国家间网络安全约束性协议何以达成*

黄　贝

【内容提要】　在新兴技术领域构建国际安全规则是国际社会高度关注的热点议题。在网络安全领域，虽然全球性规则进程面临严峻挑战，但已有一些国家在双边和多边层面达成了具有一定约束力的国际条约和政府声明等网络安全正式协议。为什么只有部分国家间的网络安全合作能够达成约束性协议，这是一个值得研究的核心问题。既有研究大多对各类网络安全国际规则缺乏清晰界定与区分，要么未充分考虑规则构建过程中的国家间互动，要么选择性地使用案例。作者将研究对象聚焦于国家间网络安全约束性协议，将国家共同网络安全危害与国家间政权威胁认知作为自变量，构建了以国家收益—损失考量为核心逻辑的理论框架。通过对欧洲委员会《网络犯罪公约》、中美就网络安全问题达成的共识、联合国网络军控规则进程和美俄网络安全对话四个案例的比较分析与过程追踪，可以发现国家共同网络安全危害与国家间政权威胁认知分别塑造了国家间共同利益以及本国对他国违约损失与承诺可信度的预估，进而共同影响网络安全约束性协议的达成。

【关键词】　国际规则；约束性协议；国际合作；网络安全；国际安全

【作者简介】　黄贝，武汉大学政治与公共管理学院讲师（武汉　邮编：430072）。

【中图分类号】　D815　【文献标识码】　A　【文章编号】　1006－9550(2024) 11－0086－29

* 本文系国家社会科学基金重大项目“新时代下国际领导力研究”（项目批准号：21&ZD167）的阶段性成果。感谢《世界经济与政治》匿名评审专家提出的宝贵意见和建议，文中错漏由笔者负责。

一 引言

在新兴技术领域构建国际安全规则是人类社会在不同历史发展阶段均面临的课题，也是目前国际社会高度关注的热点议题。世界政治进入数字时代后，国际安全新规则的构建率先在网络空间展开。近年来，制定网络安全国际规则日益成为大国竞争的重要领域，而学界就网络安全议题能否达成全球性规则持相对悲观的看法。[①] 事实上，虽然构建网络安全国际规则的进程仍面临诸多挑战，但一些区域组织或国家已经达成具有一定约束力的政府间网络安全协议。如欧洲委员会（Council of Europe）于 2001 年出台了《网络犯罪公约》，成为全球第一部关于打击网络犯罪的国际公约；中国、美国和俄罗斯等大国之间也达成了不同形式的双边网络安全共识性文件。

在网络安全国际规则体系中，一些国家为何能达成正式协议的规律尚未被学界充分重视和研究，既有研究也没有对网络安全正式协议为什么只能在部分国家之间达成这一核心问题进行解释。本文聚焦国家间具有约束性的网络安全协议这一规则类型，将国际合作理论与网络安全议题现状进行结合，尝试提出一个以国家收益—损失考量为核心逻辑的解释框架。本文认为，当某些国家共同面临严重的网络安全危害且不存在彼此间政权威胁认知时，这些国家更容易达成具有约束性的网络安全协议。本文对欧洲委员会通过的《网络犯罪公约》、中美就网络安全问题达成的共识、联合国网络军控规则进程和美俄网络安全对话等案例进行了比较分析和过程追踪分析，验证了本文提出的理论解释框架。

二 网络安全国际规则在不同理论视角下的形成原因

学界围绕网络安全国际规则何以形成这一问题主要从社会规范、制度合作、大国博弈和历史经验等四类理论视角展开了论述。

（一）社会规范的视角

规范是建构主义理论的核心概念之一。作为国际规范形成的新兴领域，建构主义学者较早对网络空间进行了研究。这些学者从社会规范的视角出发，重点关注区

① Alex Grigsby, "The End of Cyber Norms," *Survival*, Vol. 59, No. 6, 2017, pp. 109-122; Guiguo Wang, "Are There International Rules Governing Cyberspace?" *Journal of International and Comparative Law*, Vol. 8, No. 2, 2021, pp. 357-384.

别于国际法等“硬规范”的非约束性规范,[①] 分别在结构和单元层面讨论了网络安全规范形成的影响因素。一方面，社会规范类研究基于规范的生命周期理论，认为非约束性规范在网络空间内的形成有赖于其社会化过程。玛莎·芬尼莫尔（Martha Finnemore）认为，旧规范移植至网络空间是新规范形成的最优路径，应关注网络规范形成与进化的过程而非最终结果。[②] 袁正清等认为，网络规范的成功构建不仅需要对规范的内容进行探讨，还需理解规范构建的社会进程和特定行为体之间的相互作用。[③] 另一方面，社会规范类研究还从单元层面探讨了影响规范形成的行为体言辞、认知和社会实践等策略性因素。有学者将联合国信息安全政府专家组（UNGGE）于2013年和2015年达成的共识报告归因于联合国框架下有效的程序性规则。[④] 也有学者认为，网络安全规范困境形成的原因在于各行为体之间认知的差异及其对议题的高度敏感性。[⑤]

（二）制度合作的视角

关注全球治理、国际合作与国际制度的学者往往从制度合作的角度来理解网络安全协议的形成规律。约瑟夫·奈（Joseph S. Nye）认为，在网络空间治理领域已形成一套由松散耦合的规范和机制组成的机制复合体。[⑥] 奈提出了有助于各国就网络安全国际规则达成合作的三个因素：一是谨慎和对不确定后果的恐惧，二是与软实力相关的声誉成本，三是使规范内化的国内政治压力。[⑦] 奈还在后续研究中补充了国家间协调这一同等重要的因素。[⑧] 此外，还有学者从责任性机制构建与机制间

① Eneken Tikk-Ringas, “International Cyber Norms Dialogue as an Exercise of Normative Power,” *Georgetown Journal of International Affairs*, Vol. 17, No. 3, 2016, pp. 47-59.

② Martha Finnemore, “Ethical Dilemmas in Cyberspace,” *Ethics & International Affairs*, Vol. 32, No. 4, 2018, pp. 457-462; Martha Finnemore, “Cultivating International Cyber Norms,” in Kristin M. Lord and Travis Sharp, eds., *America's Cyber Future: Security and Prosperity in the Information Age* (*Volume Ⅱ*), Washington, D. C.: Center for a New American Security, 2011, pp. 87-102.

③ 袁正清、肖莹莹：《国际规范研究的演进逻辑及其未来面向》，载《中国社会科学评价》，2021年第3期，第129—145页。

④ Mark Raymond, “Social Practices of Rule-Making for International Law in the Cyber Domain,” *Journal of Global Security Studies*, Vol. 6, No. 2, 2021.

⑤ 齐尚才：《认知差异、双向互动与全球性规范建构——以网络安全规范的建构为例》，载《当代亚太》，2019年第3期，第129—156页。

⑥ Joseph S. Nye, “The Regime Complex for Managing Global Cyber Activities,” Global Commission on Internet Governance Paper Series, Paper No. 1, 2014.

⑦ Joseph S. Nye, “Normative Restraints on Cyber Conflict,” *Cyber Security: A Peer-Reviewed Journal*, Vol. 1, No. 4, 2018, pp. 331-342.

⑧ Joseph S. Nye, “The End of Cyber-Anarchy? How to Build a New Digital Order,” *Foreign Affairs*, Vol. 101, No. 1, 2022, p. 32.

共同演化等角度探讨了网络安全规则形成的其他影响因素。①

（三）权力政治的视角

近年来，大国围绕网络安全规则展开的博弈日益加剧，既有研究分析了权力政治因素对构建全球性网络安全规则带来的负面影响，其影响主要表现在三个方面：第一，美国的网络空间霸权使全球层面的网络安全规则难以形成，并导致网络规则在形成过程中出现了阵营化和碎片化问题。② 第二，现实主义理论的相关概念（如安全困境）对网络空间的影响根深蒂固，阻碍了网络规则的形成，③ 网络空间总体上仍处于“脆弱的稳定状态”。④ 第三，未来网络安全国际规则日益表现为国家间价值观、制度平台与规则主导权的博弈，而规则的演进取决于国家和非国家行为体之间的力量博弈，⑤ 这在一定程度上阻碍了全球性网络安全规则形成的过程。

（四）历史经验的视角

由于互联网技术实现大规模普及的时间并不长，国际社会通过制定规则来应对网络空间安全威胁的经验尚不丰富，因此有学者分析了与互联网技术类似的相关技术领域的国际规范，总结其从无到有的历史经验，尝试通过技术类比的方式获得经验与借鉴。奈回顾了自 1945 年以来核技术领域相关规范的形成过程，力图从中得出构建网络安全规范的规律性经验。⑥ 也有学者探讨了海洋和外太空等空间国际法的形成过程，试图从国际法中寻找参考价值。⑦ 但有学者将化学武器、生物武器、核武器与网络武器进行比较后认为，国际社会在未来达成全球性网络规则的前景并不

---

① Mark Raymond，“Managing Decentralized Cyber Governance：The Responsibility to Troubleshoot，”*Strategic Studies Quarterly*，Vol. 10，No. 4，2016，pp. 123-149；王明国：《竞争、拟态与变异：互联网国际制度的共同演化》，载《世界政治研究》，2020 年第 1 期，第 74—99 页。

② Tim Stevens，“Cyberweapons：Power and the Governance of the Invisible，”*International Politics*，Vol. 55，No. 3-4，2018，pp. 482-502；Roger Hurwitz，“The Play of States：Norms and Security in Cyberspace，”*American Foreign Policy Interests*，Vol. 36，No. 5，2014，pp. 322-331；黄子豪：《网络空间国际规范生成：现状、难点与进路》，载《战略决策研究》，2021 年第 2 期，第 63—79 页；黄颖：《新兴技术视域下的网络空间“碎片化”探究》，载《国际政治研究》，2022 年第 4 期，第 95—119 页。

③ 鲁传颖：《全球网络空间稳定权力演变、安全困境与治理体系构建》，格致出版社、上海人民出版社 2022 年版；Ben Buchanan，*The Cybersecurity Dilemma：Hacking，Trust，and Fear Between Nations*，Oxford：Oxford University Press，2016。

④ 江天骄：《全球网络空间的脆弱稳定状态及其成因》，载《世界经济与政治》，2022 年第 2 期，第 129—154 页。

⑤ 郎平：《网络空间国际秩序的形成机制》，载《国际政治科学》，2018 年第 1 期，第 25—54 页。

⑥ Joseph S. Nye，“Nuclear Lessons for Cyber Security?”*Strategic Studies Quarterly*，Vol. 5，No. 4，2011，pp. 18-38.

⑦ 李彦：《网络空间国际法发展路径问题探析——以海洋、空气空间和外空国际法的发展路径为切入点》，载《理论月刊》，2016 年第 9 期，第 182—187 页。

乐观。[①]

综上，既有研究虽然从社会规范、制度合作、大国博弈和历史经验等视角为该领域的理论研究奠定了基础，也为本文的研究提供了诸多启发，但这些研究仍存在一些局限，主要表现在三方面：第一，既有研究往往将网络安全领域的国际规则、规范和协议等文本混为一谈，但没有对其进行清晰界定与区分。第二，受规范扩散等理论学说的影响，既有研究虽然高度重视规则本身的政策表述和文本意义的解读，但对规则和协议背后的国家间互动缺乏讨论，也未能探究国家间正式协议何以形成的具体机制。第三，既有研究大多具有单一的理论偏好，倾向于有选择性地寻找更符合其理论假设的经验案例。有鉴于此，本文重点关注网络安全领域内国家间约束性协议，在本议题研究范围内尽可能收集了相关完整的案例，通过案例分析对网络安全协议的形成条件进行了探索。

三　国家间约束性协议的概念辨析

对于社会科学研究而言，如果不对研究对象进行明确界定以及对研究类型进行范围框定，该研究就很难展开。[②] 因此，明确界定国际规则体系中的“国家间约束性协议”这一概念尤为重要，这样可以将该概念与其他相近的概念进行区分，从而避免概念的混用。

（一）国家间约束性协议的定义

国家间约束性协议是国际规则的主要形式之一。国际规则是国际机制的重要组成部分，也是维持国际秩序的核心构成要素。[③] 国际规则既包括正式规则，也包括基于社会层面规范、习惯和个人内在信念的行为准则等非正式约束规则。[④] 作为一种正式规则，国家间约束性协议是指由相关国家政府达成且约定了共同行为准则的正式协议。界定该概念主要依据两个标准：其一，达成协议的主体是一国政府。其二，该协议的内容是相关国家对行为准则的共同承诺。

国家间约束性协议包括国家间法律性协议（即国际法）和政治性协议。虽然有

① Brian M. Mazanec, *The Evolution of Cyber War: International Norms for Emerging-Technology Weapons*, Lincoln: University of Nebraska Press, 2015.

② 刘丰：《类型化方法与国际关系研究设计》，载《世界经济与政治》，2017 年第 8 期，第 45—49 页。

③ 阎学通、何颖：《国际关系分析》（第三版），北京大学出版社 2017 年版，第 43 页。

④ Douglass C. North, *Institutions, Institutional Change, and Economic Performance*, Cambridge and New York: Cambridge University Press, 1990, p. 40.

一些研究将国家间约束性协议等同于国际法，但政府间不具有法律意义的政治性协议也日益受到学界重视。[①] 这两类协议具有不同程度的约束力。相较于国内法，国际法虽然缺乏强力执行机构作为其后盾，但当缔约国违反国际法时，受到侵害的国家或集体可以对违反国际法的国家采取相应的惩罚措施，如单方面提出终止条约以及采取适当的报复性措施等。[②] 因此，国际法对签约国而言是约束力最强的一种国际行为准则。[③] 国家间政治性协议的约束力来自两方面：一是国际舆论压力。由于国家间政治性协议是一国政府公开做出的国际承诺，如果违背承诺，该国政府将面临来自国际和国内观众的舆论压力，使本国在国际道义性和国内声誉上受损。二是他国的反制。一国如果违背其承诺，其他参与国可能对该国进行反制，使其遭受实际利益上的损失。[④] 虽然国家间法律性协议与政治性协议在约束力大小方面存在差别，但这两类协议共同构成了对一国政府具有约束力的正式国际规则。

（二）国家间约束性协议与相近概念的比较

1. 国家间约束性协议与广义的国际协议

国家间约束性协议并不等同于广义的国际协议。国际协议是国家间合作的基本表现形式，体现在现代国际关系的诸多领域。[⑤] 国际协议涵盖了国家间军事盟约、和平协议、经济贸易协定和政府间声明等。如前所述，本文关注的国家间约束性协议将约定的共同行为准则作为协议的主要内容，是相关国家围绕构建共同行为准则而达成的最终合作成果。也就是说，国家间约束性协议属于广义的国际协议的子集，但并非所有的国际协议都是国家间约束性协议。当然，具体内容中不包含国家共同行为准则的国际协议（如表达网络安全合作意愿以及宣布开展网络安全对话的政府间声明）并非毫无作用，因为这些协议可能不仅体现了国际合作进程所处的不同阶段，还能推动后续合作的开展乃至最终约束性协议的达成。因此，本文在案例过程追踪中将这类非约束性协议视为阶段性合作共识，以区别作为最终合作成果的约束性协议。

---

① 刘宏松：《国际防扩散体系中的非正式机制》，上海人民出版社 2011 年版，第 37 页；Farshad Ghodoosi，“Binding Political Commitments，” https：//illinoislawreview. org/online/binding-political-commitments/，访问时间：2024 年 3 月 4 日；US Congressional Research Service，“International Law and Agreements：Their Effect upon U. S. Law，” https：//sgp. fas. org/crs/misc/RL32528. pdf，访问时间：2024 年 3 月 4 日。

② 蒂莫西·希利尔著，曲波译：《国际公法原理》（第二版），中国人民大学出版社 2006 年版，第 7—9 页。

③ 阎学通、何颖：《国际关系分析》（第三版），第 299 页。

④ 阎学通著，李佩芝译：《大国领导力》，中信出版社 2020 年版，第 25—29 页；周建仁：《战略信誉、同盟结构与同盟弱化》，载《国际政治科学》，2020 年第 2 期，第 1—50 页。

⑤ 田野：《国际协议自我实施的机理分析：一种交易成本的视角》，载《世界经济与政治》，2004 年第 12 期，第 27 页。

2. 国家间约束性协议与国际规范

本文对网络安全领域的国家间约束性协议与不具有约束力的国际规范进行了区分，主要原因有两点：其一，约束性协议与非约束性国际规范的形成过程并不相同。其二，以国际法为代表的正式协议与非约束性规范在网络空间的治理实践中往往被视为不同类型的政策选项，一些国家对这两类协议也会表现出不同偏好。因此，一些受到较多网络安全国际规则研究讨论的网络安全规范并不属于本文的研究范围，包括由政府参与推动的自愿和非约束性网络安全规范（如联合国信息安全政府专家组提出的相关报告、北大西洋公约组织公布的《塔林手册》）以及由非政府行为体提出的规范倡议（如“网络空间国际法保护牛津进程”“网络空间信任和安全巴黎倡议”）。[①] 当然，国家间约束性协议与国际规范是一组有区别但并不完全对立的概念，因为“法律可以作为制定规范的基础，而规范也可以被编纂为法律”。[②] 一些获得国际社会广泛接受的国际规范很有可能发展为国际协议并获得正式的合法性，进而对国际安全秩序产生显著影响。[③] 国家间约束性协议与类似概念的关系如图 1 所示。

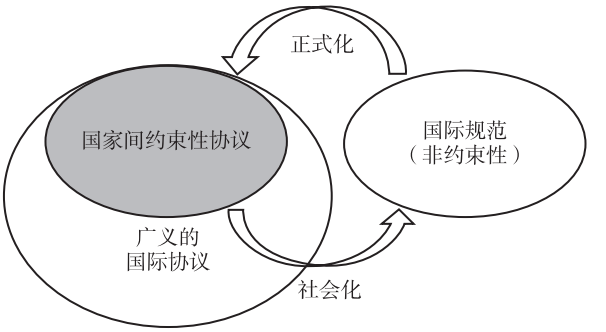

图 1　国家间约束性协议与相近概念的关系

资料来源：笔者自制。

注：灰色区域为本文研究的范围。

① 一些关注非约束性网络安全规范的研究已对其价值进行讨论，参见鲁传颖、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》，载《全球传媒学刊》，2020 年第 1 期，第 102—115 页；王蕾：《自下而上的规范制定与网络安全国际规范的生成》，载《国际安全研究》，2022 年第 5 期，第 130—156 页。

② Martha Finnemore and Duncan B. Hollis, “Constructing Norms for Global Cybersecurity,” *American Journal of International Law*, Vol. 110, No. 3, 2016, pp. 441-442.

③ 如“保护战俘”等非约束性规范通过海牙公约体系和日内瓦公约体系等国际法进一步确立，参见 Martha Finnemore, *National Interests in International Society*, Ithaca: Cornell University Press, 1996；徐进：《暴力的限度——战争法的国际政治分析》，中国社会科学出版社 2012 年版。

四 国家间网络安全约束性协议达成的收益—损失分析

为解释国家间网络安全约束性协议的形成原因，本文将国家共同网络安全危害与国家间政权威胁认知作为自变量，构建了以国家收益—损失考量为核心逻辑的理论框架，并在此基础上提出本文的研究假说。

（一）国家间网络安全约束性协议达成的分析框架

相关国家为达成网络安全约束性协议而展开的对话与谈判本质上都属于国际合作的范畴，合作的内容主要是各国共同做出的关于网络安全行为准则的正式承诺。本文假定参与网络安全约束性协议谈判进程的各个国家都是理性行为体，都会出于维护本国在该领域的现实利益而采取行动。这意味着本文解释范围内的协议进程至少应由两个在网络安全领域具有实际利益的国家组成。①

本文认为，相关国家能否顺利达成网络安全约束性协议主要取决于各国对合作收益与损失的权衡。国际合作的基础是各国通过合作获得收益，但如果有国家出现了违约，之前达成的协议反而会成为遵约国的一种单方面自我约束，进而损害该国的利益。因此，一国不仅需要考虑合作收益的大小，还要预估对方违背承诺给自身造成的损失。同时，对方的承诺可信度会影响一国对收益和损失发生概率的判断。因此，合作的共同利益、他国违约对本国带来的损失以及他国承诺的可信度等因素会共同影响网络安全约束性协议的达成情况。当相关国家通过合作实现的共同利益越大，对他国违约损失的预估值越小，且认为对方的承诺可信度越高，这些国家就越有可能通过合作达成协议。

事实上，一些受到较多关注的其他影响因素（如协议议题和协议类型）也可以被纳入收益—损失的分析框架（如图 2）。

第一，协议的具体议题会影响一国对共同利益或他国违约损失的预估，进而影响不同议题内约束性协议达成的难度。② 例如，在网络军控议题内形成的政府间约束性协议就具有消极合作的特点，签署国更需要考虑自身获得的相对收益；而政府

① 一些在数字技术领域较为落后的中小国家很可能因其在该领域不具有切实的现实利益而不参与国家间网络安全约束性协议的谈判进程，或基于其他领域的利益需求而采取追随大国的策略，只是在形式上参与谈判进程。

② 学界目前对网络安全议题存在不同的分类方法，如根据威胁行为类型、威胁者类型或威胁目标类型等不同标准进行了分类。参见约万·库尔巴里贾著，鲁传颖等译：《互联网治理》（第七版），清华大学出版社 2019 年版，第 93 页。具体网络安全事件也可能存在跨议题性或争议性。本文将依据具体协议谈判中一国政府给出的官方界定来判定其议题所属的类别。

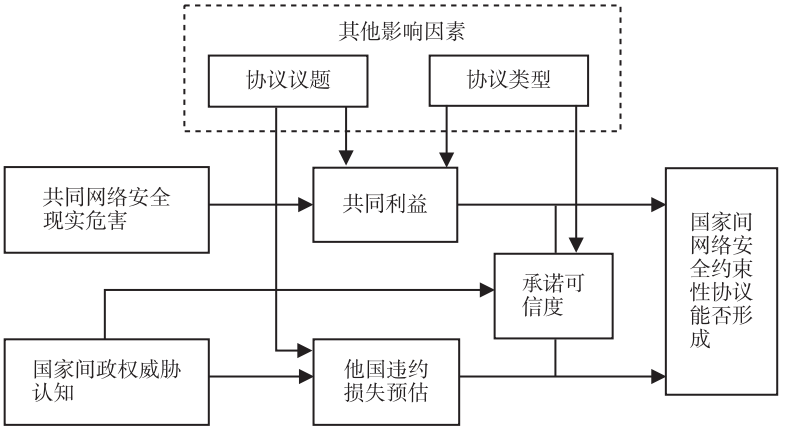

图 2　国家间网络安全约束性协议达成的收益—损失分析框架

资料来源：笔者自制。

在网络犯罪议题上达成的协议主要针对的是犯罪分子、民间黑客等非政府行为体，相关国家考虑更多的是各自获得的绝对收益，在该领域达成协议的难度较网络军控议题则更小。[①] 同时，网络军控等高政治议题对国家安全而言也更为敏感，一国对他国在该议题内违约造成的损失预估值可能较高，对经济和社会领域相关的网络犯罪等议题的预估值则较低，因此后者达成约束性协议的可能性更大。

第二，协议类型（多边或双边）会影响一国对国家间共同利益与他国承诺可信度的判断，进而对协议的达成产生不同方向的影响。一方面，随着谈判成员数量的增加，国家间共同利益协调的难度也随之增大，从而降低了达成协议的可能性；另一方面，在国家间共同利益相对稳定的情况下，多边协议具有的强规范性会给签署国带来更大的潜在违约成本。[②] 因此，多边形式的协议类型也可能会提高相关国家的承诺可信度，促成协议的达成。例如，虽然美国与俄罗斯难以通过双边形式在打击网络犯罪领域达成正式协议，但双方愿意在联合国多边机制下就网络犯罪达成全球性公约开展谈判。上述两个因素与下文讨论的主要自变量是互补性关系，而非互斥性关系。本文将控制这些已知因素的影响，进一步探究在协议议题和协议类型相似的情况下究竟是哪些因素影响了协议达成的不同结果。

① Joseph S. Nye, "Nuclear Lessons for Cyber Security?" pp. 21-22.

② 董柞壮：《科技协议如何影响双边关系——基于双重差分的因果分析》，载《世界经济与政治》，2024 年第 7 期，第 113 页。

（二）本文的主要自变量

本文认为，影响国家间网络安全约束性协议能否达成的主要自变量有两个：一是相关国家共同面临的网络安全现实危害是否严重，二是国家间是否存在政权威胁认知。其中，前者构成了国家间合作的共同利益即共同安全需求，后者影响了一国对他国违约后果可承受性与承诺可信度的看法。这两个自变量通过收益—损失机制使相关国家达成约束性协议的概率也随之发生变化。

1. 共同面临的网络安全现实危害

国家在网络安全领域开展合作的共同利益主要来自相关国家在应对共同安全威胁（即网络安全现实危害）时产生的共同安全需求，这与各国在现实空间中进行安全合作的情况相似。国际合作理论已对共同利益的重要性进行了充分论述，如现实主义理论论述了应对共同安全威胁对于联盟等安全合作形成的重要作用。[①] 有学者提出，共同收益是国际合作的原动力，包含着应对共同威胁的意涵。在当前全球性和区域性治理事务中，应对共同威胁已成为国际合作的重点。[②]

从历史上看，战争法和核不扩散条约等国际安全规则的诞生都与国际社会遭受重大安全损失后产生的共同安全需求有关。例如，19—20 世纪爆发的一系列战争导致的悲剧直接促使国际社会构建和发展了现代战争法的相关规则。[③] 再如，核武器的使用后果以及冷战初期大气层核试验带来的严重放射性污染等问题促使国际社会逐步建立了核不扩散和核裁军规则。[④] 与之类似，网络安全事件造成的危害性后果也会使各国从理性层面认识本国在该领域面临的安全问题，危害导致的后果也会带来政府和民众的恐惧情绪，从而在情感层面驱使国家采取行动。这种理性考量与主观心理共同催生出国家对网络安全领域国际规则的强烈需求，让相关国家在该领域形成共同利益并开展合作。

本文对网络安全现实危害的变量操作化主要基于两个维度：一是网络安全现实危害的严重性维度，二是网络安全现实危害的共同性维度。这两个维度分别对应四个具体指标（见表 1）。其中，严重性维度对应的指标分别考察的是某领域的网络安

① 詹姆斯·多尔蒂、小罗伯特·普法尔茨格拉夫著，阎学通等译：《争论中的国际关系理论》（第五版），世界知识出版社 2013 年版，第 563 页。

② 刘笑阳：《国家间共同利益：概念与机理》，载《世界经济与政治》，2017 年第 6 期，第 102—121 页；肖晞、宋国新：《共同利益、身份认同与国际合作：一个理论分析框架》，载《社会科学研究》，2020 年第 4 期，第 125—133 页。

③ 张卫华：《1949 年日内瓦四公约：国际人道法的基本标准的编纂和发展》，载《人权》，2016 年第 5 期，第 110—127 页。

④ 戴颖、李彬、吴日强：《禁忌与军备控制》，载《世界经济与政治》，2010 年第 8 期，第 48—62 页。

全事件在一国的影响范围、影响后果以及是否直接危害该国的关键基础设施。共同性指标则反映了相关国家在应对某领域内网络安全事件的危害而形成的共同利益，这种共同性具体包括两类经验现象：其一，相关国家的网络安全事件是否来源于共同的第三方行为体。其二，网络安全事件是否彼此相关。

表 1　国家共同面临的网络安全现实危害的测量指标

变量维度	具体指标	说明	经验证据举例
严重性	受影响的个人和行业是否迅速增多	体现其总体影响范围	网络安全事件发生的数量、事件影响的个人与企业的数量及其占比等
	造成的生命财产损失是否迅速增多	体现其影响后果	网络安全事件造成的金额损失等
	是否多次危及国家的关键基础设施	体现其对国家安全层面产生的重大影响	政府机关、国防、通信、能源、交通、金融和公共服务等关键基础设施受到破坏的具体网络安全事件
共同性	是否为相关国家需要共同应对的安全问题	体现其是否在国家间存在共性或关联性	来自共同第三方或彼此间的具体网络安全事件及数据

资料来源：笔者自制。

当某个案例同时满足表 1 中的四项具体指标时，本文即认为相关国家在某领域内共同面临的网络安全现实危害比较严重。由于网络安全事件通常具有隐匿性，一国政府对网络安全数据信息也有所保留，因此本文难以对上述指标提供有效且可操作的统一量化标准，而是将各案例中的经验事实与指标进行了对应。本文的相关事实材料主要来自联合国、欧洲委员会、国家政府的官方文件、微软公司等知名企业的研究报告以及相关媒体报道和学术研究资料等。

2. 国家间政权威胁认知

通常来说，国际合作并不必然建立在国家间互信的基础上，许多国家间合作协议的达成是由共同利益而不是互信驱动的。[①] 然而，网络安全的特殊性使这种情况在网络空间发生了改变。受网络空间对国家安全的敏感性以及网络行动核查困难的影响，作为一项基本政治信任，如果各国政府间不存在彼此政权安全威胁的认知，那么这将有助于促成协议的达成。

具体而言，国家间政权威胁认知是指一国政府认为对方是否会直接威胁本国政

① Yan Xuetong, "Strategic Cooperation Without Mutual Trust: A Path Forward for China and the United States," *Asia Policy*, Vol. 15, No. 1, 2013, pp. 4-6.

权安全，即威胁本国的政治制度或领导人执政地位的稳定。[①] 导致这种认知形成的行为包括他国对本国领导人执政地位合法性与本国政治制度的公开反对、他国意图推动本国政权更迭的行动以及对本国选举进行直接干预等。国家间政权威胁认知一般通过两种因果机制对协议谈判的结果发挥作用：一是影响一国对他国违约给本国带来损失的预估，二是影响本国对他国承诺可信度（即违约概率）的预估。

一方面，由于网络空间与国家安全在多个领域高度关联，一国政府往往认为，他国在网络安全领域内违约会对其构成政权安全威胁，带来的损失是自身难以承受的。互联网其实是一国的重要基础设施，与政治、经济和社会各方面已经实现了深度融合。一国对互联网等数字技术的依赖使网络空间对其国家安全而言具有高度敏感性，他国在该领域违约带来的安全风险可能直接危及本国的政权安全利益。因此，一国政府会倾向于提高对政权威胁国违约的损失预估。

另一方面，由于国家对网络行动的准确归因面临严峻的技术挑战，因此一国对彼此承诺可信度的判断也受政权威胁认知这一主观因素的影响。在常规武器和核武器军控等传统安全协议谈判中，一国往往需要明确判断彼此是否会履行其承诺的核查方式。[②] 然而，由于网络空间领域存在归因问题，一国政府难以完全准确地认定攻击者的地理定位和真实身份。[③] 例如，虽然美国政府近年来声称已经具备可靠的归因能力，但其归因行动仍多次遭到其他国家的质疑，完全可靠的归因技术和国际社会普遍认可的归因流程并不存在。[④]

在此情况下，国家间政权威胁认知较大程度地影响了一国对他国承诺可信度的判断。网络空间是国家间互动的新场域，各国用于判断彼此在该领域内可信度的历史履约情况和制度性保障的现实经验并不丰富。有研究指出，在无法直接观察对方

① 关于政权安全概念的讨论，参见 Richard Jackson，“Regime Security，” in Alan Collins，ed.，*Contemporary Security Studies*，New York：Oxford University Press，2013，pp. 161-75；孙学峰、张希坤：《美国盟国华为 5G 政策的政治逻辑》，载《世界经济与政治》，2021 年第 6 期，第 116 页；陈根锋、孙学峰：《美国盟国对中国智能监控技术的政策选择》，载《当代亚太》，2022 年第 3 期，第 26—57 页；朱杰进、胡馨予：《经济成本视角下经济制裁的有效性》，载《国际政治科学》，2023 年第 3 期，第 59—86 页。

② 李彬：《军备控制理论与分析》，国防工业出版社 2006 年版，第 121 页；吴日强：《大国竞争中的军备控制与全球战略稳定——以美苏核军控谈判为例》，载《外交评论》，2021 年第 6 期，第 59—62 页；江天骄：《同盟安全与防扩散——美国延伸威慑的可信度及其确保机制》，载《外交评论》，2020 年第 1 期，第 125—154 页。

③ 刘子夜：《论网络胁迫成功的条件》，载《国际政治科学》，2020 年第 2 期，第 148—183 页；杜雁芸：《网络军备控制为何难以施行？——基于客观层面视角分析》，载《国际论坛》，2015 年第 2 期，第 1—6 页。

④ 鲁传颖：《对国际安全领域公开溯源问题认知差异的思考》，载《中国信息安全》，2022 年第 5 期，第 75—78 页。

声誉和可信度时，对承诺可信度的评估一般依赖于决策者的个人印象和个人偏好等主观认知因素。[①] 也有分析认为，当前美国等西方国家的网络归因具有明显的意识形态色彩。[②] 因此，当一国政府应对他国政府对其执政地位和政治制度等政权安全利益带来的直接挑战时，该国政府对他国在网络安全领域违约概率的预估将更高。简言之，国家间政权威胁认知通过改变一国对他国违约带来损失的判断会影响合作协议的达成情况。当相关国家认为彼此不威胁对方政权安全时，它们更有可能展开合作；反之，相关国家则会失去合作的意愿。国家间政权威胁认知变量的测量指标是：一国政府是否认为他国政府直接威胁了自身的政治制度或本国领导人执政地位。这种威胁认知的主体和客体都是一国的政府或领导人，而非其他层面的行为体。

此外，由于国际合作并不是突发性事件，其合作通常是一个动态演变的过程，国家共同面临的网络安全现实危害和国家间政权威胁认知这两个因素往往以渐进的形式影响着协议谈判。随着网络空间安全形势、国家间关系和国内政治等因素的变化，相关国家间共同面临的网络安全现实危害与政权威胁认知会在不同时期发生重大变化：要么使国家间的合作有所推进，产生一些阶段性成果（如非约束性合作文件）；要么产生国家间合作的阻碍，甚至导致谈判进程终止。因此，本文的理论框架还将时间维度纳入其中，强调对案例的动态观察与过程追踪。在实证检验部分，本文对自变量进行考察的时间窗口为国家间合作出现结果（如签署合作协议）的前十年内，其原因在于：如果时间窗口过长，研究将难以清晰辨认自变量对因变量产生的因果效应；如果时间窗口过短，鉴于达成一项网络安全约束性协议涉及启动、协商和产生结果的完整过程，短期因素也不足以驱动整个合作进程，其检验也将失去意义。基于上述理论框架，本文提出两项研究假说。

假说 1：当相关国家在网络安全领域共同面临严重的现实危害且这些国家间不存在政权威胁认知时，它们更有可能达成网络安全约束性协议。

假说 2：当相关国家在网络安全领域并未共同面临严重的现实危害或这些国家彼此间存在政权威胁认知时，它们更有可能无法达成网络安全约束性协议。

---

① Tod Hall and Keren Yarhi-Milo, "The Personal Touch: Leaders' Impressions, Costly Signaling, and Assessments of Sincerity in International Affairs," *International Studies Quarterly*, Vol. 56, No. 3, 2012, pp. 560-573; 刘子夜：《论网络胁迫成功的条件》，载《国际政治科学》，2020 年第 2 期，第 148—183 页。

② Garrett Derian-Toth, et al., "Opportunities for Public and Private Attribution of Cyber Operations," https://ccdcoe.org/uploads/2021/08/Tallinn_Papers_Attribution_18082021.pdf，访问时间：2024 年 3 月 5 日。

五 案例检验

本文根据联合国网络政策门户（UNIDIR Cyber Policy Portal）数据库[①]和相关国家的政府公开信息，收集了已有结果的 16 个网络安全约束性协议的案例。出于案例代表性与相关事实材料的公开性和充足性的考虑，本文选择了四个重点案例。其中，欧洲委员会通过的《网络犯罪公约》和中美就网络安全问题达成的共识属于正面案例，联合国网络军控规则进程与美俄网络安全对话则属于负面案例。

除对重点案例进行比较分析与过程追踪外，本文还对其他案例进行了简要检验。[②] 研究步骤主要分为三步：首先，通过重点案例的比较分析检验两个主要自变量（国家共同的网络安全现实危害是否严重与彼此间是否存在政权威胁认知）与协议达成结果之间的因果关系。其次，通过重点案例的过程追踪来检验自变量发挥作用的因果机制。最后，对其他案例进行简要检验以验证理论框架对全案例样本的解释力。

（一）欧洲委员会《网络犯罪公约》

2001 年 11 月 23 日，欧洲委员会成员中的 30 个国家共同签署了全球第一部针对网络犯罪的国际法文件《网络犯罪公约》。[③] 该公约内容可归纳为三方面：第一，通过实体刑法条款规定了 9 种网络犯罪行为。第二，通过程序法条款规定了专门的调查程序和特别措施。第三，规定了引渡和主动提供信息等国际合作的一般规定以及特殊协助机制。[④]《网络犯罪公约》的首批签署国包括 26 个欧洲委员会成员国以及美国、日本、加拿大和南非 4 个观察员国。由 11 个国家的专家代表组成了负责《网络犯罪公约》起草的网络犯罪专家委员会，代表分别来自荷兰、比利时、加拿大、芬兰、法国、德国、意大利、日本、葡萄牙、英国和美国。[⑤] 囿于篇幅，本文主要对美国、英国、法国、德国和日本 5 个参与《网络犯罪公约》起草谈判的大国进行分析。

---

① United Nations Institute for Disarmament Research, “Cyber Policy Portal,” https://cyberpolicyportal.org/, 访问时间：2024 年 3 月 7 日。

② 本文预期将案例研究检验的因果假设作为概率性解释而非必然性解释，相关探讨参见叶成城、曹航：《比较案例研究中的或然性问题分析》，载《复旦学报（社会科学版）》，2023 年第 6 期，第 171—179 页。

③ Council of Europe, “Chart of Signatures and Ratifications of Treaty 185,” https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185, 访问时间：2024 年 3 月 7 日。

④ Council of Europe, “Convention on Cybercrime,” https://rm.coe.int/1680081561, 访问时间：2024 年 3 月 7 日。

⑤ 参见 Council of Europe, “Convention on Cybercrime: Special Edition Dedicated to the Drafters of the Convention (1997-2001),” https://rm.coe.int/special-edition-budapest-convention-en-2022/1680a6992e, 访问时间：2024 年 3 月 7 日。

1. 共同面临严重的网络安全现实危害

全球互联网在20世纪90年代迅速普及并取得较快发展。美国、英国、德国、法国和日本等发达国家的互联网用户规模在此时期快速增长，这些国家在电子商务领域占据着全球领先的位置，因而也成为最早在网络犯罪领域遭受严重现实危害的国家。

首先，网络犯罪在这些发达国家的影响范围迅速扩大，其造成的损失也在不断增加。美国的一份调查报告指出，在2000年前后，已有超过半数的美国受访者遭受过未经授权的网络访问。① 英国国家打击犯罪调查局（NCA）指出，1999年英国家庭共遭遇了100多万起网络犯罪事件。近1/5的英国公司曾遭到黑客攻击，超过1/3的英国公司曾是电子邮件攻击的受害者。② 德国计算机系统遭受的互联网入侵的比例从1996年的37%迅速上升至1999年的57%。③ 日本作为东亚地区早期互联网发展的“领头羊”，同样面临与日俱增的网络犯罪问题。日本警察厅（NPA）拘留审查的计算机犯罪案件数从1993年的32件增长至2000年的559件，日本各地警察在2000年受理的相关犯罪咨询数曾达到11135件，约为1999年的4倍。④

其次，发达国家的政府机构、金融服务部门和医疗部门出现加速拥抱互联网的趋势，针对这些关键基础设施部门的网络犯罪也随之初现端倪。一方面，一些网络黑客出于经济目的对发达国家的金融和医疗行业等基础设施发起了攻击。1990年，欧洲国家发生了首次针对医学研究机构的电脑病毒攻击。该电脑病毒制造者威胁受到攻击的机构，声称这些机构如果不支付赎金，他们将摧毁其核心数据。这一事件导致大量有价值的医学研究数据丢失。⑤ 1995年，美国花旗银行（Citibank）的计算机系统遭受黑客组织入侵，造成约1100万美元的损失。该案件是美国首个网上银行劫案，也给刚刚兴起的美国电子金融业敲响了警钟。⑥ 另一方面，黑客主义（hack-

① U. S. Department of Justice, “Remarks of the Honorable Janet Reno Attorney General of the United States to the National Association of Attorneys General,” https://www.justice.gov/archive/ag/speeches/2000/01-10-2000.pdf, 访问时间：2024年3月7日。

② “Report: UK Cybercrime Booms,” https://www.wired.com/1999/06/report-uk-cybercrime-booms/, 访问时间：2024年3月7日；Juraj Sikra, Karen V. Renaud and Daniel R. Thomas, “UK Cybercrime, Victims and Reporting: A Systematic Review,” *Commonwealth Cybercrime Journal*, Vol. 1, No. 1, 2023, pp. 28-59.

③ Wolfgang Wopperer, “Computer Crime,” https://www.imia.com/wp-content/uploads/2023/07/EP02-2002-Computer-Crime-2.pdf, 访问时间：2024年3月6日。

④ 日本警察庁：『平成13年警察白書』, https://www.npa.go.jp/hakusyo/h13/h130204.pdf, 访问时间：2024年3月16日。

⑤ “United Nations Manual on the Prevention and Control of Computer-Related Crime,” https://digitallibrary.un.org/record/162804, 访问时间：2024年3月7日。

⑥ “Hacking Theft of $10 Million from Citibank Revealed,” https://www.latimes.com/archives/la-xpm-1995-08-19-fi-36656-story.html, 访问时间：2024年3月8日。

tivism）成为个人和民间团体在网络空间挑战一国政府的新工具，政府机构的网站和服务器成为黑客频繁攻击的目标。1995 年，一个自称“斯特拉诺网络（Strano Network）”的国际黑客组织为抗议法国政府的核能和社会政策，对法国政府机构的多个网站发动了网络攻击。① 在 1999 年北约介入科索沃战争期间，黑客也通过带有电脑病毒的电子邮件和其他手段攻击了多个北约国家的政府网站。②

最后，网络犯罪活动呈现出明显的跨国性特征并具有一定的共同性。在美国花旗银行黑客事件中，美国联邦调查局（FBI）发现涉案人员分布于俄罗斯、美国、英国、以色列和荷兰等多个国家。③ 1998 年，英国政府与其他 13 个国家的警察部门合作破获了一个国际儿童色情组织，在欧洲、北美洲以及大洋洲等地区逮捕了约 100 名嫌疑人。该案件引发的公众舆论直接推动了欧美相关国家在网络犯罪领域的国内立法进程，也体现出构建网络犯罪国际规则的紧迫性。④ 与此同时，一些发达国家日益意识到国际合作在打击网络犯罪方面的重要性，纷纷表态要构建打击网络犯罪的共同国际标准。1985 年，欧洲委员会计算机犯罪问题特设专家委员会开始讨论要建立打击计算机犯罪的国际规则。1989 年，该委员会通过了“第 1 号建议 R（89）9”相关文件，建议各成员国政府在审查其立法或开始新的立法时要考虑计算机犯罪等相关内容。⑤ 美国也通过八国集团（G8）呼吁积极推动网络犯罪国际协议的达成。在 1997 年八国集团首脑会议上，美国政府提出了多项打击网络犯罪的行动倡议。⑥ 1998 年，八国集团峰会通过了打击网络犯罪的十项计划，提出了修改相关国内法与国际法进行协调的措施。⑦ 由此可见，发达国家在 20 世纪 90 年代就已经开始在网络犯罪领域共同面对严重的网络现实挑战，使得这些国家在该领域的合作需求日趋紧迫，形成了合作的共同利益。

---

① Dorothy E. Denning, “The Rise of Hacktivism,” *Georgetown Journal of International Affairs*, September 8, 2015.

② Eric J. Sinrod and William P. Reilly, “Cyber-Crimes: A Practical Approach to the Application of Federal Computer Crime Laws,” *Santa Clara University School of Law*, Vol. 16, No. 2, 2000, pp. 177-232.

③ “Citibank: Russian Hackers Broke into System,” https://www.upi.com/Archives/1995/08/18/Citibank-Russian-hackers-broke-into-system/6086808718400/, 访问时间：2024 年 3 月 9 日。

④ “This Club Had Its Own Chairman and Treasurer. Its Business Was Child Abuse,” https://www.theguardian.com/uk/2001/feb/11/tracymcveigh.martinbright, 访问时间：2024 年 3 月 10 日。

⑤ Council of Europe, “Recommendation No. R (89) 9 of the Committee of Ministers to Member States on Computer-Related Crime,” https://rm.coe.int/09000016804f1094, 访问时间：2024 年 3 月 12 日。

⑥ David L. Speer, “Redefining Borders: The Challenges of Cybercrime,” *Crime, Law and Social Change*, Vol. 34, No. 3, 2000, p. 263.

⑦ “Ten Principles to Combat High-Tech Crime,” https://dig.watch/resource/ten-principles-combat-high-tech-crime, 访问时间：2024 年 3 月 10 日。

2. 国家间政权威胁认知

冷战结束后，美、英、法、德、日等发达国家在整体上拥有较高水平的相互信任，彼此间并没有产生政权威胁认知。

首先，欧洲一体化进程向政治、外交和安全等多个领域全方位推进，其成员国之间的政治关系达到第二次世界大战结束以来前所未有的水平。其次，美欧双方重新构建了跨大西洋关系以及北约的未来图景。虽然美欧之间仍存在贸易争端，科索沃战争也一度给美欧关系带来挑战，但双方通过《跨大西洋宣言》《新跨大西洋议程》以及美欧联合行动计划等文件重塑了彼此间的伙伴关系，让美国“前所未有地介入欧洲”。① 最后，日美关系在冷战结束后进行了“再定义”，日欧关系也迅速发展。日本时任首相小渊惠三（Keizo Obuchi）在1999年访美时表示：“我可以满怀信心地说，日美关系正处于历史上最好的时期。”② 日欧领导人也一致强调双方在共同价值观的基础上实现政治互信，并将21世纪第一个十年定为“日欧合作十年”。③

总之，冷战结束后，上述发达国家不断调整并加深了彼此间的同盟与伙伴关系，这也为相关国家在打击网络犯罪等新议题上实现合作提供了重要的政治保障。这种政治互信有助于协议谈判国提升彼此承诺可信度的预估。有学者指出，如果将发达国家应对网络犯罪的制度与法律安排置于联合国框架下，有可能会受国家间政治矛盾所困，各国的承诺难以发挥其作用与效力。④ 欧洲委员会也表示，成员国对区域内其他国家司法体制的信任为这些国家在新兴科技领域进行国际合作以及开展相关协议谈判奠定了基础。⑤ 因此，上述发达国家更倾向于与盟友或伙伴进行合作，在打击网络犯罪领域构建共同的国际标准与行动准则。

3. 协议的谈判与出台

20世纪90年代日益严峻的网络犯罪问题使发达国家在该领域的共同利益迅速扩大，这些国家间良好的关系也为其构建国际规则提供了政治基础。在此背景下，欧洲国家、美国和日本等国在构建关于打击网络犯罪的约束性协议方面展开谈判与合作。

---

① Riccardo Alcaro, John Peterson and Ettore Greco, eds., *The West and the Global Power Shift: Transatlantic Relations and Global Governance*, London: Palgrave Macmillan, 2016, pp. 85-86.

② Ministry of Foreign Affairs of Japan, “Prime Minister Keiz Obuchi's Speech in Los Angeles,” https://www.mofa.go.jp/region/n-america/us/pmv9905/laspeech.html, 访问时间：2024年3月9日。

③ Ministry of Foreign Affairs of Japan, “Japan-EU Summit Joint Conclusions,” https://www.mofa.go.jp/region/europe/eu/summit/joint0007.html, 访问时间：2024年3月12日。

④ David L. Speer, “Redefining Borders: The Challenges of Cybercrime,” p. 270.

⑤ Council of Europe, “Working for Greater Confidence in Judicial Systems,” https://search.coe.int/archives?i=0900001680962b13, 访问时间：2024年3月9日。

欧洲委员会长期关注网络犯罪议题，该机构拥有丰富的国际立法经验并对非成员国的参与持开放态度，因此该组织成为一个理想的协议谈判平台。1995 年，欧洲委员会部长委员会通过了一项构建网络犯罪国际法律工具的设想。① 1997 年，负责《网络犯罪公约》起草事项的网络犯罪专家委员会正式成立，美国和日本等观察员国的代表也直接参与了该公约的起草工作。②

1997 年 4 月，《网络犯罪公约》的起草和磋商进程正式开始。此后，网络犯罪专家委员会召开的全体会议与起草小组会议交替举行：起草小组先对《网络犯罪公约》的内容进行技术性和法律性探讨，全体会议再对其讨论的内容进行确认。整个谈判过程经历了 10 次全体会议、15 次起草小组会议和 3 次关于该公约解释性报告的会议。③ 网络犯罪专家委员会主席亨里克·卡斯帕森（Henrik Kaspersen）指出，“各缔约方能在较短时间内就《网络犯罪公约》及其第一附加议定书的最后文本达成共识实属例外”。葡萄牙代表也认为，各国专家“在大多数问题上达成了广泛的一致意见”，这使公约作为解决方案被迅速接受。④ 在 2001 年 11 月 8 日举行的欧洲委员会部长委员会第 109 次会议上，《网络犯罪公约》的正式文本及其解释性报告顺利通过。在主要签署国共同面临严重网络安全现实危害和彼此间不具有政权威胁认知两个因素的共同推动下，网络犯罪领域的首个国际条约顺利达成。

（二）中美两国就网络安全问题达成的共识

2015 年 9 月，中美两国政府达成了网络安全领域的多项共识。在网络安全领域，双方同意展开关于网络犯罪的调查和信息协助合作，承诺不从事或支持窃取网络商业机密的行为，及时回应有关恶意网络活动提供信息及协助的请求，并共同制定和推动国际社会网络空间合适的国家行为准则。⑤ 这一共识性文件是中美两国就网络安全行为准则达成的首份双边合作成果，它虽然不具有国际法意义，但对相似

① Council of Europe，“Council of Europe Committee of Ministers Recommendation No. R（95）13，”https：//rm. coe. int/CoERMPublicCommonSearchServices/DisplayDCTMContent？documentId = 09000016804f6e76，访问时间：2024 年 3 月 12 日。

② Council of Europe，“Bureau of the CDPC（European Committee on Crime Problems），Meeting，November 1996，”https：//search. coe. int/archives？i = 09000016804d6d2d，访问时间：2024 年 3 月 10 日。

③ Council of Europe，“Convention on Cybercrime：Special Edition Dedicated to the Drafters of the Convention（1997-2001），”https：//rm. coe. int/special-edition-budapest-convention-en-2022/1680a6992e，访问时间：2024 年 3 月 7 日。

④ Council of Europe，“Convention on Cybercrime：Special Edition Dedicated to the Drafters of the Convention（1997-2001），”https：//rm. coe. int/special-edition-budapest-convention-en-2022/1680a6992e，访问时间：2024 年 3 月 7 日。

⑤ 《习近平访美期间中美关于网络空间的共识与成果清单》，http：//www. cac. gov. cn/2015-09/28/c_1116702255. htm，访问时间：2024 年 3 月 10 日。

议题内后续形成国家间协议的内容产生了极大影响。①

1. 两国共同面临严重的网络安全现实危害

中美两国都拥有庞大的互联网用户群体，也面临严峻的网络犯罪形势。这些恶意的网络活动不仅难以溯源其行为体发起国，也让双方对彼此产生猜疑。因此，中美在应对网络安全现实危害这一问题上具有较大的合作需求。

首先，从受影响人群范围来看，2009 年约有 52%的中国网民遭受过网络攻击，2015 年约有 95.9%的中国手机网民遭遇过手机信息安全事件。② 从具体经济损失来看，网络犯罪风险导致中国每年遭受的经济损失多达 600 亿美元，位列亚洲第一。③ 2015 年，网络犯罪活动对美国造成的经济损失已达 10.7 亿美元，接近 2005 年之前的十倍，美国联邦调查局也正式将高科技犯罪认定为最严重的犯罪类型之一。④ 同时，美国政府开始刻意塑造和鼓吹所谓“网络商业窃密事件”带来的威胁。美国军方有官员称，针对工业信息和知识产权的网络间谍活动已造成了美国历史上最大规模的财富转移，美国的公司每年因知识产权盗窃而导致的损失约 2500 亿美元。⑤

其次，中美两国均遭受了一系列针对国家关键基础设施的网络攻击事件。例如，2012 年 9 月至 2013 年 2 月，中国一些政府部门、重要信息系统以及科研机构等单位的网站被境外组织入侵并植入网站后门。⑥ 此外，境外黑客组织还长期针对中国政府机构和科研院所发起有组织的网络攻击。⑦ 而根据工业安全事件信息库（RISI）的数据显示，美国是 1982—2014 年遭受工业关键基础设施网络攻击事件最多的发达

① 参见 Duncan B. Hollis，“China and the US Strategic Construction of Cybernorms：The Process Is the Product，” Temple University Legal Studies Research Paper，Vol. 19，2017，p. 6。

② 《〈2009 年中国网民网络信息安全状况调查系列报告〉发布》，https：//www. isccc. gov. cn/xwdt/xwkx/04/251908. shtml；中国互联网络信息中心：《2015 年中国手机网民网络安全状况报告》，http：//www. cac. gov. cn/files/pdf/cnnic/2015phone. pdf，访问时间：2024 年 3 月 12 日。

③ 《网络安全保险或成企业标配 遇攻击勒索均可赔付》，https：//www. sohu. com/a/142745560_ 114731，访问时间：2024 年 3 月 12 日。

④ Internet Crime Complaint Center，“2015 Internet Crime Report，” https：//www. ic3. gov/AnnualReport/Reports/2015_ IC3Report. pdf，访问时间：2024 年 3 月 9 日；“New FBI Boss Says Cyber Crime，Not Terrorism，Is Top of Feds’ Todo List，” https：//www. theregister. com/2014/02/27/new_ fbi_ boss_ pledges_ cyber_ crime_ not_ terrorism_ will_ dominate_ agency_ in_ the_ next_ decade/，访问时间：2024 年 3 月 12 日。

⑤ Josh Rogin，“NSA Chief：Cybercrime Constitutes the ‘Greatest Transfer of Wealth in History’，” https：//foreignpolicy. com/2012/07/09/nsa-chief-cybercrime-constitutes-the-greatest-transfer-of-wealth-in-history/，访问时间：2024 年 3 月 12 日。

⑥ 《中国遭境外黑客攻击日趋严重》，https：//www. isc. org. cn/article/25000. html，访问时间：2024 年 3 月 13 日。

⑦ 《境外黑客组织“海莲花”首曝光 多次攻击中国》，https：//www. sohu. com/a/17084141_ 115052，访问时间：2024 年 3 月 13 日。

国家，针对美国发起的网络攻击占工业安全事件信息库事件总数的 58%，相关网络攻击尤其集中于美国的电力、交通、水资源和石油等重要行业。①

最后，中美两国不仅共同面临来自第三国跨国网络犯罪的威胁，双方还意识到网络安全风险具有彼此的关联性。美国政府一直鼓噪所谓“中国网络安全威胁”，②但实际上美国又是中国遭遇网络安全威胁的主要境外来源地。根据中国国家互联网应急中心提供的数据，2014 年 3 月 19 日至 5 月 18 日，位于美国的 2077 个木马或僵尸网络控制服务器，直接控制了中国境内 118 万台主机，135 台位于美国的主机承载了 563 个针对中国网站的钓鱼页面，造成网络欺诈侵害事件 1.4 万次。③ 由此可见，中美所面临的网络安全现实危害既来自第三方，也存在两者的关联性（特别是美国针对中国发动的网络攻击）。中美两国政府均表示有必要管控双边网络安全风险，主张加强双方网络安全合作。

2. 两国政府间认知情况

总体来说，虽然中美政治关系在网络安全领域达成共识性文件之前并非一帆风顺，但两国政府均未将双边矛盾视为对彼此政权安全的直接攻击与挑战，这在一定程度上为中美两国共同推动网络安全合作提供了重要政治条件。

2008 年奥巴马政府上台后，中美两国关系呈现出合作与波折并存的态势。一方面，2009—2012 年，中美两国政府领导人共会面 14 次，通电话 5 次，保持着较为密切的往来频率，④ 两国领导人也表示应加强在网络安全等全球性问题上的协调合作；另一方面，美国在网络安全领域却多次挑起矛盾，导致两国网络安全关系一度陷入僵局。⑤ 虽然中美两国的政治关系不时受负面因素的影响，但双方都保持着正面互动的意愿。在奥巴马政府时期，中美两国在经济与贸易、国防和全球治理等领域的双边合作不断深化。2014 年 11 月，在美国总统奥巴马对中国进行国事访问期间，中美两国领导人同意在双方利益重叠或一致的领域扩大合作，并对存在的分歧进行了坦诚务实的沟通，尽可能地缩小差距。奥巴马还重申美国欢迎“一个和平、

① Robert Ighodaro Ogie，“Cyber Security Incidents on Critical Infrastructure and Industrial Networks，” https：//ro. uow. edu. au/cgi/viewcontent. cgi? article = 1217&context = smartpapers，访问时间：2024 年 3 月 14 日。

② 李峥：《中美网络安全互动：挑战与机遇》，载《复旦学报（社会科学版）》，2016 年第 3 期，第 148 页。

③ 《炒作中国网络威胁 美国用心险恶》，http：//www. xinhuanet. com/world/2015-08/03/c_ 128088361. htm，访问时间：2024 年 3 月 15 日。

④ 《中国同美国的关系》，https：//www. mfa. gov. cn/web/gjhdq_ 676201/gj_ 676203/bmz_ 679954/1206_ 680528/sbgx_ 680532/，访问时间：2024 年 3 月 15 日。

⑤ 汪晓风：《中美经济网络间谍争端的冲突根源与调适路径》，载《美国研究》，2016 年第 5 期，第 89—90 页。

繁荣、稳定并在世界上发挥负责任作用的中国”持续发展。①

上述分析表明，奥巴马政府时期的美国对华政策没有将双边网络安全领域议题上升至国家安全层面，也没有对违约损失进行高估，因此有美国智库分析认为，中美两国政府在该时期均默认彼此间的网络活动处于各自预期的范围之内，这使双方克服了议题中的一些分歧与模糊，进而顺利达成共识。② 为实现网络安全合作，中美两国政府也有意在该议题上进行“降温”，避免合作受阻。奥巴马表示，网络黑客和商业窃密等问题并不是中美两国特有的问题，相关活动还涉及非政府行为体，两国可以共同努力实现合作。③ 中国在对美国国内炒作所谓“中国网络安全威胁”时也多次表示，中美作为两个网络大国，对抗和摩擦不是双方的正确选择，不应该将网络安全问题过度“政治化”。④ 在此背景下，中美虽然在一些网络安全议题上不时会产生摩擦，但两国仍将网络安全视为双边合作重要的议程，并对达成约束性协议持积极态度。

3. 协议的谈判与出台

在两国共同利益和政府间良性认知的推动下，2013 年中美两国政府建立了中美网络安全工作组，就双边网络关系和网络空间规则等内容展开对话。⑤ 2014 年，受美国炒作所谓中国“网络经济间谍威胁”的无端指控，该机制暂时中断运行。2015 年，中美两国政府重启双边网络安全对话，并试图通过一份双边协议确定共同规则标准。2015 年 9 月 9—12 日，中美两国高层官员就共同打击网络犯罪等问题交换了意见。在 2015 年 9 月习近平正式访问美国期间，中美两国最终共同推出了这份共识成果。

此外，中美两国就网络安全问题达成共识这一案例也排除了网络安全摩擦和网络观念差异等因素会导致国家间无法达成网络安全正式协议的竞争性观点，这表明网络治理理念不同的国家在拥有共同安全需求和不存在相互威胁认知的情况下仍可

① The White House，“Remarks by President Obama and President Xi Jinping in Joint Press Conference，” https：//obamawhitehouse. archives. gov/the-press-office/2014/11/12/remarks-president-obama-and-president-xi-jinping-joint-press-conference，访问时间：2024 年 3 月 16 日。

② Evan Burke，“The Obama-Xi Summit and the Prospects for a Global Norm Against Commercial IP Theft，” https：//carnegieendowment. org/posts/2021/06/the-obama-xi-summit-and-the-prospects-for-a-global-norm-against-commercial-ip-theft? lang=en，访问时间：2024 年 3 月 17 日。

③ The White House，“Remarks by President Obama and President Xi Jinping of the People’s Republic of China After Bilateral Meeting，” https：//obamawhitehouse. archives. gov/the-press-office/2013/06/08/remarks-president-obama-and-president-xi-jinping-peoples-republic-china-，访问时间：2024 年 3 月 17 日。

④ Everett Rosenfeld，“US-China Agree to Not Conduct Cybertheft of Intellectual Property，” https：//www. cnbc. com/2015/09/25/us-china-agree-to-not-conduct-cybertheft-of-intellectual-property-white-house. html，访问时间：2024 年 3 月 18 日。

⑤ 《中美网络工作组会间会在北京举行》，https：//www. fmprc. gov. cn/wjb_ 673085/zzjg_ 673183/bmdyzs_ 673629/xwlb_ 673631/201312/t20131204_ 7642720. shtml，访问时间：2024 年 3 月 18 日。

以超越摩擦与分歧，实现在网络安全议题上的合作。

（三）联合国网络军控规则进程

1. 合作概况

1998 年，俄罗斯向联合国大会裁军与国际安全委员会（即联合国大会第一附属委员会）提交了“国际安全背景下信息和电信领域的发展”决议草案，网络军控议题正式进入联合国议程。[①] 此后，虽然美国和俄罗斯等大国在网络军控等具体问题上的不同立场导致针对网络军控协议的谈判一直未能进行，但联合国关于宏观性网络安全议题的讨论日益增多。2004 年，联合国成立了信息安全政府专家组，对网络空间相关国际规范进行探讨。[②] 2018 年，联合国增设了信息安全开放式工作组（OEWG），其范围涵盖了所有联合国会员国以及工业界、非政府组织和学术机构等行为体。联合国的网络安全规则构建由此进入“双轨并行”的新阶段。

在联合国信息安全政府专家组平台上形成的报告成果虽然并不是专门针对网络军控议题的讨论，但内容涉及约束和限制网络空间国家军事行动的相关议题，在议程设置和规范塑造上具有重大意义。不过，从形式上看，这些报告大多具有“自愿”和“非约束性”特征，并不属于由国家间正式缔结的约束性协议。也就是说，网络军控领域的国家间约束性协议目前在联合国等全球性平台上尚未形成。

2. 网络战的现实后果与协议达成困境

本文认为，国际社会在联合国这类全球性平台上难以达成网络军控协议的主要原因在于网络战对多数国家造成的现实危害尚不严重，因此国际社会也缺乏强烈的合作需求。

自 2007 年爱沙尼亚遭到大规模网络攻击和 2010 年伊朗纳坦兹核设施电脑网络遭到名为“震网”的病毒攻击等重大网络安全事件后，国际社会对网络战的威胁感知迅速增强，“网络珍珠港”等描述网络战的概念频繁出现在公众视野中。[③] 然而，“网络威胁膨胀（cyber threat inflation）”和网络“超安全化（hyper-securitization）”的说法也随之出现，认为网络安全威胁和危害被夸大了。学界和政策界据此也调整

① 《从国际安全的角度来看信息和电信领域的发展》，https://www.un.org/zh/ga/55/doc/A55-140add1.pdf，访问时间：2024 年 3 月 20 日。

② United Nations，“Developments in the Field of Information and Telecommunications in the Context of International Security，”https://disarmament.unoda.org/ict-security，访问时间：2024 年 3 月 20 日。

③ 杨楠：《网络空间军事化及其国际政治影响》，载《外交评论》，2020 年第 3 期，第 84 页。

了对网络武器攻击实际影响力的评估。①

一方面，虽然“网络空间进攻方占优”在网络攻防讨论中一度成为主流观点，但后续研究对这类判断提出了越来越多的挑战，主要表现在三方面：其一，随着网络攻防技术的迅速发展，某个拥有计算机的个体对一个国家发起网络攻击的现象已很难出现。② 其二，由于网络攻击越发需要保持隐蔽状态，这会使网络攻击的成本不断提高。③ 其三，有效的网络防御使网络攻击的难度显著上升。④ 另一方面，网络攻击对国家安全产生颠覆性影响的预测也受到诸多质疑。虽然网络攻击可以为军事行动提供强大的辅助作用，但参战方对网络工具的单独运用并不能直接造成军事上实质性的杀伤效果，也无法实现军事占领或迫使对手投降。⑤ 有学者指出，网络武器很大程度上依然作为传统军事行动的配合手段，只能发挥其低于常规武力水平的作用。⑥

从国家军事力量参与网络军事行动的客观情况来看，已知的网络军事行动大多只涉及美国和以色列等少数国家。⑦ 这些网络行动在军事层面发挥的作用也相对有限。事实上，即使“震网”病毒攻击曾对伊朗核设施产生了实质性破坏，但该次行动也未能迫使伊朗放弃核计划，反而促使伊朗加速了其网络部队的建设。⑧ 有鉴于此，国际社会通过网络军控应对网络战所获得的共同利益仍然较低，各国暂时缺乏进行协议谈判的共同需求。当然，一些阻碍谈判的其他因素同样不可忽视。例如，美国试图推动战争法等既有国际法向网络空间延伸，企图将其军事霸权延伸至网络空间。对此，中国坚决反对网络空间军事化，呼吁维护和平、安全、开放、合作和

① Jon R. Lindsay and Lucas Kello, “Correspondence: A Cyber Disagreement,” *International Security*, Vol. 39, No. 2, 2014, pp. 181-192; Miguel Alberto Gomez and Christopher Whyte, “Breaking the Myth of Cyber Doom: Securitization and Normalization of Novel Threats,” *International Studies Quarterly*, Vol. 65, No. 4, 2021, pp. 1137-1150.

② Rebecca Slayton, “What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment,” *International Security*, Vol. 41, No. 3, 2016/17, pp. 72-109; Adam P. Liff, “Cyberwar: A New ‘Absolute Weapon’? The Proliferation of Cyberwarfare Capabilities and Interstate War,” *Journal of Strategic Studies*, Vol. 35, No. 3, 2012, pp. 401-428.

③ Erik Gartzke and Jon R. Lindsay, “Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace,” *Security Studies*, Vol. 24, No. 2, 2015, pp. 316-348.

④ 沈逸、江天骄：《网络空间的攻防平衡与网络威慑的构建》，载《世界经济与政治》，2018 年第 2 期，第 58—61 页。

⑤ Timothy J. Junio, “How Probable Is Cyber War? Bringing IR Theory Back in to the Cyber Conflict Debate,” *Journal of Strategic Studies*, Vol. 36, No. 1, 2013, pp. 125-133; Thomas Rid, “Cyber War Will Not Take Place,” *Journal of Strategic Studies*, Vol. 35, No. 1, 2012, pp. 5-32.

⑥ Lennart Maschmeyer, “The Subversive Trilemma: Why Cyber Operations Fall Short of Expectations,” *International Security*, Vol. 46, No. 2, 2021, pp. 51-90.

⑦ “Cyber Operations Tracker,” https://www.cfr.org/cyber-operations, 访问时间：2024 年 4 月 10 日。

⑧ 沈逸、江天骄：《网络空间的攻防平衡与网络威慑的构建》，载《世界经济与政治》，2018 年第 2 期，第 60 页。

有序的网络空间。大国对网络军控的观念和立场差异使它们在扩大共同利益和降低潜在损失的评估上面临挑战。此外，网络军控国际制度等公共产品供给不足以及既有网络空间国际治理机制效率低下等问题也导致提升合作承诺可信度的制度化保障机制严重缺位，阻碍了全球性网络军控协议的达成。①

（四）美俄网络安全合作

1. 合作概况

1996 年，美国与俄罗斯高级别军事代表团首次围绕网络战问题举行了非公开会晤，但未能达成任何协议。② 在共同安全需求的驱动下，美俄两国间实质性和机制化的网络安全合作始于美国奥巴马政府时期。2011 年 6 月，美俄两国负责网络安全事务的高级官员发表共同声明，呼吁建立双边网络安全工作组。③ 2013 年 6 月，美俄两国元首正式宣布成立网络安全工作组以负责评估信息通信技术威胁并提出具体的共同应对措施，两国同意采取一系列信息技术领域的信任构建措施。④

美俄网络安全工作组原计划于 2013 年 7 月推动两国网络安全合作磋商，但在当年 8 月发生了“棱镜门”事件，该事件逐步引发了美俄双边矛盾，此后美俄关系持续走向低谷。在此情况下，美俄网络安全对话机制陷入困境。截至目前，美俄两国仍未就网络安全问题重启对话合作，双边达成约束性协议的可能性较低。

2. 美俄两国政府间威胁认知的变化与双边谈判的中断

美俄两国在网络治理观念方面存在分歧，也时常在网络安全领域发生摩擦。然而，美俄网络安全协议谈判进程的中断并非由这些分歧因素所致，而是由两国间政权威胁认知因素所决定的。

2010 年之后，美俄关系多次受大选干预和地缘政治危机等事件的冲击，两国政治关系并不稳定。2011—2012 年，美国政府围绕俄罗斯国家杜马选举和俄罗斯总统

① 鲁传颖：《网络空间安全困境及治理机制构建》，载《现代国际关系》，2018 年第 11 期，第 51—52 页；江天骄：《全球网络空间的脆弱稳定状态及其成因》，载《世界经济与政治》，2022 年第 2 期，第 140—142 页；郎平、陈琪琪：《网络空间国际治理的机制复杂性及其影响》，载《同济大学学报（社会科学版）》，2023 年第 6 期，第 57—58 页。

② 王军：《多维视野下的网络战：缘起、演进与应对》，载《世界经济与政治》，2012 年第 7 期，第 95 页。

③ The White House，“Joint Statement by Cybersecurity Coordinator Schmidt and Deputy Secretary Klimashin，” https：//obamawhitehouse. archives. gov/sites/default/files/uploads/2011_ klimashin_ schmidt_ cyber_ joint_ statement. pdf，访问时间：2024 年 4 月 22 日。

④ The White House，“FACT SHEET：U. S. -Russian Cooperation on Information and Communications Technology Security，” https：//obamawhitehouse. archives. gov/the-press-office/2013/06/17/fact-sheet-us-russian-cooperation-information-and-communications-technol，访问时间：2024 年 4 月 23 日。

大选多次对普京总统表达质疑和公开批评。[①] 俄罗斯对此予以强烈回击，指责美国试图干预俄罗斯内政。[②] 奥巴马在连任美国总统后虽然表露出改善美俄关系的意向，但2013年发生的“棱镜门”事件和2014年爆发的乌克兰危机使美俄两国政治关系再次恶化。在此情况下，美俄网络安全工作组尽管处于停滞状态，但两国网络安全相关部门的高级官员仍有会晤。[③]

2016年，美国指责俄罗斯用黑客行为干扰了美国大选，该事件标志着美俄间政权威胁认知的塑造达到高峰，这也导致两国网络安全合作进程彻底中断。美国政府及其媒体声称，俄罗斯政府在2016年美国总统大选中针对美国选民、参选团队和选举系统采取了一系列网络行动，试图影响美国总统大选的结果。[④] 2016年10月8日，美国政府正式指控俄罗斯黑客在美国大选期间对民主党的电脑系统发起网络攻击。[⑤] 奥巴马随后宣布对涉嫌参与此次事件的9个俄罗斯实体和个人发起“冷战后对俄最严重的制裁”。[⑥] 特朗普上台后，该事件继续在美国国内发酵。美国的情报机构联合发布报告称，该事件意在“破坏公众对美国民主进程的信心”。[⑦]

在政权威胁认知高企的情况下，网络安全合作对美俄双方尤其是对美国而言已成为低概率选项。一方面，美国各界认为美俄网络安全合作会对其所谓民主体制带来重大风险，造成美国难以承受的损失。这种对潜在损失的强烈认知甚至改变了美国领导人在该领域的决策。特朗普就任美国总统后表示要与俄罗斯讨论组建“一个不可渗透的网络安全部门”，以应对干预选举的网络攻击等问题。[⑧] 这一倡议很快引发了美国国内的强烈反对，认为这会威胁美国的国家利益。美国联邦调查局网络刑

① “Putin Once More Moves to Assume Top Job in Russia,” https://www.tuscaloosanews.com/story/news/2011/09/24/putin-once-more-moves-to-assume-top-job-in-russia/28389776007/, 访问时间：2024年4月23日。

② “Putin Says U.S. Stoked Russian Protests,” https://www.reuters.com/article/us-russia-idUSTRE7B610S20111208, 访问时间：2024年3月23日。

③ “First on CNN: U.S. and Russia Meet on Cybersecurity,” https://edition.cnn.com/2016/04/17/politics/us-russia-meet-on-cybersecurity/, 访问时间：2024年4月23日。

④ 刘子夜：《论网络胁迫成功的条件》，载《国际政治科学》，2020年第2期，第173—175页。

⑤ “US Officially Accuses Russia of Hacking DNC and Interfering with Election,” https://www.theguardian.com/technology/2016/oct/07/us-russia-dnc-hack-interfering-presidential-election, 访问时间：2024年4月25日。

⑥ The White House, “FACT SHEET: Actions in Response to Russian Malicious Cyber Activity and Harassment,” https://obamawhitehouse.archives.gov/the-press-office/2016/12/29/fact-sheet-actions-response-russian-malicious-cyber-activity-and, 访问时间：2024年3月23日。

⑦ National Intelligence Council, “Assessing Russian Activities and Intentions in Recent US Elections,” https://www.intelligence.senate.gov/sites/default/files/documents/ICA_2017_01.pdf, 访问时间：2024年3月23日。

⑧ “Trump-Putin Meeting Rekindles Ridiculed Cyber Plan,” https://www.politico.eu/article/trump-putin-cybersecurity-joint-task-force-meeting-rekindles-ridiculed-plan/, 访问时间：2024年4月23日。

事调查部门的官员指出，美国应首先考虑确保俄罗斯不会利用从合作中获得的情报来损害美国利益。① 美国前国防部部长阿什顿·卡特（Ash Carter）也表达了类似观点，坚决反对特朗普就网络安全议题与俄罗斯进行合作的提议。在一片批评声浪中，特朗普随后表示放弃该提议。②

另一方面，美国政府对俄罗斯在网络安全领域的承诺可信度并不抱期待。时任美国驻联合国代表妮基·黑利（Nikki Haley）在谈及美俄网络安全合作时表示，美国无法信任俄罗斯。③ 曾担任美国国家安全委员会国际网络政策主任的梅根·施蒂费尔（Megan Stifel）也表示，美俄执法部门此前进行的网络犯罪信息交换合作实质上变成了“俄罗斯情报机构和犯罪集团的招募工具”。美国白宫网络政策主管罗布·克纳克（Rob Knake）指出，虽然不应否认美国与主要数字对手保持对话的必要性，但由于俄罗斯对美国抱有“恶意”，所以应将俄罗斯排除在美国网络外交对象之外。④

在此背景下，特朗普在其执政中后期对俄罗斯网络安全政策越发强硬，这一态势延续至拜登执政时期。2022 年乌克兰危机爆发之后，美国政府多次强调俄罗斯正在探索针对美国的网络攻击方案。美俄两国在网络空间的“信任真空”表明，美俄网络安全合作难以在短期内重启。⑤ 综上，本文对重点案例的比较分析可见表 2。

首先，从求同的角度来看，欧洲委员会达成《网络犯罪公约》和中美就网络安全问题达成共识这两个正面案例在协议议题与协议类型等因素上并不具有相同点，但相关国家由于面临共同的严重网络安全现实危害，各方也不存在彼此间政权威胁认知，因此都顺利地实现了合作并达成了协议成果。这在一定程度上检验了国家共同的网络安全现实危害以及国家间政权威胁认知两个自变量与国家间网络安全约束性协议达成之间的相关性，也说明了案例的差异性特征并不足以决定协议的达成情况。

其次，从求异的角度来看，本文在四个重点案例中对其他影响因素进行了控制，如谈判类型、协议议题和国家间网络观念差异等，这便于验证自变量对协议达成结果的影响。

---

① “Trump-Putin Meeting Rekindles Ridiculed Cyber Plan,” https://www.politico.eu/article/trump-putin-cybersecurity-joint-task-force-meeting-rekindles-ridiculed-plan/，访问时间：2024 年 4 月 23 日。

② “Trump Backtracks on Cyber Unit with Russia After Harsh Criticism,” https://www.reuters.com/article/us-usa-trump-russia-cyber-idUSKBN19U0P4，访问时间：2024 年 3 月 23 日。

③ “Donald Trump: Time to Work More Constructively with Russia,” https://www.bbc.com/news/world-us-canada-40549475，访问时间：2024 年 3 月 23 日。

④ “Trump's Cyber Tweets Cause Dismay, Confusion,” https://www.politico.com/story/2017/07/09/trump-russia-cyber-experts-240340，访问时间：2024 年 3 月 23 日。

⑤ The White House, “Statement by President Biden on Our Nation's Cybersecurity,” https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/21/statement-by-president-biden-on-our-nations-cybersecurity/，访问时间：2024 年 4 月 21 日。

表 2　重点案例比较分析情况

重点案例	时间	共同网络安全现实危害	国家间政权威胁认知	控制变量	协议达成结果
欧洲委员会《网络犯罪公约》（正面案例）	2001 年	严重	不存在	谈判类型（多边）	达成
联合国网络军控规则进程（负面案例）	1998 年开始	不严重	—		未达成
中美就网络安全问题达成的共识（正面案例）	2015 年	严重	不存在	协议议题（网络犯罪）、谈判类型（双边）、网络安全观念差异（较大）	达成
美俄网络安全对话（负面案例）	2011 年开始	—	存在		未达成

资料来源：笔者自制。

注：囿于篇幅，本文对两个负面案例的分析仅限于导致协议未达成的某一个关键自变量，未对另一个自变量展开详细论述，在表格中以“—”标识。

最后，本文通过对重点案例的过程追踪验证了理论框架中的因果机制。欧洲委员会达成《网络犯罪公约》、中美就网络安全问题达成共识以及联合国网络军控规则进程三个案例分别从正面或负面的视角分析了共同网络安全现实危害通过塑造相关国家共同利益进而影响合作结果的具体过程。欧洲委员会达成《网络犯罪公约》的案例展示了国家间政权的互信可以提升相关国家承诺的可信度，有助于各方达成协议。中美就网络安全问题达成共识这一案例表明，美国对华威胁认知弱化将有助于降低违约损失预估并促成双方协议的达成。美俄网络安全对话案例作为负面案例也检验了政权威胁认知因素在解释力方面的有效性。

此外，本文还简要分析了其他非重点案例（见表 3）。本文的案例池有 12 个非重点检验案例，其中有 10 个案例的自变量与因变量取值情况与研究假说一致，仅有 2001 年《独联体打击计算机信息领域犯罪合作协定》和中德网络安全磋商这两个案例不符合本文理论框架。在 2001 年《独联体打击计算机信息领域犯罪合作协定》案例中，独联体各成员国在 2001 年的互联网普及率均不及 10%，这表明相关国家面临的网络安全现实危害并不严重，但在这种情况下仍达成了合作协议。[①] 但该案例并不满足本文的理论假定，即该协议是一个由单一大国发起且其他中小国家采取追随方式进行的谈判，并不是本文假定的各国基于自身在该领域的实际利益而进行磋商协调后达成的协议。在中德网络安全磋商案例中，中德两国在该时期产生了应对

① 参见“World Development Indicators,” https://databank.worldbank.org/source/world-development-indicators，访问时间：2024 年 3 月 25 日。

网络犯罪的共同利益，但两国未能通过合作达成协议，该案例待相关资料更加充分后可做进一步的深入分析。

表 3　非重点案例检验情况

名称	时间	主要议题	类型	共同网络安全现实危害	国家间政治威胁认知	协议达成结果	是否符合本文理论框架
《非盟网络安全和个人数据保护公约》	2014 年	网络犯罪	多边	严重	不存在	达成	符合
《阿拉伯国家联盟打击信息技术犯罪公约》	2010 年	网络犯罪	多边	严重	不存在		
《上海合作组织成员国保障国际信息安全政府间合作协定》	2009 年	网络犯罪、网络恐怖主义	多边	严重	不存在		
《东盟关于预防和打击网络犯罪的宣言》	2017 年	网络犯罪	多边	严重	不存在	达成	符合
《美洲全面网络安全战略》	2004 年	网络犯罪	多边	严重	不存在		
《中俄关于在保障国际信息安全领域合作协定》	2015 年	网络犯罪、网络恐怖主义	双边	严重	不存在		
中英达成网络安全合作共识	2015 年	网络犯罪	双边	严重	不存在		
中澳高级别安全对话达成的网络安全合作共识	2017 年	网络犯罪	双边	严重	不存在		
《俄罗斯—印度信息通信技术安全保障领域合作协议》	2016 年	网络犯罪、网络恐怖主义	双边	严重	不存在		
《俄罗斯—伊朗信息安全保障领域合作协议》	2021 年	网络犯罪、网络恐怖主义	双边	严重	不存在		
《独立国家联合体打击计算机信息领域犯罪合作协定》	2001 年	网络犯罪	多边	不严重	不存在	达成	不符合
中德网络安全磋商	2015 年开始	网络犯罪	双边	严重	不存在	未达成	

资料来源：笔者自制。

六　结论

本文结合国际合作理论与网络安全议题的现状构建了国家间网络安全约束性协议达成的收益—损失分析框架，以国家共同网络安全危害与国家间政权威胁认知为自变量分析了国家间网络安全约束性协议何以达成的具体机制。本文认为，国家共同网络安全危害与国家间政权威胁认知两个自变量分别通过影响国家间合作的共同利益以及对他国违约损失与承诺可信度的预估，共同影响了国家间网络安全约束性协议成果的达成情况。

在理论层面，本文基于既有研究探究并细化了影响协议达成的具体因素与运行机制。虽然既有研究日益关注传统的权力政治因素对网络安全规则的影响，但本文的研究发现，地缘政治与大国竞争等宏观政治因素只有在催生国家间政权威胁认知时才更有可能导致协议达成的失败。此外，本文还对非重点案例进行了检验，进一步提升了理论框架的解释力。

在现实层面，本文对制定新兴技术领域的国际安全规则具有一定的启示意义。例如，各大国当下正围绕构建人工智能国际规则展开合作，虽然西方发达国家在人工智能领域存在明显的治理观念分歧，但包括美国、欧盟和英国在内的十个国家和组织仍能达成合作并共同签署《人工智能框架公约》等法律性协议。对此，中国可在具有客观安全合作需求的基础上创造出各方构建相关规则的政治条件，也可在双边和多边层面与伙伴国率先达成协议，塑造并扩散群体性规则共识。

本文对数字技术领域国际规则的形成规律进行了初步理论探讨，但也存在三点不足，可在未来的研究中做进一步探讨。首先，本文的分析主要基于网络安全国际合作在其初期阶段的经验事实，随着未来案例的增多，相关理论可能会无法充分解释出现的新现象，但这也能为知识的增进提供新的契机。例如，假使《联合国打击网络犯罪公约》在一些国家存在彼此政权威胁认知的情况下顺利达成，这种新的“反常”案例可以激发相关研究进一步拓展本文提出的理论框架。其次，本文提出的理论框架主要关注国家互动层面的因素，并没有深入讨论国际制度设计、国内政治和领导人特征等其他层面的因素。最后，未来的研究有必要辨析法律性协议与政治性协议得以达成的差异性规律以及影响协议约束力的关键因素。

（截稿：2024 年 8 月　责任编辑：赵远良）

bloc-oriented approach, maritime security, stigmatization

【Author】He Jiajie, Lecturer at the School of International Relations and Public Affairs, Fudan University.

Why Are Binding Inter-State Cybersecurity Agreements Formed?

Huang Bei (86)

【Abstract】The construction of international security rules in emerging technology fields has become a critical focus for the international community. In the realm of cybersecurity, although the process of establishing global rules faces significant challenges, some countries have already reached international treaties, government statements, and other formal cybersecurity agreements at bilateral and multilateral levels. Why do some international cybersecurity collaborations result in binding agreements while others cannot? Existing research often lacks clear distinctions among different types of cybersecurity rules, overlooks the dynamic interactions between states during the rule-making processes, or selectively applies case studies. This paper focuses on binding cybersecurity agreements between countries and uses common consequences of cybersecurity threats and the perception of regime threats between states as independent variables. The author constructs a theoretical framework based on countries' gain-loss analysis and conducts a comparative analysis and process tracing of four cases: the Council of Europe's Convention on Cybercrime, the consensus between China and the United States on cybersecurity issues, the UN process on cyber arms control rules, and US-Russia cybersecurity dialogues. The study finds that common consequences of cybersecurity threats and perceptions of regime threats between countries, by shaping common interests in cooperation and influencing the estimation of default losses and the credibility of commitments, jointly affect the achievement of binding cybersecurity agreements.

【Key Words】international rules, binding agreements, international cooperation, cybersecurity, international security

【Author】Huang Bei, Lecturer at the School of Political Science and Public Administration, Wuhan University.