摘　　要

与各国网络空间国内法治，以及国际法治其他领域相比，网络空间国际法治仍然任重道远，广大发展中国家急需广泛反映自身利益的区域性乃至全球性的网络空间国际规则。网络空间国际法治的参与行为体主要包括主权国家、政府相关国际行为体、非政府行为体等，主权国家是网络空间国际法治的关键，没有主权国家参与其中，网络空间合作便不可能有效、长期的展开，网络空间的国内法治与稳定秩序无法建立。“数字鸿沟”、共同的网络安全威胁与挑战、法律政策问题等因素，是网络空间国际法治的现实困境。

网络空间国际法治与网络安全国际合作的良性互动表现为相互促进，网络空间国际法治能促进相关国际合作的长期、有效开展，网络安全国际合作有助于解决网络空间国际法治困境并促进网络空间国际法治实践的发展。国际机制与国际合作成效两者之间有着紧密的关系，国际机制在降低交易成本、增强合作者谈判能力、确定合作权益等方面，以及在纠纷协调解决、监督执行以及对背叛的惩罚等方面都发挥着重要作用；国际法律机制作为国际机制中的一种，或者作为国际机制法制化的结果之一，其本身并非国际法，却是国际法治实践的组成部分，它提高了国际机制促进合作的各种效能。合作是国际法治的基础，某领域国际合作长期稳定的进行，会激发该领域国际法治实践的产生与发展，因为一种重要的国际关系，必然需要一定的法律规范进行调整，网络安全国际合作也是如此，网络安全国际合作关系的变化，也需要网络空间国际法做出改变，这是法的适应性的表现。

网络大国之间的实质性网络安全合作，是促进网络安全国际合作、解决网络空间领域的国际法治困境，并实现二者的良性互动的关键。面对网络空间博弈与网络霸权挑战等威胁，中俄两国作为世界信息网络大国，积极参与区域性、全球性信息网络安全合作，积极推动网络空间国际法治实践的发展，为引领信息网络安全国际合作打下坚实基础，网络空间的国内、国际法治实践使得中俄网络安全合作更制度化、规范化。

中俄网络安全合作最初是在上海合作组织、金砖国家以及联合国等多边合作的框架下展开的，目标是维护网络主权、促进国际信息网络安全合作、联合打击共同的网络安全威胁、制定网络空间国际规则。中俄网络安全合作坚持尊重网络主权、维护网络和平与安全、推进全球共治共享、依法治理网络空间的原则。除了中俄各自网络安全法律体系存在的问题外，中俄网络安全合作存在核心利益诉求不同、缺少实质性合作、网络霸权主义持续威胁等问题与障碍。

中俄积极参与和推动区域性和全球性信息网络安全合作，为双边和多边合作积累了丰富的经验；随着“一带一路”与欧亚经济联盟对接合作的不断推进，中俄两国有着深厚的合作基础与巨大的合作潜力，为中俄网络安全合作的完善奠定

了现实基础。网络空间国际法治视域下，为了完善中俄网络安全合作法律机制，双方应当健全中俄网络安全实质合作的制度保障，充分利用现有的网络空间全球治理平台开展合作，并提高网络安全的多元主体协同共治能力。

关键词：网络安全；国际法治；国际合作；网络主权

Abstract

Compared to domestic rule of law in cyberspace, as well as other areas of International rule of law, International rule of law in cyberspace still has a long way to go. Developing countries urgently need regional and even global cyberspace International rules that broadly reflect their own interests. The actors involved in the International rule of law in cyberspace mainly include sovereign states, government related International actors, non-governmental actors, etc. Sovereign states are the key to the International rule of law in cyberspace. Without the participation of sovereign states, cyberspace cooperation cannot be effective and long-term and the domestic rule of law and stable order in cyberspace cannot be established. "The digital divide", common cybersecurity threats and challenges, legal and policy issues, and other factors are the practical dilemmas of the International rule of law in cyberspace.

The positive interaction between International rule of law in cyberspace and International cooperation in cybersecurity is manifested in mutual promotion. International rule of law in cyberspace can promote the long-term and effective development of relevant International cooperation, and International cooperation in cybersecurity can help solve the dilemma of International rule of law in cyberspace and promote the development of International rule of law practice in cyberspace. There is a close relationship between International mechanisms and the effectiveness of International cooperation. International mechanisms play an important role in reducing transaction costs, enhancing the negotiating ability of partners, determining cooperation rights and interests, as well as in coordinating and resolving disputes, supervising implementation, and punishing betrayal. As one of the International mechanisms, or as a result of the legalization of International mechanisms, International legal mechanisms are not International law, but rather an integral part of the practice of International rule of law, which enhances the various effectiveness of International mechanisms in promoting cooperation. Cooperation is the foundation of International rule of law, and the long-term and stable progress of International cooperation in a certain field will stimulate the emergence and development of International rule of law practice in that field. An important International relationship inevitably requires certain legal norms to adjust, so is International cooperation in cybersecurity. Changes in International cooperation in cybersecurity also require changes in International law in cyberspace, which is a manifestation of the adaptability of law.

Substantive cybersecurity cooperation between major cyber powers is the key to

promoting International cooperation in cybersecurity, resolving the dilemma of International rule of law in the cyberspace field, and achieving a benign interaction between the two. Faced with threats such as cyberspace gaming and cyber hegemony challenges, China and Russia, as major information and cyber powers in the world, actively participate in regional and global information and cyber security cooperation, actively promote the development of International legal practice in cyberspace, and lay a solid foundation for leading International cooperation in information and cyber security. The domestic and International legal practice in cyberspace has made China and Russia's cybersecurity cooperation more institutionalized and standardized.

The China-Russia cybersecurity cooperation was initially launched under the framework of multilateral cooperation such as the Shanghai Cooperation Organization, BRICS countries and the United Nations, with the goal of safeguarding cyber sovereignty, promoting International cooperation on information and cyber security, jointly combating common cybersecurity threats and formulating International rules in cyberspace. China-Russia cybersecurity cooperation adheres to the principles of respecting cyber sovereignty, maintaining cyber peace and security, promoting global shared governance and law-based governance of cyberspace. In addition to the problems existing in China and Russia's respective cybersecurity legal systems, there are problems and obstacles in the cybersecurity cooperation between China and Russia, such as different demands for core interests, lack of substantive cooperation, and continuous threat of cyber hegemony.

China and Russia have actively participated in and promoted regional and global information and cyber security cooperation, and accumulated rich experience for bilateral and multilateral cooperation. As the cooperation between the Belt and Road Initiative and the Eurasian Economic Union continues to advance, China and Russia have a profound cooperation foundation and huge cooperation potential, which lays a practical foundation for the improvement of the legal mechanism of China-Russia cybersecurity cooperation. From the perspective of the International rule of law in cyberspace, in order to improve the legal mechanism of China-Russia cybersecurity cooperation, the two sides should improve the institutional guarantee for substantive cooperation on China-Russia cybersecurity, make full use of the existing global cyberspace governance platform to carry out cooperation, and enhance the ability of multiple actors to cooperate and govern cybersecurity.

Keywords: Cybersecurity; International Rule of Law; International Cooperation; Cyber Sovereignty

目　　录

第 1 章　绪论 1
1.1　选题背景和意义 1
1.1.1　选题背景 1
1.1.2　研究意义 1
1.2　国内外研究现状 2
1.2.1　中俄网络安全合作研究 2
1.2.2　网络安全合作机制或者法律机制研究 3
1.2.3　国际法律机制对国际合作的促进研究 4
1.3　研究方法与创新之处 4
第 2 章　网络空间国际法治的确立与困境 6
2.1　网络空间国际法治的确立历程 6
2.2　网络空间国际法治的参与行为体 7
2.2.1　主权国家（国家行为体） 8
2.2.2　政府相关国际行为体 9
2.2.3　非政府行为体 11
2.3　网络空间国际法治的现实困境 11
2.3.1　“数字鸿沟”与数字不平等 11
2.3.2　全世界共同面临的网络安全威胁 13

2.3.3 政策法律层面存在的问题 14
第 3 章 网络空间国际法治与网络安全国际合作的互动 15
3.1 国际法治对网络安全国际合作的促进..... 15
3.2 网络安全国际合作对国际法治发展的促进..... 17
3.3 国际法治与网络安全国际合作良性互动的关键..... 18
第 4 章 中俄网络安全合作的进程、原则与现状 20
4.1 中俄网络安全合作进程..... 20
4.1.1 多边框架下的中俄网络安全合作 20
4.1.2 中俄双边网络安全合作 21
4.2 中俄网络安全合作的基本原则..... 22
4.2.1 尊重网络主权原则 22
4.2.2 维护网络和平与安全原则 23
4.2.3 推进全球共治共享原则 24
4.2.4 依法治理网络空间原则 25
4.3 中俄网络安全法治水平与合作现状..... 26
4.3.1 中国网络安全法律体系的现状 26
4.3.2 俄罗斯网络安全法律体系的现状 28
4.3.3 中俄网络安全合作的现状 29
第 5 章 国际法治视域下如何完善中俄网络安全合作 31

5.1　健全中俄网络安全实质合作的制度保障 31
5.1.1　健全网络安全治理与国际合作相关法律制度 31
5.1.2　促进中俄网络安全合作机制的落实 31
5.2　充分利用现有的网络空间国际治理平台 32
5.2.1　联合国框架内的网络安全合作 32
5.2.2　上合组织、金砖国家框架内的网络安全合作 33
5.2.3　“一带一路”框架内的网络安全合作 34
5.3　提高网络安全的多元主体协同共治能力 35
第 6 章　结论 37
参考文献 38
作者简介 42
致　　谢 43

第 1 章　绪论

1.1　选题背景和意义

1.1.1　选题背景

网络安全问题作为非传统安全问题之一，其与国家安全与发展利益息息相关，凭借着网络空间的全球性与流动性，突破了传统的物理与地域界限，几乎渗透到世界的各个领域，并超越疆界阻隔以及种族文化差异[①]。国际网络不法行为需要规制，和平时期的网络行动更需要国际对话与合作。在网络空间几乎“无孔不入”的同时，各国亦积极拥抱网络信息技术的巨大优势以维护自身利益，并利用网络空间开展各领域的竞争与合作。针对网络安全问题，任何国家都无法单打独斗，不得不谋求与他国进行合作，妄图单独或者联合掌控全世界网络空间的想法更是不切实际。即使是作为网络霸权国的美国，亦是积极谋求与盟友不断加强网络安全合作并趋于常态化。甚至于一直强调美国优先的特朗普政府，为了围追堵截华为的 5G 技术，也不得不软硬兼施地促使一些盟国一同打压华为。

在网络安全领域，中俄两国有相似的处境和诉求，两国同为网络大国，也同为网络安全的“相对弱者”。两国既面临着日益复杂的网络犯罪、网络恐怖主义、网络安全核心技术受制于人等国内网络安全问题，也面临着网络主权原则不断被挑战、网络安全理念被西方无端指责、网络空间治理的制度性话语权较弱的国际网络安全问题。面对共同的网络安全机遇与挑战，基于共同的网络安全治理理念，两国非常重视网络安全自身建设与推进合作，协作推进信息网络空间发展。无论是双边还是多边网络安全合作，网络安全合作有序有效而又稳定的推进离不开国际机制。制度化、规范化的国际法律机制提高了国际机制的有效性，作为国际机制中的一种，或者说作为国际机制法制化的结果之一，它使得国际机制促进合作的各种效能得到了提高，并且无论是条约法还是习惯国际法本身也具有相同的功能。

网络安全合作的法律机制是主权国家、国际组织等国际行为体，用以规范调整网络安全合作关系推进、实施的国内法律、条约、政策、程序等的集合。网络安全合作法律机制本身并非国际法，确是网络空间国际法治的重要组成部分，并与网络空间国际法相互转化。正因如此，中俄两国既不断加强国内网络安全立法、执法，又不断推进两国网络安全各方面合作与交流的法律进程、加强网络空间立法合作、推动构建全球信息网络空间治理秩序。[②]

1.1.2　研究意义

[①] 参见生忠军、姜峭帆：《打造网络空间命运共同体：价值、挑战、路径》，《世界社会主义研究》2019 年第 3 期，第 37 页。

[②] 李燕：《2021 年版〈俄罗斯国家安全战略〉及中俄安全合作》，《俄罗斯学刊》2022 年第 1 期，第 128 页。

理论意义。网络空间没有物理边界不意味着其为“全球公域”，网络的每个节点、终端都处于主权国家的管辖之下。网络安全问题是开放的而不是封闭的，网络安全需要有效的合作机制，网络空间硬法机制约束力较强，但发展缓慢，因此即使是范围小、约束力小的双边网络安全合作软法机制，也是维护国家网络主权、网络空间利益，推动网络安全合作、完善网络空间治理体系的不错选择。从国际法治视角研究中俄网络安全合作，丰富了中俄网络安全合作的研究体系，并为提升我国网络安全法治化水平、维护网络主权、建构良好网络空间秩序、提升我国在网络安全国际规则制定中的影响力与话语权，提供理论支持，以期解决网络空间法治困境，促进网络空间国际法治的发展。

现实意义。基于网络空间的全球性与流动性，为维护国家在网络空间的安全与发展利益，网络安全合作要立足国内安全，放眼全球治理。中俄网络安全合作具有深厚的基础和广阔的前景，双方在网络安全领域具有共同理念、利益和关切，而中俄网络安全合作法律机制的建构与完善，使得双方网络安全合作水平提升到新的高度，将加强双方各自网络安全治理能力，共同推进有利于双方乃至广大发展中国家的网络空间国际规则的制定，为维护本地区和国际网络安全发挥重要的作用。

1.2　国内外研究现状

1.2.1　中俄网络安全合作研究

国际社会就国际法适用于网络空间已基本达成共识，即使是西方主导制定的《塔林手册 2.0》也没有采用全球公域论，而是强调国家主权对于整个网络空间的适用，明确了国际法适用于网络空间，但目前直接研究中俄网络安全合作机制或者法律机制的文献较少，一般散见于研究中俄网络安全合作或者区域、国际网络安全合作机制的文献之中。国内外学者关于中俄网络安全合作的研究，大多集中在双方合作的共识、合作的领域、合作的多边平台等方面，具体包括共同打击网络犯罪、网络恐怖主义、网络安全技术等方面的合作机制研究，以及联合国框架下、上合机制或金砖机制下的中俄网络安全合作研究，网络空间秩序构建与规则制定的博弈与合作研究，或者从宏观层面提出应当完善现有的中俄网络安全合作机制等。

正如黄志雄教授[①]所言，中俄等新兴国家阵营，旗帜鲜明地支持网络空间的国际法治，近年来多次提出制定网络安全、网络军备竞赛等领域行为准则的倡议，例如共同起草并向联合国大会提交《信息安全国际行为准则》，以及共同力主在联合国框架内制定新的网络犯罪国际公约。

[①] 黄志雄：《国际法在网络空间的适用：秩序构建中的规则博弈》，《环球法律评论》2016 年第 3 期，第 12-16 页。

Cho Y.等[①]认为，中俄正在积极建立网络安全机制来提高话语权，为了制定限制网络恐怖主义、互联网军事使用和网络技术的标准，中俄通过上海合作组织与区域国家一道积极参与的网络安全相关合作。

Hsiung C.W.[②]认为，互联网监管是中俄网络安全合作的最重要领域之一；中俄在区域和全球层面协调政策，旨在影响和塑造有关互联网控制和信息通信技术使用的国际法律和规范体系；中俄就媒体和信息合作不断进行对话，加强人工智能、信息技术和互联网等领域的技术进步直接交叉。

张文伟[③]提出，中俄已就信息安全问题进行了多轮磋商，正准备共同打击利用互联网信息技术干涉国家内政、破坏国家主权等犯罪活动。

1.2.2　网络安全合作机制或者法律机制研究

多数学者认为，数字鸿沟、信任缺失、网络空间霸权等障碍，以及某些国家的政府部门主导的网络攻击事件，导致了国际网络安全合作难以长效稳定的推进，也导致了有效国际合作机制难以真正建立或者实施。但区域网络安全合作确实取得了显著成果，尤其是欧盟、美国与其盟友的网络安全合作，虽然主要西方国家一直将中俄等国视为网络安全的主要“假想敌”。为了实现共同利益、减少不确定性风险，合作机制特别是法律机制仍然是网络安全合作的重要保障，正如王孔祥博士[④]所说，“解决网络安全问题的理想办法是达成具有法律约束力的国际文件，哪怕是在小到双边层面的范围内达成仅具有软法效力的协议，也是难能可贵的”。

黄志雄教授[⑤]指出，联合国信息安全政府专家组是网络空间国际法领域最重要的多边机制之一，但国际法是国家之间妥协的结果，美国等在网络空间拥有主导话语权的西方国家在许多问题上立场过于强硬，而其对其他国家的合法呼吁包容性不足，也没有充分权衡各方利益，将 2017 年联合国第五次信息安全专家组失败的责任推卸给中国、俄罗斯和其他国家。

Tehrani P.M.等[⑥]认为，网络恐怖主义是一种国际犯罪，应通过跨国合作对其进行普遍管辖，国际法是一个必要的工具，虽然各国必须建立自我监管的法律机制，但这种机制需要得到国际协议和适当的国家立法的支持。

---

① See Cho Y. and Chung J., “Bring the State Back In: Conflict and Cooperation Among States in Cybersecurity”, Pacific Focus, Vol.32, No.2, 2017, pp.311-312.

② See Hsiung C.W., “China’s Technology Cooperation with Russia: Geopolitics, Economics, and Regime Security”, The Chinese Journal of International Politics, Vol.14, No.3, 2021, pp.460-465.

③ 张文伟：《上海合作组织信息安全合作：必要性、现状及前景》，《俄罗斯东欧中亚研究》2016 年第 3 期，第 102 页。

④ 王孔祥：《网络安全的国际合作机制探析》，《国际论坛》2013 年第 5 期，第 3-6 页。

⑤ 黄志雄：《网络空间国际规则博弈态势与因应》，《中国信息安全》2018 年第 2 期，第 32 页。

⑥ See Tehrani P.M., etc., “Cyber terrorism challenges: The need for a global response to a multi-jurisdictional crime”, COMPUTER LAW & SECURITY REVIEW, Vol.29, No.3, 2013, pp.207-208.

Orji U.J.[①]认为，信息和通信技术在非洲国家的传播和互联网渗透引起了区有关国家对网络安全的担忧，一些非洲政府间组织制定了网络安全法律框架，《非盟网络安全公约》的通过标志着非洲网络安全治理的一个重要里程碑。

1.2.3　国际法律机制对国际合作的促进研究

多数学者认为，尽管国际机制存在局限性与有效性的疑问，但国际机制显然能够促进国际合作，服务并规范国际合作，国际机制理论的三大流派都没有否认国际机制的作用，只不过是作用大小的问题。国际机制作为一套原则、规范、规则和决策程序等的集合，其法制化的结果包括国际法律规范，或者可以说国际法律规范就是国际机制的一种。关于国际法律机制与国际合作的关系，部分学者进行了具体论述。

李彦[②]从网络犯罪国际法律机制建构的维度出发，认为国际法律机制对国际社会合作打击网络犯罪和各国的网络犯罪立法均起到了积极作用，在全球性国际法律机制的进程难以一蹴而就的背景之下，可分步骤推进之，以建构区域性合作机制确定为阶段方向。

成志杰[③]通过总结中俄的契约合作指出，中俄关系的契约合作包括双方缔结的双边条约和共同参加的各种多边及带有普遍性的国际条约，中俄这种“有契约的正式合作”并不意味着限制双方的积极性和能动性，而是鼓励各自优势得到充分的发挥，增强了对双方行为的可预判性。

通过现有文献可知，国际机制或者法律机制建立或者完善的前提是特定合作领域的国际主体之间存在合作关系，换言之，机制并非合作的充分条件。中俄两国网络安全合作的领域非常广泛，并且已经在多个机制框架下开展双边、多边网络安全合作，现有文献也已经对双方网络安全合作机制进行梳理，分析机制面临的问题并提出了解决方案。通过现有文献可知，法律机制的建立完善是促进网络安全合作的理想办法，该机制既要有国内立法支持，也要有国际法特别是条约法的规范，不少文献虽然提出应当将合作机制进行法制化建构或完善的观点，但并未提出具体方案，这为本文研究提供了契机。

1.3　研究方法与创新之处

文献分析法。通过阅读有关网络安全、网络安全国际合作、网络安全合作法律机制等主题的文献资料，学习该领域相关知识，厘清有关文献的思路框架。根据拟定的基本框架，对文献资料进行综合分析后，总结研究现状，精读有关重点

[①] See Orji U.J., “Multilateral Legal Responses to Cyber Security in Africa: Any Hope for Effective International Cooperation?”, https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7158472, last visited on 12 September 2022.

[②] 李彦：《网络犯罪国际法律机制建构的困境与路径设计》，《云南民族大学学报（哲学社会科学版）》2019 年第 6 期，第 138-142 页。

[③] 成志杰：《网状伙伴外交机制：中俄合作的新路径》，《俄罗斯研究》2015 年第 3 期，第 125-126 页。

内容，研究国际法律机制与国际网络安全合作的关系，分析网络安全合作领域有哪些国际行为体参与其中，总结网络安全合作法律机制产生的现实基础，探究中俄网络安全合作法律机制存在的不足与完善的可行性。

比较分析法。域外特别是西方国家的网络安全合作起步较早，虽然其中确实有敌视、打压中国的内容，但仍有较多可资借鉴之处。因此在对比分析域外网络安全合作法律机制的理念模式、实际效果等内容的基础上，充分利用其在制度规则、实施机制等方面的合理之处，以期在国际法治视野下完善中俄网络安全合作。

创新之处。面对网络安全国内国际的诸多挑战，中俄两国在双方具有共识的基础上开展多领域多平台的实质性合作，同时学界对此课题不断进行理论研究与实践深化。但是两国如能够不断完善网络安全合作，积极落实两国达成的协议等法律文件，这将有利于两国网络安全合作的稳定性与实效性，增强网络安全合作互信，对网络空间国际法治实践发展做出大国贡献，这也是本文的创新点。

第 2 章　网络空间国际法治的确立与困境

2.1　网络空间国际法治的确立历程

网络空间的治理与规则，经历了从“自我规制”、“国内法治”到“国际法治”的历史性演变。互联网发展早期，其建设与发展的相关理论和技术刚刚起步，互联网还只是一个个封闭的小圈子，主要是相关行业科研人员自治或者行业自律。随着统一开放的互联网的诞生，各国纷纷制定互联网国内立法与政策，网络空间开始走向“国内法治”的阶段。虽然各国国情、网络发展状况以及国家制度不尽相同，但由于关键信息基础设施重要性与脆弱性同在，且网络空间突破了传统的物理与地域界限，几乎渗透到社会生活的各个领域，网络安全问题直接影响着政治安全、经济安全、社会安全等国家安全的各方面，诸多国家都制定了应对网络安全问题的国内立法，形成了较为成熟稳定的网络安全国家战略与网络安全法律体系，内容各有不同但又有其共性。在中国，中共十八大以来，面对网络安全与信息技术领域的复杂形势与严峻挑战，党中央高度重视互联网的治理与发展，统筹协调各方面各领域信息化和网络安全重大问题，推动网信事业和网络安全治理取得历史性成就，提出一系列新思想新观点新论断，形成了网络强国战略思想，这对网络法律制度建设作出了方向指引。中国《网络安全法》是网络安全法律规范体系的基本法，在此基础上又相继颁布了《个人信息保护法》《数据安全法》等法律法规，不断充实、完善和发展着中国网络安全法律规范体系，提高了中国网络安全保障水平。

除了在顶层设计上制定网络安全基本法律作为以外，诸多国家也制定符合本国国情的个人信息安全、数据安全保护的法律。例如中国 2021 年 6 月通过了《数据安全法》、8 月又通过《个人信息保护法》，日本 2020 年修订《个人信息保护法》及新加坡 2020 年修订《个人数据保护法》等，构建并完善个人信息安全、数据安全的法律保护体系。[①]此外，面对共同的网络安全威胁，尤其是黑客犯罪和网络恐怖主义犯罪的巨大威胁，各国都比较重视预防和制裁网络犯罪，加大对网络犯罪的打击力度；网络安全立法愈加具体细化，已开始有国家针对某种互联网形态出台专门立法，如俄罗斯出台针对网络博主专门性立法《知名博主管理法案》，德国《社交网络执行法》明确界定了社交网络平台与社交网络违法内容，强化政府对社交媒体平台的法律监管并设置巨额罚款等。[②]因此即便是发展中国家，不论该国网络技术实力和数字经济强弱，其网络安全国内法律体系或者网络安全国内法治日臻完善。

[①] 参见李芳、程如烟：《主要国家数字空间治理实践及中国应对建议》，《全球科技经济瞭望》2020 年第 6 期，第 33-38 页。

[②] 周丽娜、陈晴：《国外网络信息安全治理体系现状及启示》，《社会治理》2020 年第 9 期，第 71-75 页。

由于互联网起源于美国，美国等西方国家不仅拥有绝对的技术优势，而且对网络空间的国际法治问题关注和研究较早，并且是首先就网络空间国际法的适用提出更系统建议的国家。2011 年，奥巴马政府首次将“网络空间法治”的概念引入美国的《国际网络空间战略》。随着现实世界的国际关系和国际秩序开始向网络空间延伸，这必然要求网络空间国际立法的强化，以使国际法在网络空间的秩序构建中发挥重要作用，网络空间国际法治也随之兴起，网络空间法治的兴起符合当代国际关系、国际机制法制化的发展趋势。但是，与日臻完善的网络空间国内法治相比，甚至与国际关系和国际法的大多数其他领域相比，网络空间国际法治仍然任重道远。围绕着网络空间国际秩序构建和规则主导权，以美国、欧盟为代表的西方国家，和以中国、俄罗斯等为代表的新兴国家，两大阵营由于意识形态、国家利益等方面的差异乃至对立，他们对于网络空间国际法治存在一系列重要分歧，这些分歧主要体现在：规则形式之争，即立足于既有国际法规则还是制定新的国际法规则；规则内容之争，即适用何种内容的国际规则，以及规则制定模式之争[①]。

《布达佩斯网络犯罪公约》是欧美主导的区域性公约，作为世界上第一个打击网络犯罪的公约，其对非缔约国家也影响深远，诸多国内立法以及区域公约借鉴其内容或者框架，但公约代表的是西方发达国家的利益诉求，虽然之后逐渐吸纳发展中国家，但仍不具有广泛代表性，不能反映发展中国家的普遍利益；[②]北约牵头制定的《塔林手册 1.0 版》与《塔林手册 2.0 版》，都属于非官方的国际公法学家的研究成果，不具有任何国际法上的约束力，但它们都着眼于已然存在的具有习惯法地位的实然法，而不是倡导新的应然法，所代表的还是西方国家的立足于既有国际法规则的主张，反映西方利益诉求的性质未发生根本改变。因此从国际法层面维护网络安全依然有很长的路要走，广大发展中国家仍然很难有效开展打击网络犯罪的国际合作，急需广泛反映自身利益的区域性乃至全球性的网络空间国际规则[③]。

2.2　网络空间国际法治的参与行为体

马克思主义哲学确立了人的主体性，作为实践主体的人并不只是单个的人，就如同法律上的人不仅指自然人那样。实践的客体或对象不同，主体范围也不同，实践主体可分为个人主体、集团主体、社会主体和人类主体四种基本形式。网络空间国际法治的实践主体或者参与行为体不仅有主权国家，主权国家、政府相关

[①] 参见黄志雄：《网络空间国际规则博弈态势与因应》，《中国信息安全》2018 年第 2 期，第 31-32 页。
[②] 黄惠康：《中国特色大国外交与国际法》，法律出版社 2019 年版，第 367 页。
[③] 参见杨帆：《“一带一路”框架下网络安全国际合作机制研究》，《“一带一路”法律研究》2021 年第 2 期，第 327-328 页。

国际行为体、非政府行为体等都在网络空间国际法治中发挥着重要作用，都是不可替代的。

2.2.1　主权国家（国家行为体）

互联网信息技术发展到今天，网络空间已成为与传统物理空间同等重要的第五疆域。如果不承认网络空间中国家主权的地位，不仅所谓的网络空间自由成为空谈，网络空间的繁荣成为泡影，发展中国家的主权也会遭受霸权国的严重侵犯。网络空间的人受国家管辖，网络空间的计算机、服务器、路由器、交换机和光缆等物理设施受国家管辖，互联网涉外运行规则是人为制定的而非自然法则，任何人必须遵守，所以“不可规制”“自在自为之物”等一些说辞没有依据。没有网络主权，网络空间就不可能有真正的自由、秩序、发展和繁荣。国家享有主权，主权属于国家，国家主权是一国固有之对内最高、对外平等与独立之权力，网络主权也是如此，网络主权是主权国家在其领网范围内的最高权力，这种政治权力是权责一致且应当向本国人民负责的，国家应当维护网络空间的人民利益与国家安全；全球互联网治理体系，应当坚持网络主权原则，各国平等享有网络主权，平等开展网络空间的各项合作，独立参与网络空间共治，保障网络空间和平发展，构建全球网络空间新秩序。因此主权国家已深深嵌入到网络空间的国际法实践之中，没有主权国家参与其中，网络空间合作便不可能有效、长期的展开，网络空间的国内法治与稳定秩序无法建立，国际层面上也不能平等参与、共同利用和进行有效合作，网络安全国际法治要么有名无实、要么荡然无存。

上文提到，互联网发展早期主要靠的是相关行业科研人员自治或者行业自律，因此主权国家并非一直是网络空间的主要治理主体。随着网络空间安全形势的日益严峻，安全威胁日益恶化复杂，国际社会日益认识到普遍认可与遵守的行为规范的重要性，目前的网络空间安全问题的解决需要更多依赖国家的作为与相互合作水平。2013 年，斯诺登曝光了美国监听全世界的“棱镜”计划，这一事件说明了美国所谓的“互联网自由”的虚伪性，迅速推进了网络空间国际法治实践进程的改革，也加强了国家政府在网络空间治理中的作用。网络空间走向“大治理”的趋势已十分明显，各利益攸关方进一步加强了综合协调，除了有协商平台，更有网络安全治理与合作机制，各国越来越倾向于通过双边和多边机制寻求国家合作，以便就网络安全、网络空间国际规则等方面达成更大共识。但无论如何，国家主体的行动，特别是是大国之间的协调与互动，将对网络空间治理的未来与方向产生深远影响。[①]这是因为，尽管网络空间的国际规则和法律机制的引入可能涉及全球、多边和双边等多个层面，但在网络空间享有巨大利益、最具备网络实力并争夺主导权的仍然是大国。大国首先达成共识并制定相应的国际规

[①] 李艳：《网络空间国际治理中的国家主体与中美网络关系》，《现代国际关系》2018 年第 11 期，第 41-46 页。

则，然后逐渐向区域乃至全球推进，因此，全球性和区域性标准的内容有时可能会重叠。在网络安全领域，中俄两国有相似的处境和诉求，两国同为网络大国，在反对西方主导的国际秩序、发挥大国作用方面有着重要的共同利益，也同为国际网络空间的“相对弱者”。面对共同的网络安全机遇与挑战，基于共同的网络安全治理理念，两国非常重视网络安全自身建设与推进合作，协作推进信息网络空间发展，不断推进、完善网络空间国际法治。

2.2.2　政府相关国际行为体

网络空间国际法治中的政府相关国际行为体，是指由主权国家的政府发起成立或者倡议的，行为地域超越单个国家边界的主体，包括国家联盟或国家集团、政府间国际组织、政府间国际政策倡议等。这类行为体与主权国家密切相关，所以称为政府相关国际行为体，虽然受网络空间国家利益与国际博弈的影响，但其有着相对独立的行为体身份和自身利益。

国家联盟或国家集团是两个及以上主权国家间正式或非正式的合作安排，[①]它是建立在某一方面一致性同意基础上的国家间承诺，甚至不需要缔结正式的条约或协定；[②]而政府间国际组织有其制度章程，表现为条约或者协定，也有专门的组织架构。国家联盟中，当属作为区域政治经济一体化典范的欧盟的网络安全合作机制最为完备和有序，且欧盟各成员国自身网络安全水平较高，同时欧盟也是国际组织。欧盟 2013 年出台了《欧盟网络安全战略》，2016 年出台《网络与信息安全指令》，2017 年 9 月通过修订后的《欧盟网络安全战略》，确立了欧盟层面的统一战略合作框架，为后续的合作打下了基础，积极加强内部网络安全合作，形成一致的内部协调与互动机制。为打击网络犯罪，欧盟构建强有力的法律框架，例如通过了《欧洲执法培训计划》，促进共同执法，并以此作为增进互信合作的手段；欧盟与成员国的国家执法部门展开执法合作，并协调促进欧盟各国的政府部门、司法部门以及私营部门等多利益攸关方开展打击网络安全犯罪等合作。[③]在外部合作与合作机制方面，欧盟积极推动网络安全国际合作，积极推动国际公约签订，向全世界推广《布达佩斯网络犯罪公约》，力图使欧盟制定的公约成为全球打击网络犯罪的共同标准。

政府间国际政策倡议，一般表现为国际会议的形式，重在各自立场表达，虽然“务虚”大于“务实”，但是对于各国进一步开展网络安全合作、寻求各国共识以及网络安全合作机制还是有一定积极意义的。2003 年 12 月在日内瓦召开的第一届信息社会世界峰会（WSIS），颁布了关于网络问题的《原则宣言》和《行动计划》，2005 年 11 月又在突尼斯召开了第二届 WSIS，颁布了《突尼斯信息社

[①] See Stephen M. Walt, “The Origins of Alliances”, Cornell University Press, 1990, p.12.
[②] 参见于铁军：《国际政治中的同盟理论：进展与争论》，《欧洲》1999 年第 5 期，第 16 页。
[③] 郑春荣、倪晓姗：《欧盟网络安全战略及中欧合作》，《同济大学学报（社会科学版）》2020 年第 4 期，第 42-46 页。

会议程》，这两次会议都讨论了网络安全公共政策与加强网络安全国际合作的问题。2013 年 4 月，金砖五国以“金砖国家”的名义向联合国提出《加强国际合作，打击网络犯罪》的决议草案，要求进一步加强联合国对网络犯罪问题的研究和应对。联合国互联网治理论坛（IGF）自 2006 年起每年举办一届，倾向于多利益攸关方模式，以获得更多的专家意见和多样性，以便促进互联网可持续、安全、稳定发展。我国政府、企业、行业协会、技术社群等相关方都一直重视参与联合国 IGF 进程。[①]IGF 在联合国框架下，但又仅仅局限于“论坛”的作用，并没有政策制定、政策执行的权限和能力，而且无法对多利益攸关方模式指望太多，虽然它追求的是给所有人发言的权利和机会，但形式平等并不保证实质平等，例如发达国家的利益相关方参加 IGF 的差旅费一般不是问题，而发展中国家有许多人连参会的钱都没有。可见在多利益攸关方模式下，各方实际能力差距太大，尽管可以在某些共同利益方面寻求共识，但难以取得实质性突破与成果。

在参与网络空间国际法治与网络安全国际合作的进程中，中国支持联合国发挥核心作用。联合国在国际网络安全治理机制、合作机制的建构与完善，以及网络安全治理议题设置等方面的重要乃至核心作用，在目前单边主义、霸权主义和强权政治等非技术因素冲击网络安全格局的形势下，显得更为重要，国际社会亟待在联合国框架下进一步加强网络安全合作的有效机制。因为对发展中国家而言，积极参与联合国框架下的网络安全国际合作机制，是其增强网络能力、提升话语权的最佳途径。

2004 年联合国大会成立的联合国信息安全政府专家组（UNGGE），是全球网络安全规则最重要的多边进程，是由主权国家主导的构建国际网络规范的主要机制，其议题涉及关键信息基础设施保护、网络安全事件防范以及网络人权保护等领域，旨在促进全球网络空间负责任行为规范、全球网络安全政策与国际规则的形成。UNGGE 在和平利用网络空间、国际法适用、网络空间主权与人权保护和区分责任的国际法律原则等核心问题形成原则性共识成果，对“国际法如何适用于信息通信技术的使用”进行了阐述。2018 年，中俄等国共同向第 73 届联大提交信息安全决议草案，推动建立联合国信息安全开放式工作组（OEWG），草案获得通过；2019 年，新一届 UNGGE 继续运行，首届 OEWG 成立，联合国网络安全进程进入双轨运行机制。与 UNGGE 不同的是，OEWG 议题更广泛、邀请所有联合国会员国申请参加，依托闭会期间的非正式交流会议，纳入工业界、学术界等组织成员参与交流。[②]作为联合国框架下制定网络空间国际规则的核心机制，2021 年上半年，UNGGE 与 OEWG 先后协商一致达成最终报告，标志着网络空间国际规则制定取得重要新进展。

[①] 吴才毓：《网络空间国际治理政策法律：国际组织与规则探究》，《政法学刊》2022 年第 6 期，第 120 页。
[②] 参见戴丽娜、郑乐锋：《联合国网络安全规则进程的新进展及其变革与前景》，《国外社会科学前沿》2020 年第 4 期，第 33-43 页。

2.2.3　非政府行为体

非政府行为体的活动范围，有的只在一国范围内，如国内非政府组织、国内企业和国内行业协会等，而另一些如非政府国际组织、跨国企业和国际行业协会等会有跨国行为。[①]

网络空间治理的“协同治理模式”认为，网络是跨国界的、网络空间问题是复杂系统性的，网络安全治理需要政府部门、互联网企业、科研机构、网络用户等多元治理主体进行协调与合作，才能实现网络空间的良性、有序发展，有时单靠国家政府、政府相关国际行为体无法解决。在一国内部，虽然政府掌控着网络安全的各种权力，还拥有政策规划与行政执行优势，但绝大多数网络基础设施的设计、建立、维护、运营乃至服务的供应却是由私营部门所掌控。协同治理模式既不像“多利益相关方模式”那样淡化网络主权与政府的作用，又不像“多边治理模式那样”强调政府主导与权威，而是政府、企业、国际组织、技术社群以及网络用户等各个主体平等协商，共同制订大家可接受的国际规则，并加强协调互动，共担风险与责任。不同层次的网络安全问题要充分发挥不同参与主体的优势与作用，非国家行为体的参与主体角色必不可少，尤其是在物理层和逻辑层涉及技术议题时，他们在治理效率、治理民主性等方面具有不可或缺的价值，[②]但应当看到的是，网络空间已经成为大国竞争与对抗的主战场，多方网络空间治理力量的网络安全合作中，如何在顶层设计上实现治理资源的合理配置、协调彼此责任与权力，既能有效维护本国网络安全，又能推动网络空间国际法治迈向更高水平，是一个亟待解决的问题。

2.3　网络空间国际法治的现实困境

2.3.1　“数字鸿沟”与数字不平等

“数字鸿沟”与数字不平等，是网络空间国际法治进程中，亟待解决的基础性问题。美国学者最早提出“数字鸿沟”这一概念，他们本意是关注农村和城市部分地区的美国公民，在获取信息技术方面的严重落后。互联网、数字信息技术在提高社会生产力、带给人们极大生活便利的同时，“数字贫困者”和“数字富有者”开始分化，产生此等差距的原因包括两方面：收入差距导致的接入方式差异，以及信息获取方式不同等原因导致的使用方式差异。伴随着互联网普及率的不断提升，接入互联网的成本越来越低，因接入方式差异导致的数字鸿沟逐渐缩小，而因使用差异和算法歧视导致的数字贫困和信息不对称愈加凸显，并日渐成

[①] 参见张发林、杨佳伟：《统筹兼治或分而治之——全球治理的体系分析框架》，《世界经济与政治》2021 年第 3 期，第 129-130 页。
[②] 陈少威等：《互联网全球治理体系的演进及重构研究》，《中国行政管理》2018 年第 6 期，第 73 页。

为数字不平等的主要类型。[①]

将这一概念移植到国际社会，全球“数字鸿沟”比美国国内的数字鸿沟还要严重，这凸显了发达国家与发展中国家之间、城乡之间、不同收入群体之间的差距仍然很大。上文提到，网络霸权国在政治、经济、文化等各方面企图直接或间接地控制全球网络空间，“数字贫困国”的文化、价值观、理念、意识形态等被潜移默化地渗透，只能沦为数字剥削者与霸权者利润攫取的对象和政治决策上的附属，在网络主权原则早已确立的今天，数字殖民主义作为一种全新的殖民方式，其理论和现实价值应当得到关注，[②]因此联合国贸发会也曾将全球数字鸿沟与数字殖民主义联系起来，认为数字殖民主义表现为发达国家主要技术公司通过游说、基础设施投资以及向发展中国家捐赠硬件和软件，从而形成有利于他们的国家政策导向。[③]面对数字殖民主义倾向的全球数字鸿沟，联合国贸发会在《2021 年数字经济报告》指出，为了有效缩小数字鸿沟，各国政府应以协调与合作方式制定政策，加强双边、多边对话与合作，推动建立更加富有生机活力的全球网络空间；国际电信联盟也指出，国际社会需要加强对发展中国家特别是最不发达国家的支持，各国迫切需要加强数字合作，推动完善网络基础设施。[④]

2020 年 11 月，亚太地区 15 国签署了《区域全面经济伙伴关系》（RCEP）。RCEP 缔约方大多为东亚地区的发展中国家，其中不少国家的网络安全现状与网络技术发展状况堪忧，但 RCEP 尊重包容不同缔约方数据保护措施与网络安全状况的差异，承认国际社会存在“数字鸿沟”，同时为区域内发展中国家逐步适应数字经济迅猛发展、向发达国家主导的高标准协定靠拢提供了过渡期。[⑤]RCEP 将发展中国家和经济发达国家聚集在一起，集中体现了以发展中国家为主导的，追求数字经济发展与网络安全利益的诉求，作为缔约方的中国更是高度关注网络主权及网络安全，维护本国政府在网络领域的治理权限，反对网络自由主义者去管制化的主张[⑥]。RCEP 鼓励缔约方之间发生争端时善意地进行协商，通过磋商处理争端，避免强制性司法手段，不跟随私有化、自由化的绝对主义立场，而是采取了相对灵活的路径，确保缔约方独立自主地行使网络空间主权。[⑦]RCEP 深度释放 15 国的经济潜能，加速区域合作进程，在经济复苏过程中寻求更多共识，形成更强大合力，合作维护多边主义。在数字信息基础设施建设、共同打击网络犯罪等方面的响应协调能力的网络空间合作之上，RCEP 将继续推动网络空间合作的进一步扩容，利用现有网络空间合作机制，从研究、能力建设和技术援助等方面

① 宋保振：《“数字人权”视野下的公民信息公平权益保障》，《求是学刊》2023 年第 1 期，第 129-131 页。
② 刘皓琰：《当代左翼数字殖民主义理论评介》，《当代世界与社会主义》2021 年第 2 期，第 115 页。
③ 参见王淑敏：《全球数字鸿沟弥合：国际法何去何从》，《政法论丛》2021 年第 6 期，第 11 页。
④ 刘玲玲：《加强合作，缩小全球数字鸿沟》，《人民日报》2023 年 1 月 4 日，第 15 版。
⑤ 谢卓君、杨署东：《全球治理中的跨境数据流动规制与中国参与——基于 WTO、CPTPP 和 RCEP 的比较分析》，《国际观察》2021 年第 5 期，第 116 页。
⑥ 王燕、刘丹霞：《RCEP 跨境数据流动规制与中国因应》，《国际法学刊》2022 年第 3 期，第 41 页。
⑦ 参见王淑敏：《全球数字鸿沟弥合：国际法何去何从》，《政法论丛》2021 年第 6 期，第 10 页。

开展针对性的网络安全合作，促进区域数字经济的深度融合。

2.3.2　全世界共同面临的网络安全威胁

一是网络犯罪与网络恐怖主义猖獗。2020 年以来的新冠疫情大流行，使得一段时间内远程在线办公常态化，传统办公系统的安全漏洞刺激着网络犯罪高发；数字货币等虚拟财产的迅速发展，给了金融经济类犯罪极大的空间；网络环境的复杂与隐蔽等特点，使得网络恐怖主义在方式、特点等方面都与传统恐怖主义存在很大差别[①]。网络的开放性、跨国性，使得打击网络犯罪与网络恐怖主义成为全球性难题，也使得各国有必要从合作、共享的角度来考虑网络安全问题，以中国、俄罗斯等为代表的国家采取以国家和政府主导的网络犯罪与网络安全治理模式，强调在国际合作开展中必须尊重各国的主权完整与独立，主张国家和政府在打击网络犯罪上的主导作用。[②]

二是关键信息基础设施面临诸多威胁。结合中国网络安全法律法规的规定，关键信息基础设施是指面向公众提供公共通信、网络信息服务或基本商品的，以及支撑能源、通信、金融、交通、国防等重要行业和领域运行的，一旦遭到破坏、丧失功能或者数据泄露，可能严重危害国家安全、国计民生、公共利益以及给人民生命财产造成严重损失的重要网络设施、信息系统等。[③]关键信息基础设施薄弱，使得近些年诸多国家的金融、电力、能源等关键信息基础设施频繁受到袭击。在过去的几年里，勒索软件越来越猖狂且正变得更加复杂和有针对性，勒索攻击的技术门槛进一步降低，目标越来越多地瞄准能源、医疗、电信和铁路等关键信息基础设施，特别是考虑到新冠肺炎疫情和地缘政治紧张局势的持续影响，关键信息基础设施面临的网络安全形势日趋严峻，即使是发达国家也饱受困扰[④]。

三是网络霸权主义的威胁。作为互联网强国，美国在网络核心技术、资源、标准方面占有绝对优势，在网络空间国际行为准则的制定中占有主导地位，意图与盟友联合控制全球网络，表示尊重网络主权原则，但始终坚持“互联网例外论”，坚持由美国少数几个“利益相关者”社团机构等控制全球网络，排斥国际机构和其他主权国家参与全球互联网治理。[⑤]网络空间本应作为各国共享和交流的重要平台，由各国共建共享网络空间发展红利，却沦为美国霸权主义的工具，美国利用网络技术及霸权侵犯他国政治主权与网络主权，干涉他国内政，挑起社会矛盾，煽动他国政变、改变所谓的威权国家政权；与网络软硬件相关的主要技术由美国

---

① 沙纪元、曾范敬：《国际合作视角下我国反网络恐怖主义的困境与对策研究》，《网络安全技术与应用》2022 年第 11 期，第 151 页。

② 参见江溯：《打击网络犯罪的国际法新机制》，《法学》2022 年第 11 期，第 47 页。

③《关键信息基础设施安全保护条例》第二条，中国政府网 http://www.gov.cn/gongbao/content/2021/content_5636138.htm，最后访问日期：2023 年 2 月 20 日。

④ 中国信息安全：《2022 年全球网络犯罪态势、应对与展望》，https://www.wangan.com/p/11v71c4d3f22d2c8，最后访问日期：2023 年 2 月 11 日。

⑤ 参见刘煜、程恩富：《我国网络自主权维护问题与路径分析》，《东南学术》2021 年第 6 期，第 26 页。

跨国公司控制，全球信息的流动、存储和计算主要由美国网络公司管理，而美国政府在幕后对全球信息行使绝对控制权；全球互联网网页中，绝大多是是英文，西方特别是美式的文化、价值观、理念、意识形态等潜移默化地渗透着全球网民们，“自由、人权、法治”等观念在异国他乡没有实现它们真正的价值，而是变成了文化霸权主义、“颜色革命”的工具。

2.3.3　政策法律层面存在的问题

政策与法律问题所带来的挑战，直接影响着网络空间国际法治的发展。从一国网络空间顶层设计与战略政策来看，不同的国家网络空间政策趋势给网络空间国际法治带来的影响是不同的。网络空间国际法治的实践表明，在制定网络空间战略政策时，各国会优先考虑满足自身的实际需求，并尽力保持自身在网络空间的战略优势。由于一国网络空间战略政策往往涉及多个层面，因此主权国家在网络空间的战略政策的竞争性越高，网络空间国际法治面临的挑战就越多。例如，2011 年美国《网络空间行动战略》的发布，引发了国际社会对其采取网络空间军事化措施的质疑，美国的这一举动引发其他国家不安，导致网络空间军事化趋势显著加速，使得西方国家正在竞相实施军事化的网络空间战略。

与主要西方国家在网络空间表现的军事化趋势相反，以中国和俄罗斯为代表的发展中国家采取了明确反对军事化的网络空间策略。例如，俄罗斯在《2020 年前国际信息安全国家政策基本原则》中明确表示，如果将信息和通信技术用作信息武器，违反国际法的军事或政治目的，是对国际信息网络安全的严重威胁；中国敦促各国遵守《联合国宪章》关于不得使用或威胁使用武力的原则，不得违反国际法的基本原则，将信息技术用于不符合维护网络空间安全与稳定之目的。可见，不同的国家网络空间政策趋势给网络空间国际法治带来的影响是不同的，因此如何解决网络空间军事化趋势的危机，扭转国际社会特别是主要西方国家对网络空间军事化的偏好，更加关注网络空间的可持续发展，已成为网络空间国际法治发展的直接障碍。

法治的实现，要有良好的法律的制定，网络空间法治也是如此。因此物理层、逻辑层、应用层等各层面的网络空间国际法的“好坏”，都直接影响着网络空间国际法治。如果像美国的“长臂管辖”那般，直接进行网络空间跨境、跨国执法，不仅导致管辖权冲突，更会侵犯其他国主权；而一国如果与相关国家达成网络空间执法合作协议，并且自身又通过国内法治中的涉外规定实现网络空间的涉外法治，就实现了网络空间国内法治和国际法治的有机互动。因此，网络空间的法律问题如果得不到及时和适当的解决，也可能成为国家间冲突和对抗的根源。

第 3 章　网络空间国际法治与网络安全国际合作的互动

3.1　国际法治对网络安全国际合作的促进

早期学者试图将国际机制与国际法刻意拉开距离，但实际上国际机制与国际法仅从概念上辨析就非常相近，且晚近兴起的国际机制“合法化、法制化”，也即国际法律机制，其根本目的，就是满足进一步改进或提高国际机制的效率以促进合作的需要。权力对国际法之形成与变动的影响是间接的，作为法律的国际法具有相对稳定性，不得随意立改废，否则会使人无所适从；国际机制的形成是它的形成是权力直接推动的结果，国际机制追求的是一种稳定性之下的变动性，以满足权力变动的需求。[①]同时，作为国际机制法制化结果的国际法律机制，会与国际法进行互动与整合，但其本身并非国际法，但确是国际法治实践的组成部分。国际法律机制关注特定问题领域发展与演进的一系列制度、政策等。

国际机制与国际合作之间有着紧密的联系，基欧汉认为，“当一个政府推行的政策被其他国家的政府视为能够促进对其自身目标的相互理解时，就会产生政府间合作……合作需要一个协调个人或组织行动的谈判过程”。[②]国家之间的合作不可能没有任何冲突，但在“百年未有之大变局”的背景之下，国与国之间的互动更加频密，各国的共同利益对于开展合作起着推动的作用，在合作进程中，国际机制在降低交易成本、增强合作者谈判能力、确定合作权益等方面，以及在纠纷协调解决、监督执行以及对背叛的惩罚等方面都发挥着重要作用。

国际合作是各行为体之间在政策和行动上的相互协调与适应的行为，是增进社会整体利益的一种态度和行为，[③]主权国家是国际社会最基本的成员，因此国家间合作在这个意义上具有举足轻重的地位。即使是在网络安全合作领域，国家或地区政府、政府间国际组织等主体占绝大多数，因此以国家政府为代表的传统政治权力也是网络安全合作、网络空间国际规则制定的主导力量，而私营企业、民间力量等在权力与数量上仍处于次要地位。[④]尽管新冷战思维甚嚣尘上，但开放合作无论在理论上还是实践中，依然是国际社会的主流。面对充满不确定性的、无政府状态的国际社会，国际机制为各国之间的协调与适应提供了平台和渠道。在《霸权之后：世界政治经济中的合作与纷争》一书中，基欧汉发展出了一套关于国际机制的建构与运作的系统理论，他认为国际机制确立了行为体权利的界定原则和行使范围，提供了争议解决的决策程序，虽然无法提供明确的法律责任模

[①] 高潮：《国际法战略的基本问题及其中国立场》，吉林大学 2017 年博士论文，第 44-45 页。
[②] [美]罗伯特·基欧汉：《霸权之后—世界政治经济中的合作与纷争》，苏长和等译，上海人民出版社 2006 年版，第 51-52 页。
[③] 参王明生：《国际安全机制与当代中国——一种互动关系的分析》，中国政法大学 2006 年博士论文，第 35-36 页。
[④] 参见罗昕、蔡雨婷：《全球互联网治理规则制定的分布格局与中国进路》，《中国传媒大学学报》2022 年第 3 期，第 70 页。

式，但可以促成国家遵守法律责任；通过提供可靠信息以提高透明度，降低相互作用的成本，来促进合作协议的达成和维护合作协议；并通过奖励合作的行为体及惩罚不合作的行为体促进国际合作，进而减弱国际体系的无政府性。[①]

以正式化程度与约束程度为标准，对国际机制进行分类，国际机制可以分为硬机制与软机制。国际硬机制往往依托国际组织的这个平台，拥有硬性的规则制度、法律文件，清晰、程序化的投票决策机制等，通常协调地区乃至全球的特定问题领域，对成员或合作方具有强制约束力，这虽然有利于维持合作进程中的稳定性，但正是由于硬性规定，使得运行过程不灵活而效率低下、浪费时间，产生了很多议而不决的问题，这也使得新的国际硬机制的产生存在很大的困难。国际软机制是在硬机制的基础上发展起来的，不同与硬机制，它不依托明确的组织运作机构进行协调，不采取程序化的投票决策机制，不具有强制约束力，灵活性程度较高，具有非正式化和较低层次制度化的特征，强调各国之间的协调和持续互动，以在最大程度上达成共识。同时，软机制既能推动硬机制的形成，其本身亦可能转化为硬机制。此外，由于国际机制与国际法的密切联系，通过国际软机制的意义也能间接说明国际软法之治的作用。国际硬法的形成需要巨大的成本导致硬法难以制定，硬法的强势经常会引发反感心理和抵触情绪，一国基于自身利益考量可能无视硬法，种种情形使得“硬法不硬”，而“软法也可能不软”，软法既可以补充硬法不完善、不全面、不可用的问题，也可以补正硬法过于僵化、刻板的缺陷的问题，面对不尽相同的利益追求，软法以灵活的存在方式和多样的功能模式，凝聚国家之间的共识、促进国家之间的行为统一。

国际法律机制作为国际机制中的一种，或者说作为国际机制法制化的结果之一，它提高了国际机制促进合作的各种效能。国际法律机制促进了国际关系的规范化与国际机制的有效性，它在尊重国家主权的基础上，强调各国对特定领域问题的平等参与和共同责任。国际法律机制与国际组织存在的首要意义，就是减少冲突与促进合作。国际法律机制需要适时地制定、修改、解释和补充它的决策机制可以为自身的这一过程提供制度上的保障，但实际上很难建立一个真正稳定高效的决策机制；在合作的试探阶段，类似于合同缔约阶段，它能够帮助国家找出合适的合作伙伴；在正式合作阶段，它进一步提高了各国参与国际合作的安全性与可预见性，它能够降低信息成本、确立权利义务以及监督或惩罚背叛行为，从而降低交易成本等；随着合作的逐渐深入，依赖程度的逐渐加深，开展合作的议题不断增多，不可避免地会出现各种争议，这就要求建立适当的纠纷解决机制来处理国家之间的争端和纠纷。解决国际争端的法律机制，是政治和法律手段的有机结合，是和平解决国际争端的独特制度，为妥善解决国际争端提供可靠的制度

[①] See Robert Keohane, “After Hegemony: Cooperation and Discord in the World Political Economy”, Princeton University Press, 2005, pp.88-96.

保障。[①]这是国际法的发展所追求的宗旨，也为国际法的发展提供了合理性基础。

3.2　网络安全国际合作对国际法治发展的促进

合作是国际法治的基础[②]，国家之间在互利共识的基础上进行合作，解决共同面临的问题，在合作的基础上确立稳定、有效的国际法规范，以此来保障和监督合作的长期、稳定运行。因此可以说，某领域国际合作长期稳定的进行，会激发该领域国际法治实践的产生与发展，“国际合作关系”是一种重要的国际关系，这种重要的国际关系，必然需要一定的法律规范进行调整，以使该国际合作秩序化、规范化。网络安全国际合作也是如此，从双边网络安全合作，到全球性网络安全合作，都需要相应网络空间国际法的规范与推进，而网络安全国际合作关系的变化，也需要网络空间国际法做出改变，这是法的适应性的表现。

国际电信联盟（ITU）是联合国负责信息和通信技术的专门机构，它发布了许多网络安全框架、体系、结构和标准，同时其对网络安全国际合作秉持非常积极的态度[③]。《国际电信规则》（ITR）是 ITU 的一项重要多边法律条约，因此该规则也是构建网络空间国际秩序的重要规则之一。全球信息通信技术的飞速发展，使得 ITR 不能满足国际信息通信发展的需要，两大阵营对网络空间国际秩序规则主导权争夺的战火，也烧到了 ITR 的修订上。以美国为首的发达国家阵营的主要观点是，目前国际电信垄断的环境已不复存在，因此对大多数国家而言，利用 ITR 解决问题的基础已不存在；中国坚持“合作代替对抗”的理念，与俄罗斯等发展中国家阵营坚持认为，全球范围内出现了电信业务与互联网业务融合的新趋势，ITR 作为 ITU 的重要法律文件之一，必须跟上全球电信业的新趋势、与时俱进。最终发展中国家阵营的方案得到大多数国家的支持，这是发展中国家网络安全合作促进国际法治发展的积极实践之一。

再如，打击跨国网络犯罪需要国际合作，而此等合作需要可靠、强有力、有效的执法机制，直接催生了相关正式、非正式的国际机制也即国际硬法与软法，来有效应对网络攻击和冲突。识别一行为是否为网络威胁并确定其来源不容易，而且几乎不可能明确界定各国网络空间的边界，来解决网络犯罪的管辖权冲突或者无人管辖的状况。因此，哪怕是在小范围内开展网络安全合作，就网络空间边界、管辖权冲突等法律纠纷达成合意，意义也是重大的。互联互通的网络空间之内，网络威胁也不是局部的、而是世界性的，只有国与国之间、国家与国际组织之间等开展密切合作，建立健全网络安全合作机制与法律体系，才能积极应对网络威胁与网络技术叠加效应所带来的挑战，这也同时推进了相关领域网络空间国

[①] 参见刘志云：《国际法的“有效性”新解》，《现代法学》2009 年第 5 期，第 115-116 页。
[②] 何志鹏：《中国共产党的国际法治贡献》，《法商研究》2021 年第 3 期，第 24 页。
[③] 参见马光：《论国际法上网络安全的定义和相关国际规则的制定》，《中国政法大学学报》2019 年第 3 期，第 76 页。