论国际法的“数字化转型”
——兼评《国际法的数字挑战》白皮书

黄志雄*　罗旷怡**

内容摘要:迈进数字时代,大量数字化新领域新议题给国际法带来了新的挑战。国际法协会法国分会发布了《国际法的数字挑战》白皮书,提出公私界限模糊、网络空间国际法论辩的政治性和数字鸿沟三大挑战,以及值得进一步辩论和研究的问题,为思考数字时代国际法的走向提供了参考。实质上,为适应数字技术的发展以及非国家行为体功能地位的上升,现代国际法在国际造法和渊源、国际法律关系和实体规则、实施和遵守层面都面临着全方位转型升级的需要,主要表现为:网络空间国际造法在一定程度上呈现“国退民进”的态势,国际法渊源逐渐在社交媒体中兴起;非国家行为体的网络行动冲击着国家间法律关系,国际法实体规则面临内涵重塑和转型升级;数字技术为国际法的实施提供新的工具和方案。总体而言,数字时代国际法的转型升级既有机遇也有挑战,需要审慎对待。

关键词:国际法的数字化　网络空间　数字空间　非国家行为体　国际造法　国际法渊源　国际法实施

一、引言

我们正处于第四次科技革命浪潮的中心,数字化和智能化正在带来新的时代变迁。5G、大数据、云计算、区块链、人工智能、量子计算等数字技术发展速度之快、辐射范围之广、影响程度之深前所未有,现代社会从万物互联的网络时代迈向万物智联的数字时代。如果说网络时代的“网络空间”是指基于分布广泛、互联互通技术的人造空间,那么数字时代的“数字空间”[①]则是以更加广泛的数字技术作为人类活动

*　武汉大学国际法研究所教授、博士生导师。
**　武汉大学国际法研究所博士研究生。
本文系国家社科基金重大项目“网络空间国际规则博弈的中国主张与话语权研究”(20&ZD204)的阶段性成果。

① 网络空间(cyberspace)一词最开始出现于美国科幻作家威廉·吉布森1984年的小说《神经漫游者》,后来在《塔林手册》1.0版和2.0版中有比较客观中立的界定,指的是由物理和非物理组件构成,利用计算机网络储存、修改和交换数据的环境。参见[美]迈克尔·施密特主编:《网络行动国际法塔林手册2.0版》,黄志雄等译,社会科学文献出版社2017年版,第537页。而“数字空间”这一概念由中国科学家率先提出,是指地球之上空间的认知与应用通过数字化构建的空间。它是由天基、地基观测数据驱动,以科学认知为依据,空间通信网络、大数据、云计算等现代信息技术为手段,以“天人合一”为根本,“牵一发动全身”为灵魂的空间信息大数据库,是集空间科学、空间技术、空间应用与空间服务为一体的重大空间基础设施。参见魏奉思:《数字空间是空间科技战略新高地》,《中国科学报》2016年9月6日,第1版。

根基、[①]信息存在方式越来越趋于数字形式的虚拟空间。网络空间可以被视为数字空间的一个组成部分，它为数字空间提供了基础设施和技术支持，而数字空间则是所有空间的数字化转型和升级——将物理空间的全部信息复刻到数字世界，并实现人与人之间的交互。韩国互联网之父、国际互联网名人堂入选者全吉南认为，数字空间是一个以互联网和其他网络为基础设施，涵盖人工智能、数据、物联网、网络安全和社交媒体等不同层面的数字经济和社会空间。与网络空间相比，数字空间是一个更为中性的词语，前者往往与网络安全或网络战争联系起来，而数字空间与数字经济和数字社会的语境相适应。[②]总体而言，网络空间和数字空间都是数字时代的产物，只是使用语境不同，因此，本文在涉及网络安全或网络战争议题时，沿用“网络空间”这一通用概念。

为了回应数字时代的挑战，国际法学术团体国际法协会法国分会于2022年8月31日发布了《国际法的数字挑战》白皮书（以下称《数字白皮书》），[③]专门围绕数字数据（digital data）、数字安全（digital security）和人工智能（artificial intelligence）三大议题，探讨国际法在数字领域所面临的突出问题，并鲜明地提出了三大共同挑战：公共行为体与私人行为体之间的界限问题、网络空间国际法论辩的政治性色彩以及数字鸿沟。

就《数字白皮书》自身而言，有一些值得关注的亮点：一是大致勾勒了与数字问题相关的技术和国际法问题全貌。二是在强调数字技术对国际法造成挑战的同时，也考虑到数字技术给国际法带来的机遇，既关注到各种新技术的特殊性，也认为不应过于强调技术特性，而忽略共同的挑战与法律问题，辩证地看待了新技术与国际法的关系。三是清晰地梳理了共识性规则和争议性规则、现行规则和未来发展趋势，以及三个议题的交叉法律问题和各自的关键问题，兼顾了共识与分歧、现在与未来、一般与特殊的关系。

《数字白皮书》是国际法协会梳理和构想数字时代国际法发展演变的一个阶段性成果，也是专家学者在数字时代国际规则进程中的又一积极贡献。就《数字白皮书》与《塔林手册》[④]、

---

① 参见郎平、李艳：《数字空间国际规则建构笔谈》，《信息安全与通信保密》2021年第12期，第18页。

② 参见全吉男、邓珏霜：《厘清数字空间各层面治理》，《网络传播》2021年第5期，第68-71页。

③ See White Paper 16: Digital Challenges for International Law, https://www.ilaparis2023.org/wp-content/uploads/2022/08/Numerique-VHD-EN.pdf, visited on 10 October 2022.

④ 该手册由北约智库“网络合作防御卓越中心”（以下称“北约中心”）邀请国际法学者撰写，2013年出版的1.0版主要关注“网络战”相关国际法问题，2017年出版的2.0版大幅新增了主权、管辖权、国际责任、人权法等适用于和平时期网络活动的国际法规则，初步构建了一个包括战时法和平时法、相对完备的网络空间国际规则体系。2020年12月，“北约中心”宣布启动3.0版编写进程，计划通过长达5年的工作周期，不仅根据新的实践发展对2.0版的所有章节进行更新，还将视需要增加若干新的主题（章节）。3.0版的工作程序与前两版相比也有一定变化，如目前正在面向全球学界和非政府组织征集如何对2.0版进行修订和更新的书面意见，这是此前没有过的做法。此后，“北约中心”仍将邀请不同国家的若干国际法专家组成一个国际专家组，负责编纂和最终通过新手册的全部内容，并通过举办“政府代表咨询会议”邀请各国政府代表就手册有关内容发表国家观点，最后在2026年正式推出3.0版。

“牛津进程”[①]等其他学术团体的研究和编纂来看，《数字白皮书》也有一些新发展：超越了现有国际法在网络空间适用以及个别数字新议题治理问题的视野局限，对整体宏观架构和底层逻辑进行了一些反思。《数字白皮书》在最后结论部分还提出了一些值得进一步辩论和研究的问题，包括：法律渊源、法律的制定及解释和进一步发展、对新规则的需要；国家权能、域外效力；证明和证据；法律责任和归责；包括国际法的性质和制定在内更具有理论性意义的问题。[②]

但是，《数字白皮书》的有关内容也存在局限性，未能系统全面地揭示国际法的“数字化转型”，即数字时代国际法的转型升级。总体而言，受限于具体数字领域和数字议题的人为划定，《数字白皮书》多有重复或重合之处，如安全议题与数据、人工智能部分有很大程度的重叠，因为在数据和人工智能领域也存在安全问题；非国家行为体在制定和实施法律过程中的角色和作用，多边主义国际造法的正当性危机，新技术对国际法的渊源、制定、解释和逐步发展、证据等方面的影响，现有国际法的适用等，都是三大议题共同面临的挑战，但是《数字白皮书》将这些问题分散于各议题进行不全面的讨论，使得这些共同问题显得支离破碎，不成体系。也许更重要的是，由体例和风格所限，《数字白皮书》并未对国际法渊源、国际法律关系和实体规则的“数字化转型”等内容具体展开论述，即使对国际造法和国际法实施方面有一定的涉及也不够全面和深入。本文试图在《数字白皮书》及其他相关成果的基础上，对国际法的“数字化转型”这一主题进行更为深入的探讨。

在数字时代，数字技术构成社会发展的基础和驱动力，相应地，直接参与数字技术开发、使用和数字空间治理的科技企业、学术团体等非国家行为体的地位作用显著上升。基于此，数字时代国际法的转型升级基本上是由这两大因素共同推动的。与目前国内外学界集中于国际法具体数字新领域新议题（如数字人权、数字安全、数字贸易、数字技术标准、人工智能的规制等）的视角不同，本文拟从数字技术和非国家行为体对国际法整体底层逻辑的深刻影响出发，厘清数字时代国际法在国际造法和渊源、国际法律关系和实体规则、实施与遵守方面的转型升级，以期回应数字时代国际法所面临的机遇与挑战。

---

① 该进程是在牛津大学Dapo Akande教授和美国天普大学Duncan B. Hollis教授推动下，由牛津大学道德、法律与武装冲突研究所等机构在2020年4月牵头发起的。进程不定期围绕特定专题举办线上会议，每次邀请100名左右来自不同国家的参会者（主要是国际法学者，也有少量其他领域学者和政府、国际组织代表），会后围绕该专题发布一份“牛津声明”（Oxford Statement）作为成果文件。至今举办的六次线上会议，主题分别为新冠疫情期间对医疗设备的网络攻击、疫苗研发遭受的网络攻击、网络干涉选举、信息行动、网络空间审慎义务和勒索软件的国际法规制。除第五次会议推出了一份《网络空间的审慎义务》研究报告外，其他几次会议都分别推出了相关专题的“牛津声明”。

② See White Paper 16: Digital Challenges for International Law, p.101, https://www.ilaparis2023.org/wp-content/uploads/2022/08/Numerique-VHD-EN.pdf, visited on 10 October 2022.

二、国际造法和国际法渊源的“数字化转型”

国际造法是指国际法形成和演变的过程和方式，是动态意义上的“法源”，关注国际造法中的主体、参与者、过程、机制、外部条件、结果等；而国际法渊源是指国际法存在、表现和识别的形式和依据，属于静态意义上的“法源”，主要包括《国际法院规约》第38条所指的条约、习惯、一般法律原则、判例和学说等。[①]二者的视角不同，但都以各种方式相互塑造和影响。例如，国际造法可以通过引入软法、非国家行为体、非正式程序等新的造法形式或模式，影响国际法渊源。而国际法渊源可以为国际法规则和原则的创造和发展提供框架和语言，以及确定这些规则和原则的标准和方法，从而影响国际造法进程。

（一）网络空间国际造法中“国退民进”的态势

数字时代为非国家行为体深度参与网络空间国际造法进程带来了新的机遇。第一，数字问题通常是跨国的、多维的和动态的，需要具有相关专业知识、经验或对解决这些问题感兴趣的多利益攸关方的参与。在数据保护、数字人权等问题上，非国家行为体往往比国家和国际组织拥有更多的知识、技能或资源。正如《数字白皮书》所提到的，公共行为体与私人行为体之间往往存在“数字能力的不平等”，尤其是大型网络服务提供商能够控制和利用大量与公共治理、经济活动和个人权利密不可分的数据，同时也处于人工智能技术发展的最前沿，国家政府职能的实现很大程度上依赖于这些私营部门。例如，在新冠疫情期间，科技公司向卫生部门提供大数据分析工具，在行使管辖权（收集数字证据）等方面开展公私合作。[②]第二，非国家行为体（如互联网服务提供商、平台、用户等）在塑造网络空间治理规则方面也拥有更为显著的利益或影响力。它们作为网络空间的研发者、创建者、使用者，在网络空间享有较大的自主性和创造性，尤其是互联网企业能够通过开发和运营各种网络产品和服务，获取经济利益和提高社会影响力。第三，与外空、深海、极地不同，互联网深度融入人类社会生活，不同国家基于自身发展实力、价值观等因素有不同的利益诉求，网络安全、网络犯罪等议题容易变得高度政治化，[③]加上所涉法律问题较为复杂和多变，绝大多数国家仍然保持沉默，这些因素导致了相关造法进程

① 参见[日]村濑信也：《国际造法——国际法的法源论》，秦一禾译，中国人民公安大学出版社2012年版，第4-7页。

② See White Paper 16: Digital Challenges for International Law, pp.39-47, https://www.ilaparis2023.org/wp-content/uploads/2022/08/Numerique-VHD-EN.pdf, visited on 10 October 2022.

③ 即使是在网络犯罪这一原本政治敏感度相对较低、国际合作较易达成的领域，西方国家极力推动欧洲委员会制定的《网络犯罪公约》成为全球性公约，中国、俄罗斯等国则力主在联合国框架内制定新的网络犯罪国际公约。参见黄志雄：《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16页。

缓慢,存在大量的规则赤字,这也给非国家行为体参与、影响和塑造网络空间国际造法提供了更多自由发挥的空间。因此,总体而言,网络空间国际造法进程在一定程度上呈现出“国退民进”态势,非国家行为体可以发挥其在网络空间治理中的独特优势和影响力。

在数字时代,非国家行为体通过更加多元的途径全方位参与网络空间国际造法,包括参与专门性多利益攸关方进程、提供专家意见和指导,甚至独立发表声明、报告和倡议等,为网络空间国际规范和规则的制定和解释做出贡献。

第一,非国家行为体参与各种多利益攸关方论坛和平台,在促进各方在网络空间问题上的对话、合作和形成共识等方面发挥积极推动作用。例如,民间社会组织、学术界和私营部门等非国家行为体参加联合国互联网治理论坛(Internet Governance Forum,IGF),就互联网公共政策问题开展讨论。非国家行为体还参与区域和专题互联网治理论坛(如非洲互联网治理论坛、亚太互联网治理论坛和青年互联网治理论坛)以及其他多利益攸关方倡议(如全球网络空间稳定委员会、网络空间信任与安全巴黎倡议)。非国家行为体在这些专门性论坛和平台上,提供专业知识、规范倡议或技术标准,为网络空间国际规范和规则的制定提供建议;同时,通过表达自身的诉求和利益,影响政府和其他利益攸关方的决策和行动;与其他非国家行为体建立合作伙伴关系,形成共同的价值观和目标,影响网络空间国际规则的发展方向。

第二,非国家行为体通过参与官方程序或提供独立咨询,就网络空间国际法的各个方面提供专家意见和指导。例如,民间社会组织、学术界和私营部门等非国家行为体已被邀请作为观察员或顾问参加联合国信息安全政府专家组(GGE)和联合国信息安全开放式工作组(OEWG)。非国家行为体还就如何在网络空间解释适用国际法向国家和国际组织提供独立咨询意见。例如,学术界、智库等非国家行为体发表了各种论文和简报,就网络空间主权、国家责任、自卫、人权、审慎、归因等问题提供法律分析和政策建议。

第三,更为重要的是,非国家行为体独立发表各种声明、报告和倡议,试图澄清和发展网络空间国际法规则和规范。例如,学术团体发起的《塔林手册》进程和“牛津进程”,红十字国际委员会发表关于网络行动和国际人道法的立场文件,对推动和启迪国家之间关于国际法如何适用于网络空间的辩论提供了巨大助力。近年来,一些国家在相关主题的立场声明中,也明确表示学术著作和专家报告(包括《塔林手册》、“牛津进程”、红十字国际委员会的立场文件等)被视为重要的参考资料,并大量引用相关内容,作为论证本国立场主张的依据。[①]同时,作为关键网络基础设施的运

① 例如,德国在2021年发表的关于国际法适用于网络空间的立场文件中,5次在正文中、34次在注释中引用《塔林手册2.0版》。此外,《塔林手册》内容在联合国信息安全政府专家组、联合国信息安全开放式工作组等国际谈判中也被各国援引,并在谈判案文中有一定体现。

营者、产品开发商和服务提供商的私营公司，也为塑造网络空间负责任行为规范做出了重要贡献。[①]譬如，全球网络空间稳定委员会等民间进程、微软公司牵头发起的《数字日内瓦公约》等行业进程，已经达到与联合国信息安全政府专家组、开放式工作组等多边进程相当的重要程度，共同影响《塔林手册3.0版》的启动和编纂，[②]并且可能会潜移默化地影响网络空间负责任国家行为习惯规则的形成与发展。由于国家政府职能越来越多地依赖于非国家行为体的专业知识和技术支持，非国家行为体开展的规范倡议和推广活动，必然会深刻影响和塑造国家实践与法律文化，并且随着时间的推移，很有可能演变为数字领域的习惯规则。通过书面提出并推广关于可接受的网络空间行为的规范性标准，非国家行为体可以一定程度上遏制违反规范的恶意行为。进而，在主权国家努力解决有关国际法在网络空间的适用性问题过程中，非国家行为体制定规范的做法可以作为新的习惯规则的重要来源和“孵化器”。[③]

值得注意的是，非国家行为体在网络空间的国际造法方面发挥着积极作用的同时，也给国际法带来一些挑战，即国际造法的正当性危机。

一是模糊了正式造法与非正式造法的界限。例如，《塔林手册2.0版》国际专家组声称对网络空间相关的“实然法”进行编纂，但是该领域不仅鲜有成型的专门性国际条约和国际习惯，而且相关的国家实践也较少。鉴于此，该手册大部分内容实际上是通过类推方式，去设想网络空间的“应然法”。[④]而《塔林手册2.0版》在国家立场文件和各种国际论坛、平台被广泛引用的现实，模糊了专家进程和政府官方立场、实然法与应然法、“法”与“非法”（non-law）之间的界限，并且可能造成中西方、国家与非国家行为体话语权的失衡。

二是影响国家造法的表现。虽然从全球法律多元化的视角来看，非国家行为体参与国际造法进程并不会否定国家作为国际造法主体的权威，因为国家可以选择是

① See Jacqueline Eggenschwiler & Joanna Kulesza, Non-State Actors as Shapers of Customary Standards of Responsible Behavior in Cyberspace, in Dennis Broeders & Bibi van den Berg (eds.), Governing Cyberspace: Behavior, Power, and Diplomacy 249 (Rowman & Littlefield 2020).

② See International Law and Cyber Ops: Q & A with Mike Schmitt about the Status of Tallinn 3.0, https://sites.duke.edu/lawfire/2021/10/03/international-law-and-cyber-ops-q-a-with-mike-schmitt-about-the-status-of-tallinn-3-0/, visited on 1 March 2023.

③ See Jacqueline Eggenschwiler & Joanna Kulesza, Non-State Actors as Shapers of Customary Standards of Responsible Behavior in Cyberspace, in Dennis Broeders & Bibi van den Berg (eds.), Governing Cyberspace: Behavior, Power, and Diplomacy 254 (Rowman & Littlefield 2020).

④ 参见黄志雄：《网络空间国际规则制定的新趋向——基于〈塔林手册2.0版〉的考察》，《厦门大学学报（哲学社会科学版）》2018年第1期，第6页。

否承认或接受非国家行为体提出的倡议性规范。[①]但是,目前大多数国家对某些关键问题持模棱两可或沉默的态度,导致国家同意这一国际造法正当性和有效性的依据[②]存在不确定性,影响国家造法的表现,例如条约制定滞缓、国家代表在空洞的软法规范中“寻求庇护”。相较而言,非国家行为体在数字领域所拥有的资源和能力可与国家相抗衡,并且具有强大的规则或规范塑造能力和意愿。因此,非国家行为体可能还会利用国家在这方面的权力真空,破坏国家的主导地位,进而削弱国家在数字领域实现其战略和政治目标的能力。[③]

三是非国家行为体缺乏造法者所期望的问责制、透明度和代表性,并且可能存在隐蔽的破坏公共利益或共同利益的利益或议程。例如,一些私营公司、基金会可能基于商业或意识形态动机,影响其参与国际造法过程中对个人和集体利益的平衡。此外,大多数有影响力的非国家行为体(如微软、谷歌、脸书、互联网名称与数字地址分配机构)都源于西方国家,可能会带有西方国家的价值观和利益考量,导致在网络空间国际规则博弈中的权力不对称、利益冲突和缺乏权威性或代表性等问题。联合国信息安全开放式工作组、“促进网络空间负责任国家行为的行动纲领”(the Program of Action for Advancing Responsible State Behavior in Cyberspace,POA)等进程也意识到这一点,多次研讨非国家行为体利益攸关方的参与方式,以确保其合法性、可问责性、平衡性和有效性。

总体而言,网络空间国际规则的制定在很大程度上超越了狭义上的国家主导的传统造法进程,可以理解为广义上的多利益攸关方的法律论辩和塑造活动,包括对国际法的解释和适用,确定习惯规则,通过软法规范和适用手册推动国际法的发展。数字时代这种新样态的造法进程侧重于参与塑造认知和产生造法性实践的不同行为体(国家和非国家行为体)之间的互动,网络空间国际法就是通过这种互动发展起来的。不过,在肯定非国家行为体对网络空间国际造法的积极作用的同时,需要审慎对待由此带来的正当性危机。

(二)国际法渊源在社交媒体中的兴起

迈进数字时代,各国的沟通和外交方式发生了改变,越来越多的国家元首、外交

---

① See Paul Schiff Berman, Non-State Law Making through the Lens of Global Legal Pluralism, in Michael A. Helfand (ed.), Negotiating State and Non-State Law: The Challenge of Global and Local Legal Pluralism 15-40 (Cambridge University Press 2015).

② 虽然某些国际法规则(如强行法)对所有国家都有拘束力,无论国家同意与否,但是这并不是国际造法的结果。应当明确的是,国家同意仍然是大部分国际法拘束力的依据。参见白桂梅:《国际法》,北京大学出版社2015年版,第39页。

③ See Kubo Mačák, From Cyber Norms to Cyber Rules: Re-engaging States as Law-makers, 30 Leiden Journal of International Law 877-899 (2017).

官使用互联网、脸书、推特等社交媒体作为沟通、收集信息和公共外交的新工具。[①]社交媒体使国家元首、政府高官、政治家们能够绕过传统媒体，直接进入公共辩论领域。例如，美国前总统唐纳德·特朗普在其个人推特账号上频繁发表言论。尤其是新冠疫情暴发后，数字工具被更加普遍地用于行使核心外交职能，多边外交中的视频会议和其他数字通信手段确保了外交实践和谈判的连续性。在外交实践中，社交媒体可以成为沟通谈判各方立场的重要工具。例如，英国脱欧谈判的动态是由首席谈判代表和其他参与者在推特频繁发文塑造的。[②]

推特挑战了传统的外交观念，即传统外交是通过正式的沟通渠道和非正式的面对面社交活动进行的。那么社交媒体作为表达意图的工具有多大作用？在传统面对面外交有限的情况下，这种媒介能否成为对话和发展信任的有效平台？[③]在社交媒体上发表的言论的国际法意义何在？国家代表人在社交媒体上公开发表的帖子是否构成单方法律行为、能否作为习惯国际法的证据？这些问题都值得我们进一步思考。

虽然国家单方法律行为不在《国际法院规约》第38条第1款所规定的法律渊源之列，但是李浩培先生认为单方法律行为是特殊国际法的渊源，在做出意思表示的一方与有关的他方之间产生国际法上的行为规则。国家单方法律行为的约束力与条约约束力具有同一法律基础——“诚实信用原则”（或称为“善意原则”），即其效力依据主要是保护一方对他方意思表示信赖的一般法律原则。[④]在1974年澳大利亚诉法国核试验案的判决中，国际法院认为：无论法律义务的渊源如何，管理法律义务的产生和履行的基本原则之一是诚实信用原则。信任和信心是国际合作所固有的，特别是在许多领域的合作变得越来越必要的时代。[⑤]此外，在尚不存在有关实在国际法规则的时候，国际社会往往通过单方法律行为逐渐形成法律确信、形成默示的国家合意，[⑥]从而催生新的习惯国际法。这同样适用于数字时代。

如果在社交媒体上发表的声明相当于单方法律行为，则没有理由将这些声明

---

① 2019年，Twiplomacy组织了一次推特民意调查。他们在推特上询问了世界各国领导人、政府和外交部如何使用这个平台，以及推特对数字外交有什么好处。大多数外交部回答道，“推特是推进外交和外交政策目标以及沟通外交和领事活动的工具”。See Internet and Social Media: A Focus on Diplomacy, https://www.diplomacy.edu/histories/internet-and-social-media-a-focus-on-diplomacy/,visited on 1 March 2023.

② 联合国等国际组织也利用社交媒体平台和其他数字工具来加强信息的交互性传播。例如，截至2023年5月中旬，联合国、世界卫生组织在推特的关注人数分别达到1620万和1220万。

③ See Constance Duncombe, Twitter and Transformative Diplomacy: Social Media and Iran-US Relations, 93 International Affairs 545 (2017).

④ 参见李浩培：《国际法的概念与渊源》，贵州人民出版社1994年版，第117页；Alexander Orakhelashvili, Akehurst's Modern Introduction to International Law 32 (Routledge 2019).

⑤ See Nuclear Tests (Australia v. France), Judgment, ICJ Reports 1974, para. 46.

⑥ 参见罗国强：《国际法本体论》，中国社会科学出版社2015年版，第320页。

与在其他领域做出的单方法律行为从根本上区别对待。[①]社交媒体上的声明如果满足以下四个方面的标准，一般可以被认定为单方法律行为：（1）行为人必须表达受行为条款约束的意愿或意图；（2）行为必须由代表国家并以官方身份行事的机关或官员做出；（3）声明的内容必须是可接受的合法客体（如不能与强行法规则相抵触），并且意思表示必须足够明确；（4）形式并无特殊要求，只要在社交媒体公开发表。[②]

同样，在习惯国际法方面，只要满足主体资格、内容足够明确清晰等一般条件，发表在社交媒体上的声明可以作为习惯国际法国家实践和法律确信的证据。[③]虽然还没有国家明确将社交媒体上的帖子（如在推特上发表的文字，以下称“推文”）作为国家实践或法律确信的证据，但是在官方的“国家实践摘要”（digests of State practice）中已经对国家层面账号发布的推文有所提及。[④]此外，还有其他迹象表明，各国及其代表意识到社交媒体帖子可能有助于促进习惯国际法的形成。在一次关于2021年2月联合国安理会“阿里亚办法”（Arria-formula）会议的对话中，墨西哥驻联合国法律和制裁协调员帕布罗·阿罗查·奥拉布纳加（Pablo Arrocha Olabuenaga）指出，要确定法律确信，“通常，人们（法律顾问、律师和学者）会寻找政府发布的公开声明或推特。例如，如果一个国家对军事设施或恐怖组织进行攻击，很多时候都会在其外交部网页上发表声明或者推文，从而成为学术界获取材料以提出法律论据的来源”。[⑤]

上述这些例子表明，社交媒体帖子可以成为国家和国际法律工作者寻找单方法律行为和习惯国际法相关证据的信息来源。此外，各国越来越多地集中在推特这一平台发表大量公开声明，有助于信息的集中和大数据分析，提高国家和国际法律工作者识别、分析法律渊源的效率和能力。

但是使用社交媒体作为一种公开声明形式也具有一定的局限性，例如，社交媒体帖子基于字数限制而较为简短，可能无法充分解释或澄清声明的法律依据或含义；社交媒体帖子的非正式性可能无法反映其声明的严肃性，这可能会损害其作为国家实践或法律确信证据的可信度；社交媒体帖子在国家政府部门或官员个人账号

---

① See Erlend Serendahl, Unilateral Acts in the Age of Social Media, 5 Oslo Law Review 146 (2018).

② See Erlend Serendahl, Unilateral Acts in the Age of Social Media, 5 Oslo Law Review 126-146 (2018).

③ James A. Green, The Rise of Twiplomacy and the Making of Customary International Law on Social Media, 21 Chinese Journal of International Law 1-53 (2022).

④ See, e.g., Carrielyn D. Guymon (ed.), Digest of United States Practice in International Law 2018, https://2017-2021.state.gov/wp-content/uploads/2019/10/2018-Digest-Final-Draft.pdf, visited on 1 March 2023.

⑤ See Naz K. Modirzadeh & Pablo Arrocha Olabuenaga, A Conversation between Pablo Arrocha Olabuenaga and Naz Khatoon Modirzadeh on the Origins, Objectives, and Context of the 24 February 2021 Arria-formula Meeting Convened by Mexico, 8 Journal on the Use of Force and International Law 297 (2021).

发表的自发性可能不符合国家的官方立场或政策，或者存在黑客攻击，[①]从而影响帖子的真实性和权威性。此外，如何对待社交媒体平台的动态性和短暂性，如何避免选择性或扭曲使用帖子的偏见和操纵，都存在较大挑战。这些限制决定了社交媒体的帖子即使构成单方法律行为和习惯国际法的证据，也不可能与一份深思熟虑、精心起草的官方公报具有同等的证明价值。因此，在试图识别单方法律行为、国家实践或法律确信时，应谨慎使用社交媒体帖子并进行批判性分析。[②]

此外，数字技术对条约、一般法律原则、司法判例、公法学家学说等其他渊源的影响类似，它提高了国际法渊源的可及性和可见性，但是也对渊源的真实性、完整性、代表性和有效性提出了挑战。

总体而言，迈进数字时代，非国家行为体和数字技术使得网络空间国际造法在一定程度上呈现“国退民进”的态势，国际法渊源逐渐在社交媒体中兴起。一方面，非国家行为体深度参与国际造法，为网络空间国际规范的制定和解释做出了积极贡献，但同时也面临正当性危机，模糊了正式造法与非正式造法的界限，影响国家造法的表现，缺乏问责制、透明度和代表性。另一方面，国际法渊源在社交媒体的兴起并没有改变国际法渊源的构成要素，但是其呈现方式和识别方式发生了“数字化转型”，这使其可及性和可见性得到了提升，但是其真实性、完整性、代表性和有效性变得更加不确定。

三、国际法律关系和实体规则的“数字化转型”

国际法律关系是指国际法所调整的（主要是）国家间以法律权利和义务为形式的社会关系。国际法律关系的主体是具有独立参加国际关系并直接承受国际法上的权利和义务的能力的集合体——主要是国家，以及在一定条件下和在一定范围内类似国家的政治实体，如由国家组成的国际组织。[③]国际法实体规则是指直接规定（主要是）国家间权利义务内容的行为准则。国际法实体规则构成国际法律关系的重要组成部分，它决定了国际法律关系的性质、内容和效力。

（一）非国家行为体的网络行动对国家间法律关系的冲击

互联网的普及，使得非国家行为体（包括个人、黑客组织、犯罪集团或恐怖分子

① 例如，在2020年7月，130名知名推特用户的账号被黑客入侵，导致这些账号发出的推文并非出自账号持有人之手。虽然大多数账号持有人都是娱乐界的名人，但其中被黑的用户还包括巴拉克·奥巴马和乔·拜登。See Panagiotis Kyriakou, Cryptocurrency Theft, Scam and Other Misadventures: What Prospects for International Governance?,EJIL:Talk!, 24 July 2020, www.ejiltalk.org/cryptocurrency-theft-scam-and-other-misadventures-what-prospects-for-international-governance, visited on 1 March 2023.

② See James A. Green, The Rise of Twiplomacy and the Making of Customary International Law on Social Media, 21 Chinese Journal of International Law 36 (2022).

③ 参见孙国华主编：《中华法学大辞典（法理学卷）》，中国检察出版社1997年版，第208页。

等)能够轻松利用网络技术开展行动。事实上,已知的绝大多数网络攻击都是由各种非国家行为体发起的。[①]非国家行为体的网络行动侵蚀了国际公法一直以来以国家为中心的基础。传统上,非国家行为体的资源和能力与国家相去甚远,与国家的互动也较少,国际法将国家置于其法律制度的中心,专注于国家间的互动,即几乎在所有情况下都需要国家联系来确立国际不法行为或国际法律义务。但是在数字时代,非国家行为体的资源和能力可与国家相抗衡,与国家的互动也增多,以国家为中心的国际公法法律制度不足以应对与拥有“超级权力”的非国家行为体相关的网络行动带来的安全威胁。一方面,网络手段被广泛用于间谍活动、网络犯罪、破坏稳定甚至颠覆活动,而这些网络攻击本质上难以定性。另一方面,网络介质的内在特征、追踪和控制有关活动的困难性、非国家行为体日益增强的干预性,以及国家资助非国家行为体实施恶意行为的可能性,使得识别攻击的实施者和资助者变得尤为复杂。

按照传统国际法,主权、不干涉、使用武力等规则仅适用于国家间行为,非国家行为体的行为不构成对国家主权的侵犯,不构成干涉或使用武力,除非这些行为可归于国家,即能证明非国家行为体的网络活动接受了国家的指示,或者受到国家的指挥或控制,又或者在极为例外的情况下,国家承认并接受私人活动为国家行为。[②]例如,一家公司以黑客方式反击国家(攻击国)的恶意网络行动,或者由恐怖组织对一国(受攻击国)实施的、无法归于他国的网络行动,都不构成对攻击国或受攻击国主权的侵犯。[③]但是这类非国家行为体的恶意网络行动可能会对国家中心主义造成冲击,因为无论它们是单纯的个人行为,还是出于相关国家的授意等原因可归于国家,受害国都难以通过国际法律责任实现权利救济,主要原因在于:一方面,目前国际法律责任制度没有直接规制个人网络行动;另一方面,试图将个人网络行动归于国家以追究国家不法行为责任,也面临一系列技术、政治和法律难题。[④]就后者而言,其一,在技术层面,网络攻击通常具有高度的隐秘性和瞬时性,导致受害国收集证据和识别攻击者身份十分困难。其二,在政治层面,由于公开归因会暴露应对国自身的网络能力(如拦截和检测方法、进攻和防御能力),美国、英国、德国、荷兰、瑞士、加拿大等大多数国家明确表示,归因是一国的政治决定,属于主权性事项,没有法律义务要求一国公开披露其对恶意网络活动进行归因所依据的基本信息,或对所

① See Eric Jensen, Computer Attacks on Critical National Infrastructure: A Use of Force Invoking the Right of Self-Defense, 38 Stanford Journal of International Law 207, 232-234 (2002).

② 参见《国家对国际不法行为的责任条款草案》第8条、第11条。

③ 参见[美]迈克尔·施密特主编:《网络行动国际法塔林手册2.0版》,黄志雄等译,社会科学文献出版社2017年版,第62-63页。

④ 参见张华:《论非国家行为体之网络攻击的国际法律责任问题——基于审慎原则的分析》,《法学评论》2019年第5期,第160-163页。

有情况下遭受的恶意网络活动进行公开归因。[①]其三，在法律层面，由于绝大多数网络攻击都是由非国家行为体（包括个人和黑客组织等）发起的，它们与特定国家间的法律联系往往难以确定，例如，国家对非国家行为体的控制标准以及证据标准等问题尚不明确。[②]

基于此，大多数国家和学者逐渐将审慎原则作为处理非国家行为体恶意网络行动的责任转嫁途径，即要求国家努力确保其领土或处于其政府控制下的领土或网络基础设施不被非国家行为体用来实施此类行动。目前已经发表立场声明的国家基本都赞成审慎原则适用于网络空间，但是关于网络空间审慎原则的内涵、性质、适用条件和具体义务，仍存在较大争议。此外，有学者认为将源于一国境内的网络攻击责任直接转嫁给该国的归责方式冲击了当前网络治理对于国家权利义务规则设定的“领土界限”，扩大了国家在网络中承担责任的范围，混淆了不同行为体在网络空间中的权利义务，因此有必要将其界定为一种补充或次要责任。[③]

现有国际法仅在少数领域内的个别情况下规制非国家行为体的网络行动（例如国际人权法、国际人道法以及国际刑法），但现实是，非国家行为体的网络活动时常发生，产生了与其地位不相称的巨大影响，不仅损害了目标国的安全和利益，而且归因难题容易产生误判甚至陷害，[④]进而在国家之间引发不必要的指责、冲突和对抗。即使试图将关于主权、国家责任和诉诸武力等相关规则适用于涉及非国家行为体的网络行动，也存在诸多不确定性和逻辑矛盾。总体而言，非国家行为体网络攻击的不对称性、归因难题以及规则真空，都对国家中心主义造成巨大冲击，[⑤]未来国际法可能不得不更多地关注非国家行为体在国际法中的地位、权利义务与责

① See UN Doc. A/76/136, 13 July 2021.

② 参见黄志雄：《论网络攻击在国际法上的归因》，《环球法律评论》2014年第5期；朱玲玲：《从〈塔林手册2.0版〉看网络攻击中国家责任归因的演绎和发展》，《当代法学》2019年第1期；张华：《论非国家行为体之网络攻击的国际法律责任问题——基于审慎原则的分析》，《法学评论》2019年第5期；张华：《网络空间适用自卫权的法律不确定性与中国立场表达——基于新近各国立场文件的思考》，《云南社会科学》2021年第6期。

③ 参见朱玲玲：《从〈塔林手册2.0版〉看网络攻击中国家责任归因的演绎与发展》，《当代法学》2019年第1期，第72页。

④ 比如，在美国政府和媒体的叙事中，中国政府是大量幕后攻击的主导者，即使对于不可归因于国家的黑客攻击，美方会倾向于认为中国就是攻击的源头——而不是中国电脑被捕获——然后采取反击或反制。甚至有人会利用这种心理，为了隐藏身份或故意挑拨，专门捕获中国的电脑发起攻击。在针对爱沙尼亚的网络攻击中，欧洲、中国和美国的电脑都被捕获用于进攻，而黑客留下了许多指向北京的“痕迹”。参见左亦鲁：《国家安全视域下的网络安全——从攻守平衡的角度切入》，《华东政法大学学报》2018年第1期，第152页。

⑤ See Michael N. Schmitt & Sean Watts, Beyond State-Centrism: International Law and Non-state Actors in Cyberspace, 21 Journal of Conflict & Security Law 595-611 (2016).

任。[①]

(二)国际法实体规则的内涵重塑和转型升级

网络化、数字化、智能化与人类生产生活各个领域的深度融合,网络空间与物理世界相比有着多方面的新颖性(如互联互通、匿名性等)。尽管国际社会对现有国际法的可适用性形成了一定共识,但关于相关实体规则的存在性问题,如网络空间是否存在审慎、主权等国际法规则或原则,网络空间主权原则是否具有约束力;解释性问题,如不干涉与“强制”要件、数据与作为国际人道法下受保护的“物体”、非物理影响与使用武力/武装攻击等,[②]都存在较大分歧。为适应数字时代的发展特性,一大批针对物理空间存在的现有国际法规则需要进行内涵重塑和转型升级。

例如,关于网络空间主权的讨论,既涉及存在性问题,也关涉解释性问题。网络空间主权属于原则还是规则,就是存在性问题,关系到规则约束力是否存在的问题。2017年以来,国际上出现了一场有关网络空间主权原则义务属性的大辩论,对于主权原则在网络空间的适用已经并将持续产生深远影响。大体而言,这一辩论的“反方”即否定论者尽管并不否定网络空间主权原则的存在,但却否定它本身构成一项可以约束国家网络行为、产生国际法律责任的国际法义务,英国[③]、美国[④]等少数国家政府和学者[⑤]支持这一主张。相反,辩论的“正方”即肯定论者则主张,主权既是国家间交往的基本原则,也是具有约束力的国际法规

---

① 有学者认为,“未来国际网络法规则的设计应以国家主权为根茎,以个案解决为枝叶,以多层次规则为拓展倡导国际社会共同应对网络攻击中的责任归因问题,增加对个人或团体等非国家行为体权利、义务与责任的考量”,可以参考跨界损害的国际责任认定中的类似设计。参见朱玲玲:《从〈塔林手册2.0版〉看网络攻击中国家责任归因的演绎与发展》,《当代法学》2019年第1期,第78页。也有西方学者建议直接为非国家行为体设置与网络行动相关的国际法律责任制度。See Nicholas Tsagourias, Non-Stators, Ungoverned Spaces and International Responsibility for Cyber Acts, 21 Journal of Conflict & Security Law 467-472 (2016).

② 存在性问题是指识别特定规则是否存在和有效,涉及找法的过程;解释性问题是解释特定规则的含义,关乎释法的过程。不过,存在性问题和解释性问题都属于广义上的国际法解释,二者之间的界限可能并不总是清晰的,在实际解释适用时通常是一起处理的。See Duncan B. Hollis, The Existential Function of Interpretation in International Law, in Andrea Bianchi, *et al.* (eds.), Interpretation in International Law 78-110 (Oxford University Press 2015).

③ See Jeremy Wright, Cyber and International Law in the 21st Century, 23 May 2018, https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century, visited on 1 March 2023; UN Doc. A/76/136, 13 July 2021.

④ See Paul C. Ney, DOD General Counsel Remarks at U.S. Cyber Command Legal Conference, 2 March 2020, https://www.defense.gov/News/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/, visited on 1 March 2023.

⑤ See Gary P. Corn & Robert Taylor, Sovereignty in the Age of Cyber, 111 American Journal of International Law 207, 208 (2017).

则，特定网络行动可以构成对他国主权的侵犯。奥地利[①]、巴西[②]、加拿大[③]、捷克[④]、爱沙尼亚[⑤]、伊朗[⑥]、芬兰[⑦]、德国[⑧]等国家政府以及以《塔林手册2.0版》主编迈克尔·施密特为代表的多数学者[⑨]都支持这一主张。

在具体内涵的解释性问题上，持网络空间主权义务属性肯定论的若干国家对于侵犯主权的门槛存在不同认识：一种代表性观点认为侵入他国网络且应达到特定门槛、造成特定后果才构成侵犯主权；另一种观点则主张任何未经授权的侵入他国的网络行动都可能构成侵犯主权。就前者而言，不同国家、学者对于侵犯主权需要达到何种特定门槛、造成何种特定后果（如未经许可入侵他国网络系统、窃取数据、造成网络设施的物理损害或人员伤亡等）仍存在多种不同的理解。[⑩]就后者而言，中国政府2022年向OEWG提交的《中方关于网络主权的立场》文件指出："如果一国未经许可侵犯他国基于国家主权对其境内的网络设施、网络主体、网络行为及相关网络数据和信息等享有的对内最高权和对外独立权，包括未经许可入侵他国领土或管辖范围内的网络系统，或对有关网络基础设施造成损害或破坏，或未经许可损害一国

① See Austria, Pre-Draft Report of the OEWG - ICT: Comments by Austria, 31 March 2020, https://front.un-arm.org/wp-content/uploads/2020/04/comments-by-austria.pdf, visited on 1 March 2023.

② See UN Doc. A/76/136, 13 July 2021, p.18.

③ See Government of Canada, International Law Applicable in Cyberspace, https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx?lang=eng, visited on 1 March 2023.

④ See Czech Republic, Statement by Mr. Richard Kadlčák, Special Envoy for Cyberspace, 2nd Substantive Session of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, 11 February 2020, https://www.nukib.cz/download/publications_en/CZ%20Statement%20-%20OEWG%20-%20International%20Law%2011.02.2020.pdf, visited on 1 March 2023.

⑤ See UN Doc. A/76/136, 13 July 2021, p. 25.

⑥ See Iran, Declaration of General Staff of the Armed Forces of the Islamic Republic of Iran Regarding International Law Applicable to the Cyberspace, July 2020, https://nournews.ir/En/News/53144/General-Staff-of-Iranian-Armed-Forces-Warns-of-Tough-Reaction-to-Any-Cyber-Threat, visited on 1 March 2023.

⑦ See Finland, International Law and Cyberspace: Finland's National Positions, 15 October 2020, https://um.fi/documents/35732/0/KyberkannatPDF_EN.pdf/12bbbbde-623b-9f86-b254-07d5af3c6d85?t=1603097522727, visited on 1 March 2023.

⑧ See Germany, On the Application of International Law in Cyberspace: Position Paper, March 2021, p.3, https://www.auswaertiges-amt.de/blob/2446304/2ae17233b62966a4b7f16d50ca3c6802/on-the-application-of-international-law-in-cyberspace-data.pdf, visited on 1 March 2023.

⑨ See Michael N. Schmitt, "Virtual" Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law, 19 Chicago Journal of International Law 30-40 (2018)；[美]迈克尔·施密特主编：《网络行动国际法塔林手册2.0版》，黄志雄等译，社会科学文献出版社2017年版，第62-63页。

⑩ See Michael N. Schmitt & Liis Vihul, Respect for Sovereignty in Cyberspace, 95 Texas Law Review 1639-1671 (2017) ; Harriet Moynihan, The Application of International Law to State Cyberattacks: Sovereignty and Non-Intervention, Chatham House, 2 December 2019, para.60, https://www.chathamhouse.org/2019/12/application-international-law-state-cyberattacks, visited on 1 March 2023.

在网络空间的排他性主权权利，都违反了主权原则，构成国际不法行为。”[①]法国等一些国家也持类似主张。这些不同的观点，反映了不同国家、非国家行为体在数字时代的价值偏好和发展需求不同，也是现有国际法规则在“技术适应”过程中的一大难题。

再如，传统上，一国对另一国施加的影响需要达到比较严格的“强制”（coercion）门槛（对他国选择自由的剥夺），才构成对不干涉原则的违反。[②]然而，信息和网络时代的到来，为国家通过网络手段影响乃至干涉别国内部事务提供了巨大便利。西方国家出于主导网络空间不干涉原则话语权、维护自身利益的需要，意图弱化甚至放弃“强制”要件。2017年，时任美国国务院法律顾问布莱恩·伊根（Brian Egan）在演讲中指出“干涉选举将明显构成对不干涉内政原则的违反”，但并未对“强制”要件的问题进行解释，试图绕过“强制”要件。2022年，英国总检察长苏拉·布雷弗曼（Suella Braverman）在演讲中明确：强制的实质是剥夺控制自由（freedom of control），而非选择自由（freedom of choice），譬如，一个国家的能源供应设施或者医疗设施遭受了网络攻击的侵害导致无法正常运行的情形满足“强制”的要件，属于不干涉内政原则规制的范畴。[③]为了适应网络技术的飞速发展，以及大多数网络行动极具干扰性而不具有强制性的情况，一些学者也主张重塑“强制”要件，例如，Ido Kilovaty认为，网络空间不干涉内政原则违反与否的认定不应再考量“强制”要件；[④]而Thibault Moulin则认为，“强制”要件的标准应降低为“剥夺控制”标准。[⑤]

此外，还有一些传统国际法规则在适用于网络空间时出现“失灵”情况，需要重新塑造和转型升级。例如，国际法院在1986年尼加拉瓜诉美国在尼加拉瓜境内及针对尼加拉瓜的军事及准军事行动案中提出，应当根据一项军事行动的规模和后果来判断行动是否构成对他国的“武力攻击”，这一标准被认为是一项习惯国际法规则。但是，脱离传统军事行动这一特定语境，将“规模和后果”标准套用到网络攻击上，可能会得出偏颇和似是而非的结论。[⑥]同样，网络空间的互联互通性及其数字化

---

① 《中方关于网络主权的立场》，https://meetings.unoda.org/section/oewg-ict-2021_documents_14473_documents_16363/，2022年12月1日访问。

② See Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. US), Judgment, ICJ Reports 1986, para.205.

③ See Attorney General Suella Braverman, International Law in Future Frontiers, 19 May 2022, https://www.gov.uk/government/speeches/international-law-in-future-frontiers,visited on 1 March 2023.

④ See Ido Kilovaty, Doxfare: Politically Motivated Leaks and the Future of the Norm on Non-Intervention in the Era of Weaponized Information, 9 Harvard National Security Journal 146-179 (2018).

⑤ See Thibault Moulin, Reviving the Principle of Non-Intervention in Cyberspace: The Path Forward, 25 Journal of Conflict & Security Law 423-447 (2020).

⑥ 参见黄志雄：《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9-11页。

特征为解释国际人道法有关敌对行动的主要原则和概念带来了挑战，例如，大多数网络攻击都难以区分军事目标和民用目标，也难以控制攻击的范围和程度。重要民用数据是数字化社会的重要组成部分，其中包括医疗数据、生物测定数据、社保数据、税务记录、银行账户、公司客户档案或选举名单和记录等。删除或篡改重要民用数据可迅速导致政府服务和私营企业完全陷入瘫痪，对平民所造成的伤害远远超出对实际物体造成的损坏。民用数据是否以及在何种程度上构成“民用物体”仍是一个有待解决的问题。《塔林手册2.0版》国际专家组的多数意见认为，数据的无形性质使其不符合国际人道法中“物体”的通常意义，[①]但是，红十字国际委员会认为，在这个高度依赖数据的时代，国际人道法不禁止删除或篡改此类重要民用数据的主张似乎难以与国际人道法的目的和宗旨相一致。[②]一些学者也从国际人道法的设立目的出发，认为应该防止过度军事化并最大限度地保护平民利益，条约和习惯中有关国际人道法确定战斗员身份的要素（包括关于“物体”的现行规定）并不适用于数字领域，甚至主张通过条约或习惯发展新规则。[③]

当然，除了传统国际法在网络空间中的适用性和有效性问题，数字时代还为国际法带来了许多新领域和新议题，例如，在跨境数据流动与个人数据隐私保护领域，如何确保在跨境收集、处理、存储和传输个人数据时尊重人权和基本自由，以及如何在数字经济中平衡个人、国家和私人行为体的利益；在数字贸易和电子商务规制领域，如何促进软件、云计算或在线平台等数字商品和服务的跨境流动，以及如何应对税收、知识产权、消费者保护和数字市场竞争方面的挑战；在人工智能和新兴技术监管领域，如何规范对社会产生重大影响的新技术（如人工智能、生物技术、纳米技术或区块链）的开发和部署，以及如何规避潜在的伦理风险。

这些新问题原则上可以通过发展国际法新规则来解决，以人工智能的规制为例，澄清人工智能行为体的法律地位，为人工智能治理建立新的规范和标准，或规范人工智能出于各种目的的使用和发展。然而，由于某些人工智能系统的自主性、不透明性和不可预测性，法律发展可能存在法律不确定性、范围不匹配和法律过时等

① 参见[美]迈克尔·施密特主编：《网络行动国际法塔林手册2.0版》，黄志雄等译，社会科学文献出版社2017年版，第426页。

② See ICRC, International Humanitarian Law and Cyber Operations During Armed Conflict, 28 November 2019, https://www.icrc.org/en/document/international-humanitarian-law-and-cyber-operations-during-arm-ed-conflicts, visited on 1 March 2023.

③ See Michael N Schmitt, Cybersecurity and International Law, in Robin Geiβ & Nils Melzer (eds.), The Oxford Handbook of the International Law of Global Security 667 (Oxford University Press 2021); Zhixiong Huang &Yaohui Ying, The Application of the Principle of Distinction in the Cyber Context: A Chinese Perspective, 102 International Review of the Red Cross 363-365 (2020); Kubo Mačák, Military Objectives 2.0: the Case for Interpreting Computer Data as Objects under International Humanitarian Law, 48 Israel Law Review 55-80 (2015) .

实际困难。[①]这些困难突出了为监管人工智能制定有效法律框架的挑战,并强调了政策制定者、技术专家和其他利益攸关者之间持续对话与合作的必要性。

总体而言,非国家行为体网络行动的大量增加冲击着国家间法律关系,数字技术与物理世界的深度融合导致了国际法实体规则的内涵重塑和转型升级。

四、国际法实施层面的“数字化转型”

“国际法的实施可以被视为国际法效力得以实现的一个过程,包括国际法规则的遵守和执行、国际法上权利义务的适用等问题,涉及实施主体、实施规则和实施机制等多个方面,在实践中呈现出多样性、不确定性的特点。”[②]一般情况下,国家在国际、国内两个层面对其承诺的国际义务的自我遵守是国际法的主要实施形式。但是,国家的自我遵守并非国际法唯一的或全部的实施方式,还有国际社会的谴责、国家的报复(reprisals)和反报(retorsion)等自助行为,以及用和平或武力办法解决国家间争端等多种方式。鉴于国家间自发的、松散的传统实施机制无法确保国际法的有效实施,国际组织通过国际多边合作的制度性安排,去敦促、协助和监督成员国履行其国际义务、实施国际法,解决成员国之间因实施国际法而产生的争端,并对成员国严重违反国际法的行为采取组织措施等,形成监测核查、争端解决、制裁惩罚等一系列机制。通过国际组织促进国际法的实施,本质上是对国家实施国际法的一种必要补充,是国际法实施的一种辅助机制,与国家的主体作用一起构成国际法实施的完整机制。[③]

传统上,国际法通过外交压力、谈判、调解、仲裁、裁决、制裁等多种机制得以遵守和实施。然而,这些机制可能并不总是有效或足以阻止或应对违反国际法的行为,特别是在网络空间的背景下,归因、管辖权和合作[④]面临一系列挑战,从而限制这些实施机制的开展。不过,数字技术可以为国际法的实施提供新的工具和方案,正如《数字白皮书》所说的,“法律也可以在证据领域……以及电子司法或法律技术领域运用新技术”,[⑤]尤其是人工智能的使用。

---

① See Matthijs M. Maas, International Law Does Not Compute: Artificial Intelligence and the Development, Displacement or Destruction of the Global Legal Order, 20 Melbourne Journal of International Law 10-15 (2019).

② 饶戈平主编:《国际组织与国际法实施机制的发展》,北京大学出版社2013年版,第1页。

③ 参见饶戈平主编:《国际组织与国际法实施机制的发展》,北京大学出版社2013年版,第1-13页。

④ 网络活动对合理、公平地行使管辖权提出了许多挑战。这主要是因为网络活动具有跨国性,可能迅速影响多个国家,这导致任何国家都试图对特定网络活动主张不同类型的管辖权,从而引发国家间的管辖冲突。因此,就网络活动而言,实施方面的国际合作显得尤为重要。参见[美]迈克尔·施密特主编:《网络行动国际法塔林手册2.0版》,黄志雄等译,社会科学文献出版社2017年版,第94-95页。

⑤ See White Paper 16: Digital Challenges for International Law, p. 86, https://www.ilaparis2023.org/wp-content/uploads/2022/08/Numerique-VHD-EN.pdf, visited on 10 October 2022.

就国际组织的监督性实施机制而言，数字技术可以被用来收集、分析、验证和报告有关国家或国际组织是否遵守国际法规则的数据和信息，大大提高监测和核查的效率、准确性、透明度和可信度，并增加监测和核查的范围、深度和多样性。原子能机构保障外联协调官员Carrie Mathews表示，“人工智能、机器人技术以及辐射探测和卫星图像领域的技术进步，已开始对国际保障的执行产生积极的影响……技术进步使视察员能够更好地利用他们在现场的时间，专注于视察，而不是编写报告或执行其他重复性任务”，提高了原子能机构核查的有效性和效率。[①]原子能机构最新运用的人工智能和机器学习，可以将日常流程自动化，支持人为决策，以及通过识别错误确保数据的质量和真实性，从而使分析员和视察员专注于最高价值的活动。此外，人工智能和机器学习不仅能够监视数据审查，还能加强对多个信息源的收集、整合和分析。借助人工智能，关于设施设计和核材料衡算的国家申报信息、视察期间收集的信息以及与保障相关的开源信息可以得到更高效的分析。人工智能还可以检测和应对信息安全事件。原子能机构使用集成了人工智能的商用工具来应对网络威胁、设备篡改以及对敏感信息进行认证和加密。随着核技术的进步，保障技术也在不断发展。新技术的发展即将到来，原子能机构正在积极探索创新型技术如何助力其核查任务。[②]

然而，对网络空间违反国际法行为的核查往往是困难的，因为网络技术可能被用来隐藏网络攻击发起者的身份，造成技术上的归因难题，同时政治性因素也影响到国家公开归因的积极性。当政府主导公开归因不能提供或者不方便提供足够详细的证据时，国家可能会选择与其他政府合作，以多个国家的信用作为背书，借此弥补证据的不足，为其网络事件的责任认定提供更大的政治影响力和可信度。例如，2017年，恶意软件NotPetya在对乌克兰发起攻击后在世界各地传播，感染了欧洲、亚洲和美洲的公司和政府，造成了数十亿美元的损失。英国、美国、丹麦、澳大利亚、加拿大和新西兰政府在一周之内都发表了归因声明，一致将NotPetya归咎于俄罗斯政府。虽然这种集体公开归因可以强化责任认定的效果，但是它仍然是国家根据政治需要而做出的策略选择。[③]为了客观公正、透明有效地开展网络归因调查，进一步提高归因的可信度，兰德公司提供了一个无政府归因的“全球网络归因联盟”方案，由国际专家组成的团队对重大网络事件进行独立调查和归因。成员包括来自网络安

① See Jennifer Wagman & Teodor Nicula-Golovei, The Evolution of Safeguards Technology, IAEA, https://www.iaea.org/bulletin/the-evolution-of-safeguards-technology, visited on 1 March 2023.

② See Jennifer Wagman & Teodor Nicula-Golovei, The Evolution of Safeguards Technology, IAEA, https://www.iaea.org/bulletin/the-evolution-of-safeguards-technology, visited on 1 March 2023.

③ See Ariel E. Levite, *et al.,* Managing U.S.-China Tensions Over Public Cyber Attribution, https://carnegieendowment.org/2022/03/28/managing-u.s.-china-tensions-over-public-cyber-attribution-pub-86693, visited on 1 March 2023.

全和信息技术公司以及学术界的技术专家，以及来自不同学术界和研究组织的网络空间政策专家、法律学者和国际政策专家。[①]总体而言，无论是国家集体归因还是联盟归因，一般都是为了发挥组织团体的集体力量，敦促、协助和监督国家履行其国际义务、实施国际法。

从人工智能对国家自身实施国际法来看，也是机遇与挑战并存。在条约谈判中，各国可以使用机器学习或计算文本分析来识别其谈判伙伴向联合国大会所作的大量发言模式，并据此形成其谈判立场。此外，各国可以利用人工智能工具，通过更快速、更彻底地处理有关仲裁员的信息，或通过揭示仲裁或司法裁决中的潜在模式，来改进争端解决方式。人工智能工具还可以帮助各国执行国际法。例如，国家可以开发和部署传感器来检测违反武器条约的行为，并使用人工智能来监控这些传感器。[②]

再如，为了更好地履行国际人道法义务，红十字国际委员会于2022年11月3日发布题为《红十字、红新月和红水晶标志数字化：益处、风险和可能的解决方案》（Digitalizing the Red Cross, Red Crescent and Red Crystal Emblems: Benefits, Risks, and Possible Solutions）的报告，[③]开展红十字、红新月和红水晶标志数字化的探索和示范，也是结合数字技术为加强数字时代国际人道法实施和遵守“赋能”的一个例证。国际人道法的主要原则之一是区分战斗人员和平民以及军事和民用物体。这一原则要求冲突各方不得以平民或民用物体为目标，同时必须采取一切可行的预防措施，避免或尽量减少对平民或民用物体的伤害。为了便于区分，国际人道法规定使用特殊标志，如红十字、红新月和红水晶标志，以表明某些人或物体受国际人道法保护，不得受到攻击。这些标志用于医务人员、设施和车辆，以及红十字国际委员会和红十字与红新月运动等人道主义组织。然而，在数字时代，武装冲突越来越多地涉及网络行动，如网络攻击、网络间谍、网络战等，这些行动可能影响或针对数字系统和数据。这些网络行动可能对保护物理世界中具有独特标志的人和物构成新的挑战和风险。例如，网络行动可能破坏或干扰医疗设备或设施的功能，可能危及或暴露医务人员或患者的敏感数据；它们可能在受保护人员或物体的位置或身份方面误导或混淆冲突各方；它们甚至可能对带有特殊标志的人或物体造成人身损害或伤害。为了应对这些挑战和风险，红十字国际委员会开展了红十字、红新月和红水晶标志数字化的探索和示范，目的是开发用于网络领域的“数字标志”，以表明

① See John S. Davis II, *et al.,* Stateless Attribution: Toward International Accountability in Cyberspace, https://www.rand.org/pubs/research_reports/RR2081.html, visited on 1 March 2023.

② See Wolfgang Alschner, Chapter 13: The Computational Analysis of International Law, in Rossana Deplano & Nicholas Tsagourias (eds.), Research Methods in International Law: A Handbook 203-204 (Edward Elgar Publishing Limited 2021).

③ See ICRC, Digitalizing the Red Cross, Red Crescent and Red Crystal Emblems: Benefits, Risks, and Possible Solutions, https://www.icrc.org/en/document/icrc-digital-emblems-report, visited on 1 March 2023.

某些数字系统或数据受到国际人道法的保护，不得受到攻击，进而加强数字时代国际人道法的实施和遵守。此外，红十字国际委员会还与瑞士数据科学中心开展合作项目，利用人工智能来发现并追踪武装部队和武装团体的暴力模式，为人道主义工作提供技术解决方案。①

然而，人工智能对国际法体系及其实施的影响也可能是负面的。人工智能在不友好或敌对国家行为中的应用可能带来一系列挑战，包括如何归因、确定合法性以及援引所涉不同行为体的责任等方面，都存在较大的不确定性，国际社会也尚未达成普遍认识。这些困难尤其影响到国际法的两个分支：国际人权法和国际人道法。在国际人权法方面，主要挑战包括确定脸部识别软件对人权的影响、算法中的歧视性偏见、使用人工智能造成的侵犯人权行为的归因和责任。从国际人道法的角度来看，在规制某些作战手段和方法以及评估武器的技术演变及其法律后果方面存在着挑战。在开发和使用人工智能技术过程中，国家与非国家行为体之间可能存在的牵连关系也加剧了这些挑战。在决策过程中以及在自主系统中采用不同行为体开发的人工智能解决方案，可能会引发与归因和个人责任相关的问题，特别是关于指挥官责任和个人刑事责任。即使在并不存在不法行为的情形下，非国家行为体和国家所进行的相互交织的活动，也可能引发有关问责以及如何补救人工智能技术造成的伤害等问题。②

除了学界和国家间进程讨论最多的致命性自主武器系统及其他人工智能在国际人道法和国际人权法具体领域的制定与实施的挑战外，有学者创新性地提出，人工智能能力的部署可能在一定程度上导致全球法律体系的衰落，因为人工智能系统逐渐改变了环境、激励机制，甚至是国家的价值观。无论一个国家以前通过参与或遵守国际法获得了什么利益（包括安全、国内合法性、软实力或合作），如果它现在认为（无论正确与否）它可以通过应用人工智能单方面实现这些目标，③这可能会削弱国际法的更广泛的合法性和规制能力。

因此，总体而言，包括人工智能在内的数字技术既可以促进也可以阻碍国际法

---

① See Fiona Terry & Fabien Dany, Harnessing the Power of Artificial Intelligence to Uncover Patterns of Violence, https://blogs.icrc.org/law-and-policy/2023/05/25/artificial-intelligence-patterns-violence/?_hsmi=260688067&_hsenc=p2ANqtz-_4c2b2WhbtphgCP_8rAOZAhv184YBZ9Lc-uflbLzE4txdhsJgekxPg8W4967rVRmgxIFOp1XQMRUA0_O2iPdBgPgOuiA, visited on 26 May 2023.

② See White Paper 16: Digital Challenges for International Law, pp. 96-98, https://www.ilaparis2023.org/wp-content/uploads/2022/08/Numerique-VHD-EN.pdf, visited on 10 October 2022.

③ 例如，政府可能会倾向于（或许也有理由）相信，在不久的将来，它们可能能够通过人工智能监控能力实现内部安全，通过计算的宣传（computational propaganda）而非通过公开遵守人权规范实现国内合法性，或者通过对其他国家谈判策略的预测建模而不是相互接触和妥协实现全球软实力。See Matthijs M. Maas, International Law Does Not Compute: Artificial Intelligence and the Development, Displacement or Destruction of the Global Legal Order, 20 Melbourne Journal of International Law 28 (2019).

的实施和遵守。它需要各国在使用数字技术时保持谨慎和负责的态度,坚定维护国际法的原则和价值,促进国际社会的合作与发展。

五、结语

迈进数字时代,现代国际法在国际造法和渊源、国际法律关系和实体规则以及实施层面都面临着全方位转型升级的需要,既有机遇也有挑战。这种转型升级整体上是由非国家行为体和数字技术共同作用的结果。同时,应当注意到,对于在国际法领域增加数字技术的使用所引起的一个关切是,它可能在使用有关技术的国家与不使用(或至少不广泛使用)技术的国家之间造成不平等。[①]例如,根据《世界互联网发展报告2022》,在互联网发展情况排名前十位的国家中,除中国外,均为发达国家。[②]互联网等技术上的“数字鸿沟”会造成并进一步加深国家与相关非国家行为体在认识、塑造和实施国际法等方面的“数字鸿沟”。一个持久的国际法治,它必须反映整个国际社会的利益。[③]因此,弥合数字鸿沟,共促数字时代国际法的“良法善治”,是国际社会全体成员的共同目标和长远之计,也只有弥合数字鸿沟,才能更好地回应国际法的“数字化转型”需求。

The “Digital Transformation” of International Law: Comments on the White Paper on Digital Challenges for International Law

Abstract: Stepping into the digital age, a large number of new digital fields and issues have brought new challenges to international law. The French branch of the International Law Association has released a white paper entitled “Digital Challenges for International Law”, proposing three major challenges of blurring lines between public and private actors, the politics of debates on international law in cyberspace and the digital divide, as well as some questions worthy of further debate and research, providing a useful reference for thinking about the trend of international law in the digital age. In essence, in order to adapt to the

① See Ashley Deeks, High-Tech International Law, 88 George Washington Law Review 684 (2020).

② 报告对全球48个国家和地区的互联网发展情况进行了评估,排名前十的国家分别为美国、中国、德国、瑞典、荷兰、韩国、英国、加拿大、芬兰、丹麦。参见中央网信办:《〈中国互联网发展报告2022〉和〈世界互联网发展报告2022〉蓝皮书发布》,http://www.cac.gov.cn/2022-11/09/c_1669622017232374.htm,2023年4月18日访问。

③ Brian Tamanaha, On the Rule of Law: History, Politics, Theory 136 (Cambridge University Press 2004).

development of digital technology as well as the rise of the function and status of non-state actors, modern international law is faced with the need of all-round transformation and upgrading in terms of international lawmaking and sources of international law, international legal relations, substantive rules, implementation and compliance, which are mainly manifested as: to some extent, international law-making of cyberspace presents the trend of "the state retreats and the people advance", the source of international law are gradually emerging in social media; the cyber operations of non-state actors are impacting the legal relations between states, the substantive rules of international law are facing the connotation reshaping, transformation and upgrading; and digital technology provides new tools and schemes for the implementation of international law. Overall, the transformation and upgrading of international law in the digital age entail both opportunities and challenges, which need to be treated with caution.

Key words: international law; digital age; non-state actors; international law-making; sources of international law; implementation of international law

（责任编辑：石磊）