaguchi.pdf。

② Martin C. Libicki, *Cyberdeterrence and Cyberwar*, Santa Monica: RAND Corporation, 2009, pp. 104-106; Richard J. Harknett, John P. Callaghan, and Rudi Kauffman, “Leaving Deterrence Behind: War-Fighting and National Cybersecurity,” *Journal of Homeland Security and Emergency Management*, Vol. 7, No. 1, 2010, p. 9; David D. Clark and Susan Landau, “Untangling Attribution,” *Harvard National Security Journal*, Vol. 2, No. 2, March 2011, pp. 25-40; and P.W. Singer and Allan Friedman, *Cybersecurity and Cyberwar*, New York: Oxford University Press, 2014, p. 73.

③ Japanese Foreign Ministry, “The Guidelines for Japan-U.S. Defense Cooperation.”

④ Japanese Foreign Ministry of Foreign, “Joint Statement of the Security Consultative Committee,” April 19, 2019, https://www.mofa.go.jp/files/000470738.pdf.

⑤ Japanese Foreign Ministry of Foreign Affairs, “Japan-U.S. Security Treaty,” https://www.mofa.go.jp/region/n-america/us/q&a/ref/1.html.

这充分表明美国在军事上保障日本的网络安全的承诺升级，也体现了两国有效实施网络威慑、反击以及网络延伸威慑有效性的信念。[①] 这一政策宣示具有标志性意义，不仅是美日同盟向网络空间延伸的重大突破，也是美国通过其全球联盟体系来构筑网络空间集体防御机制的关键一步。

（二）以共同防御提升网络威慑的基础

除了强化关于网络威慑的政策宣示之外，进一步提升网络攻防能力建设也是确保网络威慑可信度的关键。其中，共同防御促使美日两国尤其是能力建设相对不足的日本通过将网络安全事务迅速军事化的办法，获得更大的政策支持和资源。[②] 尽管日本政府在网络安全战略规划方面起步较晚，但其国家安全战略正逐步将关键基础设施及政府部门等面临的网络安全风险和威胁视作与传统的军事攻击等同的重大国家安全挑战，并将军事化手段作为应对网络安全挑战的优先方案。[③] 这一取向给美日两国应对网络安全挑战赋予越来越多的军事意义，并使网络安全在国防中日益处于核心地位。与传统的军事力量不同，网络攻防的实施需要有不断更新的网络安全技术和在信息技术方面专业化的网络部队，且鉴于归因困难以及国际规范欠缺等，成功实施网络威慑和反击的难度相对较大。为此，2018 年以来美日两国在网络部队的建设方面投入巨大。[④] 共同防御是双方网络部队合作的重点，一方面，共同防御为网络威慑提供必要的网络空间态势感知及溯源能力，是网络威慑的基础；另一方面，一旦网络威慑失效，良好的共同防御还能有效抵御网络攻击，确保系统的弹性，是网络威慑的补充。[⑤]

① Indo-Pacific Defense Forum, “Cyber Threats Prompt Japan, U.S. to Bolster Cooperation,” May 16, 2019, https://ipdefenseforum.com/2019/05/cyber-threats-prompt-japan-u-s-to-bolster-cooperation/.

② Paul Kallender and Christopher W. Hughes, “Japan’s Emerging Trajectory as a ‘Cyber Power’: From Securitization to Militarization of Cyberspace,” *The Journal of Strategic Studies*, Vol. 40, No. 1-2, 2017, pp. 118-145.

③ Japanese Foreign Ministry, *National Security Strategy*, December 17, 2013, https://www.mofa.go.jp/fp/nsp/page1we_000081.html.

④ Japanese Defense Ministry, “Medium Term Defense Program (FY2019-FY2023),” December 18, 2018, https://www.mod.go.jp/j/approach/agenda/guideline/2019/pdf/chuki_seibi31-35_e.pdf; and The White House, *Cybersecurity Funding*, March, 2019, https://www.whitehouse.gov/ wp-content/uploads/2019/03/ap_24_cyber_security-fy2020.pdf.

⑤ Patrick M. Morgan, “Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm,” in National Research Council of the National Academies, *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S.*

（三）以联合行动应对“灰色地带”的挑战

尽管打造了强有力的网络威慑体系，但网络空间中仍然存在大量尚未触及武装冲突门槛的恶意活动。这些恶意活动难以被威慑，也防不胜防。为此，美日两国自 2010 年以来积极包装所谓“灰色地带”挑战的概念，[①] 并通过国内政治和法律进程为其灵活开展更为积极的网络军事行动背书。从目前公布的官方文件与相关研究来看，美、日双方对于“灰色地带”这一概念存在基本共识。两国一致认为“灰色地带”作为外交谈判与武力冲突之间的复杂行动状态，包括政治、经济、军事、科技等诸多领域，对国际秩序与两国国家安全构成了严重威胁，需要双方构建更为紧密的安全合作和共同防御机制。新版《美日防卫合作指针》正是在此背景下应运而生，致力于打造从平时到战时的“无缝合作”体系。日本随后出台的新安保法提出从“灰色地带事态”到“重要影响事态”再到“生存危机事态”依次递进的作战场景，为日本行使集体自卫权，动用军事力量介入地区冲突提供了法律依据。[②]

但同时需要认识到，美日两国由于地缘环境、核心利益以及军事力量的差异，在针对网络空间“灰色地带”挑战的具体策略与措施上各有侧重。美国将“灰色地带”行动视为“修正主义国家”在全球范围内对现有国际秩序的挑战，既涵盖领土主权、金融贸易等传统领域，又向网络、太空等新兴领域延伸。美国因而主张整合其优势资源，对挑战者进行回击与遏制，甚至先发制人。尤其是在所谓俄罗斯通过网络干涉美国 2016 年总统大选的刺激下，美国深刻认识到竞争对手可能通过网络活动获得不对称的战略优势。在特朗

Policy, Washington, D.C.: The National Academies Press, 2010, p. 75-76; Colin S. Gray, “Strategic Thoughts for Defence Planners,” *Survival*, Vol. 52, No. 3, June-July 2010, pp. 159-178; and Erik Gartzke, Jon R. Lindsay, “Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace,” *Security Studies*, Vol. 24, No. 2, 2015, p. 343.

① See U.S. Department of Defense, *Quadrennial Defense Review Report*, 2010, http://archive.defense.gov/qdr/QDR%20as%20of%2029JAN10%201600.pdf, p. 73; Michael Green et al., “Countering Coercion in Maritime Asia: The Theory and Practice of Gray Zone Deterrence,” Center for Strategic and International Studies, May 2017, p. 21, https://csisprod.s3.amazonaws.com/s3fs-public/publication/170505_GreenM_CounteringCoercionAsia_Web.pdf; Japanese Defense Ministry, *National Defense Program Guidelines for FY 2011 and Beyond*, 2010, http://59.80.44.100/www.mod.go.jp/e/d_act/d_policy/pdf/guidelinesFY2011.pdf, p.13; Japanese Cabinet Secretariat, *National Security Strategy*, December 2013, https://www.cas.go.jp/jp/siryou/131217anzenhoshou/nss-e.pdf.

② Japanese Foreign Ministry, Japan, *The Guidelines for Japan-U.S. Defense Cooperation*, April 27, 2015, https://www.mofa.go.jp/region/n-america/us/security/guideline2.html.

普政府发布的《国家网络安全战略》中，美国强调以跨领域战略应对复杂的网络威胁，[①] 其核心要义就是跳出网络安全应对网络安全挑战的传统思维，发挥美国在政治、经济、军事、外交以及盟友资源等多方面的比较优势。美国国防部则相应提出“持续接触”和“防御前置”的网络作战概念，进一步模糊了网络进攻和防御的界限，旨在以低烈度的持续行动瓦解对手的网络能力。[②] 为了充分发挥跨领域战略的优势，推行更具进攻性的网络安全战略，美国积极打造包括美日同盟在内的网络空间集体防御机制，既威慑对手使其不敢轻举妄动，又通过对全球盟友的示范效应来完善网络空间行为规则，从而维护美国主导下的霸权秩序。

日本方面则利用网络空间“灰色地带”的模糊特征，在与美国打造“无缝合作”体系的同时为自身军事化松绑。[③] 从政策上看，根据 2015 年版《网络安全战略》，日本主张各项网络安全措施应“从事后应对转为事前防御……从被动实施变为倡议主导”。[④] 2018 年版《网络安全战略》进一步提出“积极网络防御”，旨在通过政企合作、军民融合，以技术诱导来搜集攻击者的信息并与盟友共享。[⑤] 这种情报搜集行动本身就介于网络攻击和防御之间，并呼应了美军提出的“持续接触”和“防御前置”原则。与此同时，日本仿照美国以跨领域战略提升网络威慑能力，要求执法机关与自卫队密切配合，以多种手段回应网络攻击，甚至包括使用进攻性网络武器。[⑥] 从法律上说，对于大多数尚未达到武力攻击级别但可能侵犯日本主权或重大国家利益的

① White House, *National Cyber Strategy*, September 20, 2018, https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf.

② Paul M. Nakasone, “An Interview with Paul M. Nakasone,” *Joint Forces Quarterly*, Vol. 92, January 2019, pp. 4-9.

③ See Scott W. Harold et al., The US-Japan Alliance and Deterring Gray Zone Coercion in the Maritime, Cyber, and Space Domains, Santa Monica: RAND Corporation, 2017, https://www.rand.org/content/dam/rand/pubs/conf_proceedings/CF300/CF379/RAND_CF379.pdf.

④ Japanese Foreign Ministry, *National Security Strategy*, September 4, 2015, https://www.nisc.go.jp/eng/pdf/cs-strategy-en.pdf.

⑤ Japanese Foreign Ministry, *National Security Strategy*, July 27, 2018, https://www.nisc.go.jp/eng/pdf/cs-senryaku2018-en.pdf.

⑥ Japanese Foreign Ministry, *National Defense Program Guidelines for FY 2019 and Beyond*, December 18, 2018, https://www.mod.go.jp/j/approach/agenda/guideline/2019/pdf/20181218_e.pdf; and Japanese Defense Ministry, “Medium Term Defense Program (FY 2019 - FY 2023).”

网络活动，将由首相或国家安全保障会议决定是否做出（军事）回应。[①] 一旦相关行为构成“重要影响事态”甚至是“生存危机事态”，首相将获得采取军事介入的授权。[②] 然而，就连时任首相安倍晋三自己也承认，对网络冲突判断的主观性较强。[③] 除此之外，由于美日同盟已经延伸至网络空间，一旦美国认为必要，日本也应当援引集体防卫原则支援美国的网络空间行动。由此可见，日本正充分利用网络空间的模糊特征，以国内政治和法律进程加速实现网络空间军事行动的自由。通过主观判定事态的严重性，日本可以采取自卫或行使集体自卫权等手段进行反击，或者采取先发制人策略，从而在实质上突破和平宪法的限制，达到扩军修宪的目的。

四、美日在网络空间国际规则领域的合作

网络空间作为与现实世界紧密相联的新兴领域，尚未形成完善的国际法规与行为规则体系，因而成为各国采取非战非和强制行动的热点空间。无论是民用还是军用网络安全保障，都涉及对相关网络行动进行准确界定从而有效应对的问题。然而，由于网络空间的跨国性、互通性、虚拟性和军民两用性等技术特征，如何准确界定网络攻击的性质并开展溯源和执法始终存在困难。从全球层面来看，联合国政府专家组（United Nations Governmental Group of Expert, UNGGE）在这一问题上开展了多轮讨论。虽然绝大多数国家都能够接受将《联合国宪章》和主权原则继续适用于网络空间，但在面对网络攻击时应何时触发自卫或集体防御，以及如何约束甚至惩罚恶意网络行为等具体问题上仍然存在较大分歧。部分国际法学家试图通过《塔林手册》提出的以是否造成物理损伤后果来界定相关网络行动是否构成武装冲突或战争行为，但是这种观点同样未能得到国际社会的普遍认同；而对于网络报复行为

① Japanese Defense Ministry, *Defense of Japan 2014*, Chapter 2, October 31, 2014, https://www.mod.go.jp/e/publ/w_paper /pdf/2014/DOJ2014_2-2-1_web_1031.pdf.

② 高兰：《日本“灰色地带事态”与中日安全困境》，《日本学刊》2016 年第 2 期，第 12—28 页。

③ 「第 189 回国会（常会）答弁書」、平成 27 年 8 月 7 日、https://www.sangiin.go.jp/japanese/joho1/kousei/syuisyo/189/touh/t189221.htm。

是否需要满足比例原则，以及如何界定和应对武装冲突门槛以下的恶意网络活动等问题，则显得更加棘手。

（一）通过国内政治和法律进程塑造国际舆论

探讨现有国际法尤其是武装冲突法如何适用于网络空间，不仅是美日两国深入开展网络安全合作并采取联合行动的法理前提，而且是美国及其同盟体系向网络空间延伸并为全球网络空间活动建章立制的重要基础。为了突破目前国际法层面的僵局，美日两国主要以分步走的方式开展合作。根据 2019 年举行的美日安保磋商，日本受到的网络攻击是否被界定为武装攻击，将在美日两国进行协商的基础上，依据对具体事件和案例的分析判断来做出决定。[①] 换句话说，美日两国并未就如何适用国际法提出明确的标准，而是采取了一种具体问题具体分析的办法。在具体场景中，由于对攻击者的确认以及对攻击所造成的安全影响的评估等都存在较大的不确定性，是否将某次网络攻击界定为武装攻击，很有可能将取决于美日两国之间基于战略利益关系的讨价还价。而对于武装冲突门槛以下的恶意网络行为，美日两国主要是通过其国内政治和法律进程，为应对所谓“灰色地带”挑战而采取包括军事行动在内的强制性手段。

除了开展针对恶意网络活动的个案研究以及国内立法合作之外，推动认可美日两国相关做法的国际共识，既可以依据主观判定网络攻击的性质而援引自卫权或集体防御原则，也可以为美日两国在网络空间开展军事和执法等强制性行动提供所谓的国际支持。由于网络攻击红线本身存在模糊性，政府间磋商以及学术界和产业界的讨论也能在一定程度上弥合各方分歧。因此，两国不仅在同盟内加强跨部门、跨领域的协调和沟通，而且围绕网络空间规则制定、积极构建与其他盟友和伙伴的区域协调机制。

（二）借助“四国机制”和东盟强化“印太”地区规则共识

美日第七届网络对话指出，双方旨在以自由民主的普世价值观推动网络空间的规则制定，而“印太”地区的自由和开放与确保网络空间的安全和可

① Japanese Foreign Ministry, “Joint Statement of the Security Consultative Committee,” April 19, 2019, https://www.mofa.go.jp/files/000470738.pdf.

靠密切相关。[①] 作为美国“印太战略”的重要基石，美、日、印、澳“四国机制”（Quad）于 2019 年升级到部长级，并强调网络安全对地区稳定的重要意义。尽管“四国机制”尚未就网络空间国际规则达成具体协议，但四国之间早已形成双边网络对话机制。

除了美日之外，美国和澳大利亚之间已经通过“五眼联盟”建立了长期的情报共享机制。美国和印度则在 2016 年的第五届网络对话上发表联合声明，双方同意就网络威胁实现信息共享，加强网络执法合作，并推动负责任的网络空间行为准则和建立信任措施。[②] 日本则以促进网络空间法治、建立信任措施以及能力建设作为其网络安全外交的三大支柱，与印度和澳大利亚开展了多轮网络对话。[③] 而印度和澳大利亚也开展了三轮网络对话，围绕网络安全和国际规则制定进行了磋商。[④]

同时，东盟也是美日两国在“印太”地区拓展网络安全合作的重要对象。早在 2014 年，美日两国就宣布将共同帮助东盟国家提升网络防御能力，建立信任措施，并围绕网络空间的规则制定开展合作。[⑤] 2016 年 9 月，日本—东盟峰会确认双方将围绕网络安全加强合作。随后，日本国际协力机构（JICA）开始为部分东盟国家的网络安全部门官员提供培训。2018 年 6 月，日本—东盟网络安全中心在泰国启动。美日两国随后又共同举办了针对东盟国家的网络安全培训项目。[⑥] 2019 年 10 月，首届美国—东盟网络对话在新

① U.S. Department of State, “The Seventh U.S.-Japan Cyber Dialogue,” November 7, 2019, https://www.state.gov/the-seventh-u-s-japan-cyber-dialogue/.

② White House, “Joint Statement: 2016 United States-India Cyber Dialogue,” September 29, 2016, https://obamawhitehouse.archives.gov/the-press-office/2016/09/29/joint-statement-2016-united-states-india-cyber-dialogue.

③ Japanese Foreign Ministry, “Third Japan-India Cyber Dialogue, Tokyo,” February 27, 2019, https://www.mofa.go.jp/press/release/press1e_000113.html; and Japanese Foreign Ministry, “The 4th Japan-Australia Cyber Policy Dialogue Joint Statement,” March 8, 2019, https://www.mofa.go.jp/fp/cp/page4e_000987.html.

④ Indian External Affairs Ministry, “3rd India-Australia Cyber Dialogue,” September 4, 2019, https://www.mea.gov.in/press-releases.htm?dtl/31794/3rd_IndiaAustralia_Cyber_Dialogue.

⑤ White House Office of the Press Secretary, “U.S.-Japan Joint Statement: The United States and Japan: Shaping the Future of the Asia-Pacific and Beyond,” April 25, 2014, https://obamawhitehouse.archives.gov/the-press-office/2014/04/25/us-japan-joint-statement-united-states-and-japan-shaping-future-asia-pac.

⑥ Japanese Ministry of Economy, Trade and Industry “US-Japan Cybersecurity Joint Training with ASEAN Member States Held,” September 14, 2018, https://www.meti.go.jp/english/press/2018/0914_001.html.

加坡举行，旨在构建开放、安全、稳定的信息通信技术环境，并就负责任的网络空间国家行为提出非约束性规范建议。该对话还将日本—东盟网络安全中心纳入合作范围，从而满足地区成员在保护关键基础设施和打击网络犯罪方面的需要。[①] 此外，美日两国还利用东盟地区论坛搭建有关网络安全信息共享和网络规则磋商的区域协调机制，尤其是日本以共同主席的身份与马来西亚和新加坡共同主持召开了第一届和第二届东盟地区论坛中的使用信息和通信技术安全会议（ARF-ISM on ICTs Security）。[②] 该会议还配套有关于建立信任措施的不限成员名额研究小组，由各国专家共同参与，并向联合国政府专家组和不限成员名额政府间工作组（Open-Ended Working Group, OEWG）提供建议。[③]

尽管“四国机制”和东盟地区论坛都尚未就网络空间国际规则达成实质性的协议，但美日两国多年来通过多个双边和地区协调机制，借助政府间磋商和技术专家培训等手段，逐步弥合相关国家在网络规则方面的分歧，并谋求在全球网络空间治理进程中进一步提升话语权和影响力。在 2019 年 9 月召开的联合国大会期间，美国与包括日本、“五眼联盟”国家在内的 26 个国家和地区组织发表了《关于在网络空间促进负责任的国家行为的联合声明》，并将中国和俄罗斯排除在外。与此同时，美国的军事同盟体系在网络空间的集体防御机制得到进一步扩展。在北约和美日同盟分别确认其安全条约适用于网络空间的基础上，日本已正式加入北约合作网络防御卓越中心，并寻求组建更加广泛的网络同盟，从而有效应对网络攻击。[④] 由此可见，在

① U.S. Mission to ASEAN, “Co-Chairs’ Statement on the Inaugural ASEAN-U.S. Cyber Policy Dialogue,” October 3, 2019, https://asean.usmission.gov/co-chairs-statement-on-the-inaugural-asean-u-s-cyber-policy-dialogue/.

② Japanese Foreign Ministry, “ARF Inter-Sessional Meeting on Security of and in the Use of Information and Communication Technologies (ICTs) and 2nd ARF-ISM on ICTs Security,” March 29, 2019. 论坛（ARF）每年在东盟轮值主席国举行外长会议。每年举行 1 次高官会、1 次安全政策会议、1 次建立信任措施与预防性外交会间辅助（ISG）会议、5 场会间会（救灾、反恐与打击跨国犯罪、海上安全、防扩散与裁军、使用信息和通信技术安全会间会）和 2 次国防官员对话会（DOD）。参见外交部：“东盟地区论坛”（最近更新时间为 2020 年 4 月），https://www.fmprc.gov.cn/web/gjhdq_676201/gjhdqzz_681964/lhg_682614/jbqk_682616/。

③ Japanese Foreign Ministry, “ARF-ISM on ICTs Security 5th SG,” January 16, 2020, https://www.mofa.go.jp/press/release/press4e_002757.html.

④ NATO, “Allies Agree Japan’s Mission to NATO,” May 24, 2018, https://www.nato.int/cps/en/natohq/news_154886.htm; and NATO, “NATO and Japan Intensify Dialogue on Cyber

国际法如何适用于网络空间的难题或将长期存在的背景下，美日两国正以国内法律、法规和国际政治进程为其网络空间自由行动乃至军事行动做背书。然而，这种做法实际上是以单个国家或国家集团的私利凌驾于人类共同利益之上，以“丛林法则”和“先占逻辑”指导下的激进实践破坏国际社会共同制定规则的基础。当前，世界上主要国家纷纷出台网络安全战略，组建以网络空间为作战领域的军事单位，在这一新兴领域进行频繁的试探与博弈，增加了冲突的风险。一旦以美日同盟为代表的传统军事同盟体系及其行动逻辑得到国际支持，无疑将加剧全球网络空间的紧张局势，或反噬美日网络安全的长期合作，甚至危及全球网络空间的战略稳定。

结 束 语

美日同盟向网络空间延伸已是不争的事实，但美日网络安全合作在多大程度上能做到“无缝衔接”还面临结构性障碍。美国期待将一个更加强大的日本整合进自己的全球网络同盟体系，日本则需借助美国的安全承诺对外强化威慑，对内以共同防御突破资源和政策的约束。然而，美国进一步承诺也意味着其承诺可信度遭受挑战的概率大幅度上升。考虑到网络空间的复杂性和不确定性，这种可信度危机或与美日同盟时隐时现的结构性矛盾产生共振效应。在传统安全领域，日本国内力图通过扩军修宪，逐渐摆脱对美国保护的长期依赖。而在网络空间这一新兴领域，日本同样面临抉择。美国利用“棱镜”项目不仅窃听对手的重要信息，同样也包括针对日本政府以及重点企业的长期监听，引发同盟信任危机。[①] 在特朗普执政后，美国外交政策更是整体上趋于单边主义，政策调整的随意性较大，且多次提出“抛弃”日本的言论。[②] 这为美日同盟的发展增添了变数，也给双方的网络共同防御带来持续

Defence,” October 9, 2019, https://www.nato.int/cps/en/natohq/ news 169493.htm?selectedLocale=en.

① “Wikileaks: US ‘Spied on Japan Government and Companies,’ ” BBC News, July 31, 2015, https://www.bbc.com/news/world-asia-33730758.

② “Trump Blasts US-Japan Defense Alliance Ahead of G20,” *Financial Times*, June 27, 2019, https://www.ft.com/content/506adafa-9864-11e9-9573-ee5cbb98ed36.

压力和风险。因此，美日同盟在对华网络威慑的协同政策上也并不完全一致。对日本来说，网络空间的模糊性很大。利用应对“灰色地带”挑战打破采取军事行动的枷锁是日本政府的着力点。但由于模糊的网络行为而卷入针对中国的网络攻击中，甚至根据跨领域战略思维将其上升到经济或军事层面可谓得不偿失。相比中日之间在网络安全议题上整体较为平和的表现，中美之间则在网络攻击、网络犯罪和科技管制等领域表现出更多的竞争和冲突。然而，这种冲突也并未无限制地延伸到传统政治和安全领域。不难发现，在各大国竞相在网络空间进行试探与博弈的同时，维护网络空间基本的战略稳定，并采取更加谨慎和克制的态度符合各方的共同利益。因此，如何管控网络冲突，避免其迅速波及现实世界，依然是今后大国协调网络空间战略稳定的重点。

对中国来说，既要密切追踪美日同盟向网络空间的延伸，又要明确两国在网络安全问题上的共同利益和可能的意见分歧。尤其在应对所谓“灰色地带”挑战这一热点问题上，中国需要进行长期深入的调查研究。一方面对美日同盟可能的联合行动做出预判并及早应对，另一方面要确定中国对“灰色地带”挑战的判定标准。比如，究竟什么样的网络行为构成所谓的“灰色地带”挑战；哪些网络行为构成国际法意义上的武装冲突，并自动触发自卫权和集体自卫权；对于网络攻击的自卫反击应该符合哪些国际法原则；对于不构成自卫反击的恶意网络行为如何应对；等等。事实上，这些问题不仅局限于中、美、日三国之间，更是当前国际社会以及全球网络空间治理面临的棘手问题。联合国政府专家组围绕上述问题的数轮谈判无果而终。部分国家和非政府组织则试图另起炉灶，设立新的标准和规范。网络空间作为与现实世界紧密相联的新兴领域，其治理需要各方群策群力，任何单一行为体的努力都难以确保网络空间的长治久安。中国作为负责任大国，在迈向建设网络强国的道路上，必然要对这些核心问题阐述自己的观点，甚至推广至国际社会，从而进一步丰富构建网络空间命运共同体的内涵。也只有这样，中国同美日两国之间才能有效确立网络安全领域的透明与信任措施，避免由于误判或意外冲突升级而造成连锁反应，影响整体战略稳定。

[责任编辑：樊文光]