论网络空间中的禁止使用武力原则

王玫黎　陈　雨*

摘　要：与网络空间有关的国际法问题日益受到学者关注，其热点问题包括在网络空间视角下对禁止使用武力原则的重新认识。当前，大多数西方学者偏重关注如何扩大诉诸武力权的范围，并以推动国际社会对诉诸武力权进行扩大化解释为导向。这与中国反对网络空间军备竞赛并积极推动建设网络空间命运共同体的态度形成鲜明对比。因此，中国有必要在充分利用联合国平台的基础上，围绕以《联合国宪章》为核心的国际法基本原则，提出对网络空间视角下诉诸武力权和战时法的中国立场，并积极应对西方的错误认识，掌握网络空间秩序制定的主导权。

关键词：网络空间　网络攻击　网络战　禁止使用武力

网络空间是全球治理和国际规则制定的新兴领域，中国政府历来高度重视对网络空间国际法治的推动。习近平总书记指出，中国应当提升对网络空间的国际话语权和规则制定权，[①] 这表明，中国在新时代必将以更加主动的姿态参与到国际网络空间治理进程中去。[②]

当前，这个新领域存在大量亟待学者阐释的概念和机制，纵览学界主要研究成果，中西方学者对某些议题实际上达成了某种程度的共识，譬如，黄志雄、朱雁新、李伯军、朱莉欣均强调了传统战争法规则可以在网络武装冲突中得到适用。[③] 以迈克尔·施密特为代表的西方学界也强调了传统战争法规则适用于网络空间的必要性。[④] 但是，传统战争法规则（尤其是禁止使用武力原则）是否以及如何在网络空间具有可适用性？中西方学者的观点有明显差异，具体集中在：第

---

* 王玫黎，西南政法大学国际法学院教授，博士生导师，西南政法大学海外利益保护研究中心执行主任。陈雨，西南政法大学海外利益保护研究中心助理研究员。本文系重庆市教委项目《人工智能对国际法的挑战与应对》（项目编号：19SKGH016）的阶段性成果。

① 《习近平：加快推进网络信息技术自主创新 朝着建设网络强国目标不懈努力》，新华网，http://www.xinhuanet.com//politics/2016-10/09/c_1119682204.htm，最后访问时间：2019年2月1日。

② 《习近平：敏锐抓住历史机遇 加快建设网络强国——在全国网络安全和信息化工作会议上的重要讲话》，人民网，http://politics.people.com.cn/n1/2018/0423/c1024-29942146.html，最后访问时间：2019年1月5日。

③ 参见黄志雄：《网络空间负责任国家行为规范：源起、影响和应对》，载《当代法学》2019年第1期；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》，载《厦门大学学报（哲学社会科学版）》2018年第1期；黄志雄：《国际法视角下的“网络战”及中国的对策——以诉诸武力权为中心》，载《现代法学》2015年第5期；朱雁新：《试析武装冲突法的适用条件——“武装冲突”》，载《西安政治学院学报》2011年第6期；李伯军：《论网络战及战争法的适用问题》，载《法学评论》2013年第4期；朱莉欣：《〈塔林网络战国际法手册〉的网络主权观评介》，载《河北法学》2014年第10期。

④ See Michael N. Schmitt, “Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework”, (1999) 37 *Columbia Journal of Transnational Law* 885, p. 890; Michael N. Schmitt, “Cyber Operations and the Jus Ad Bellum”, (2011) 56 *Villanova Law Review* 569, p. 573.

一，网络空间中各专有名词的内涵尚不统一；[①] 第二，论证可适用性之根本目的大相径庭；[②] 第三，对网络空间中传统战争法规则的理解莫衷一是。[③] 本文拟对上述三个问题进行总结和回应，进而推动禁止使用武力原则在网络空间的贯彻，并为理解网络空间中的传统战争法规则提供中国思路。

一　禁止使用武力原则在网络空间的可适用性

《联合国宪章》第2条第4项规定："各会员国在其国际关系上不得使用威胁或武力，或以与联合国宗旨不符之任何其他方法，侵害任何会员国或国家之领土完整或政治独立。"

长期以来，学界对"使用武力"的讨论集中于"武力"是否在军事手段之外还包括经济胁迫等其他形式。[④] 1970年联合国大会通过的《关于各国依联合国宪章建立友好关系及合作之国际法原则之宣言》（以下简称《国际法原则宣言》）强调，各国不得以任何形式的胁迫侵害任何国家的政治独立或领土完整。[⑤] 1974年联合国大会通过的《各国经济权利和义务宪章》再次强调了这一立场。[⑥] 1999年国际法院作出的《威胁使用和使用核武器合法性》咨询意见指出，禁止使用武力原则并不局限于特定的武器，[⑦] 这也就意味着，武力之构成与否并不会与使用特定的武器有关，易言之，只要某种手段的使用可以被理解为一种交战形式，并被用以破坏生命和财产，即可以被认定为"使用武力"。[⑧]

这些规定似乎会让人们自然地相信包括经济胁迫在内的、甚至是网络行为等各种非传统军事行为也可以解释为《联合国宪章》第2条第4项中的"武力"。笔者赞成此种观点。

（一）解释《联合国宪章》第2条第4项时所持的基本态度

《联合国宪章》第2条第4项在表达中采用了"或"，将"使用威胁或武力"与"以与联合

① 以"网络战"（Cyber War）这一概念为例，西方学者克拉克认为：网络战是指未经其他国家授权，出于添加、更改或伪造数据，或对电脑、网络设备或为计算机控制的任何对象造成破坏的意图，而渗透入该国的计算机、网络或任何其他可能会影响到计算机系统的设备的行为。See Richard Clarke, *Cyber War* (Harper Collins Publishers, 2010), p. 67. 中国学者黄志雄认为：网络战是指国家直接或间接发起的网络攻击。黄志雄：《国际法视角下的"网络战"及中国的对策——以诉诸武力权为中心》，载《现代法学》2015年第5期，第145页。

② 西方有观点认为应当通过论证禁止使用武力原则在网络空间具有可适用性而拓宽主权国家的自卫权行使范围。See Jay P. Kesan & Carol M. Hayes, "Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace", (2012) 25 *Harvard Journal of Law & Technology* 429, pp. 530 – 543. 但是中国学者主要希望通过论证可适用性而强化主权国家对禁止使用武力原则的遵守，黄志雄、朱雁新等均持该观点。

③ 以传统战争法中的"比例原则"为例，仅在理解该原则中的一个概念"附带损害"上，学界就有较大分歧，详见下文阐释。

④ Malcolm N. Shaw, *International Law* (New York: Cambridge University Press, 8th edn, 2017), p. 2097.

⑤ 参见《国际法原则宣言》序言第9段：各国负有义务避免为侵害任何国家政治独立或领土完整之目的，使用军事、政治、经济或任何其他形式的胁迫。

⑥ 参见《各国经济权利和义务宪章》第1条：任何国家不得以任何形式干涉、强迫或威胁其他国家。

⑦ 《威胁使用和使用核武器合法性》第38、39段，国际法院网站，https://www.icj-cij.org/en/case/95，最后访问日期：2019年4月1日。

⑧ Ian Brownlie, *International Law and the Use of Force by States* (Oxford University Press, 1963), p. 362. 朱雁新也认可此观点，参见赵白鸽主编：《中国国际人道法：传播、实践与发展》，人民出版社2012年版，第119页。

国宗旨不符合的任何其他方法”并列。结合《维也纳条约法公约》解释之通则,[①] 笔者认为这意味着两层含义：第一层为：任何与联合国宗旨不符的方法在评价上都是消极的；第二层为：这些消极的方法若在效果上与使用威胁或武力产生的效果相当，则应当被禁止。[②]

其次，上述解释与国际法院对第 2 条第 4 项一贯秉持的严格的解释态度并无不合。第 2 条 4 项对各成员国的义务仅有一条限定，即不得采取任何可能会侵害任何成员国或国家之领土完整或政治独立的行为，至于这种行为本身的形式无需更是无法限定。若结合联合国“维持国际和平与安全”的首要宗旨来解读，这样的观点则更为自然通畅。就此，史久镛先生精辟地总结道：第 2 条第 4 项的用语重在表明广义的禁止，辅以有限的例外。[③]

在笔者看来，只有正确运用解释《联合国宪章》第 2 条第 4 项所持的基本方法，才能够准确分析禁止使用武力原则在网络空间的可适用性。

（二）理解和区分《联合国宪章》三个名词的必要性

《联合国宪章》在不同条款中分别使用了“使用武力”“武力攻击”和“侵略”这三个名词。[④] 关于这三个名词内涵的争议，一直没有停止过,[⑤] 但是，对这三个名词有一个清晰的理解对国家行为的界定和自卫权的启动至关重要。

在“尼加拉瓜案”中，国际法院首次提及了对“使用武力”和“武力攻击”的区分。国际法院认为有必要对“最严重的使用武力的形式”（the most grave forms of the use of force）以及“一般的使用武力的形式”（less grave forms）进行区分。国际法院同时指出，那些“最严重的使用武力的形式”往往构成了“武力攻击”（armed attack）,[⑥] 这说明，国际法院认为并非所有的“使用武力”都属于“武力攻击”，但我们至少可以确定，所有的“武力攻击”都必然“使用了武力”。[⑦] 更重要的是，“使用武力”是判断一国是否违反《联合国宪章》第 2 条第 4 项和相关国际习惯法的标准，而考虑到自卫权以“武力攻击”为前提条件,[⑧] 所以“武力攻击”是判断一国是否可以对发动武力的对象国进行自卫的标准。[⑨]

---

① 《维也纳条约法公约》第 31 条规定：条约的解释应当遵循每个用语的通常意义，同时应当放在上下文中，结合条约制定的宗旨和目的，秉持善意解释。

② 这样的思路旨在维护《联合国宪章》的宗旨，该观点类似于前美国海军陆战队法律顾问沃尔特·夏普（Walter Sharp）的观点，其被黄志雄总结为“目的论”，主要是指任何违背《联合国宪章》宗旨的行为都应当属于第 2 条第 4 项的约束范围。当前，国内学界的主流观点（以黄志雄和朱雁新为代表）是：网络行动是否构成《联合国宪章》第 2 条第 4 项中的“使用武力”，应当综合考虑该行动的手段、后果、目的和范围等因素。

③ 这里有限的例外仅指国家自卫权的行使以及联合国安理会采取的武力行动两种。参见史久镛：《国际法上的禁止使用武力》，载《武大国际法评论》2017 年第 6 期，第 3 页。

④ “使用武力”参见《联合国宪章》第 2 条第 4 项、“武力攻击”参见第 51 条、“侵略”参见第 1 条第 1 项和第七章。

⑤ Vida M. Antolin-Jenkins，“Defining the Parameters of Cyberwar Operations：Looking for Law in All the Wrong Places?”，（2016）51 *Naval Law Review* 132，p. 150.

⑥ 《尼加拉瓜诉美国案判决书》第 191 段，国际法院网站，https：//www. icj – cij. org/en/case/70，最后访问日期：2019 年 4 月 1 日。

⑦ 即认定一个行为是否构成“武力攻击”所要求的规模与效果必然超过认定一个行为是否构成“使用武力”所要求的规模与效果。

⑧ 史久镛：《国际法上的禁止使用武力》，载《武大国际法评论》2017 年第 6 期，第 4 页。

⑨ 《联合国宪章》第 51 条规定：联合国会员国只有在受到“武力攻击”时，在安理会采取必要办法之前，有权行使自卫权。也就是说，任何一种“使用武力”的行为，只有当其达到“武力攻击”的门槛时，遭受国才有权行使自卫权，若没有达到这样的门槛，该行为只是一种非法行为，不能启动自卫权。

区分“使用武力”和“侵略”也有着类似的意义，因为“侵略”是联合国安理会在《联合国宪章》第七章下行使其权力时面临的一种情况。[①] 1974 年联合国大会通过的《关于侵略定义的决议》指出，“使用武力”是侵略行为的显见证据，任何国家不得以任何性质的理由，不论政治性、经济性、军事性或其他性质的理由，为侵略行为做辩护。[②] 该文件同时不完全列举了七种被认定为侵略行为的行为，这七种行为无一例外地都至少可以认定为“使用武力”的行为。[③] 也就是说，所有的“侵略”都“使用了武力”造成，但并非只要“使用武力”就一定构成“侵略”。

至此，我们可以得到一个结论：依据《联合国宪章》，一个国家行为可以分为三种类别。第一种是没有越过第 2 条第 4 项门槛，不构成“使用武力”的行为；第二种是越过了第 2 条第 4 项的门槛，构成“使用武力”但不构成“武力攻击”的行为；第三种是构成“武力攻击”并据以启动自卫权的行为。

二　禁止使用武力原则适用于网络空间的困境

虽然我们承认了禁止使用武力原则在网络空间的可适用性，也从理论上对这“使用武力”“武力攻击”进行了区分，但是如果将这些名词置于网络空间这个新语境中，就会发现很多适用困境。

（一）界定网络行动的困境

1. 网络行动构成“使用武力”

一个广为接受的理论是：如果一个网络行动产生的物理效果达到了“使用武力”的标准，该行动则可以构成“使用武力”。主张这个观点的代表人物是美国国务院前法律顾问高洪柱，[④]

---

① 〔美〕迈克尔·施密特主编：《塔林手册 2.0 版》，黄志雄译，社会科学文献出版社 2017 年版，第 342—343 页。

② 《关于侵略定义的决议》指出，侵略是指一个国家使用武力侵犯另一个国家的主权、领土完整或政治独立，或以本《定义》所宣示的与《联合国宪章》不符的任何其他方式使用武力。参见《关于侵略定义的决议》第 1、2、5 条。

③ 《关于侵略定义的决议》第 3 条：
（a）一个国家的武装部队侵入或攻击另一国家的领土，或因此种侵入或攻击而造成的任何军事占领，不论时间如何短暂，或使用武力吞并另一国家的领土或其一部分；
（b）一个国家的武装部队轰炸另一国家的领土，或一个国家对另一国家的领土使用任何武器；
（c）一个国家的武装部队封锁另一国家的港口或海岸；
（d）一个国家的武装部队攻击另一国家的陆、海、空军或商船和民航机；
（e）一个国家违反其与另一国家订立的协定所规定的条件使用其根据协定在接受国领土内驻扎的武装部队，或在协定终止后，延长该项武装部队在该国领土内的驻扎期间；
（f）一个国家以其领土供另一国家使用让该国用来对第三国进行侵略行为；
（g）一个国家或以其名义派遣武装小队、武装团体非正规军或雇用兵，对另一国家进行武力行为，其严重性相当于上述所列各项行为，或该国实际卷入了这些行为。

④ 高洪柱提出了相当著名的一个例子：如果 A 国利用恶意代码攻击了 B 国的大坝并由此对下游人民的生命和财产造成巨大损失，那么 A 国此举与直接用一个炸弹轰炸大坝没有区别，都属于“使用武力”。迈克尔·施密特也认可这样的观点，他认为：如果网络行动可以产生传统武力产生的后果，例如投掷炸弹、发射大炮等等，那就没有理由将这样的网络行为排除出《联合国宪章》第 2 条第 4 项的适用范围。因此，一个可以直接导致（或很有可能导致）平民伤亡或者民用物体损坏的网络行为就属于“使用武力”。See Michael N. Schmitt, “*Cyber Operations and the Jus Ad Bellum*”, (2011) 56 *Villanova Law Review* 569, p. 573.

他清楚地表示：如果网络行动将会导致平民受伤、死亡或者民用物体损坏，那这个行动就是“使用武力”。但是，这样的观点无法回应一个事实：有些网络行动是不会产生物理上的效果的，但这并不妨碍这些网络行动对国家主权的侵犯。①

因此，如果要想延续上述路径将某些网络行动认定为“使用武力”，必须要完成的一个任务是：拓宽对“效果”的理解。这项任务最直观地体现在《塔林手册 2.0 版》中，专家组从“规模和效果”② 的角度总结了八种因素用以辅助判断一个网络行动是否属于“使用武力”，它们分别是严重性、即时性、直接性、侵入性、效果的可衡量性、军事性、国家的介入程度、合法性。③

这样的观点将“效果”的定义拓宽了许多，但是考虑到这些因素依赖大量的调查和彻底的分析，所以虽然它们对事后分析大有裨益，却无法在战时为国家提供及时有效的帮助。

在此基础上，值得思考的一个问题是：“经济损失”是否应当涵盖到这些因素中。所谓的考虑经济损失就是指：国家受到某一网络行动的影响后，通过对比该行动前后其呈现的经济数据来辅助判断该行动是否属于“使用武力”。这个问题的提出主要是因为学者们已经关注到两方面事实。一方面，当今世界经济相互交融，抛开经济损失谈网络行动的负面影响是不现实也是不全面的。④ 另一方面，网络行动产生的间接影响远远超过了其直接影响，⑤ 而间接影响中最重要的表现就是经济损失。因为修复系统需要巨大资金，⑥ 网民对网络的恐惧也会影响整个市场表现，尤其会重创电子商务的发展。⑦

2. 什么样的网络行动构成“武力攻击”

根据《空战和导弹战国际法手册》，⑧“计算机网络攻击”是指：操纵、扰乱、剥夺、削弱或破坏驻留在计算机或网络的信息，或计算机和网络本身的行动，或者是控制计算机或计算机网络

① Priyanka R. Dev，“Use of Force and ‘Armed Attack’ Thresholds in Cyber Conflict：The Looming Definitional Gaps and the Growing Need for Formal U. N. Response”，（2015）50 *Texas International Law Journal* 381，p. 388.

② “规模和效果”一词最早在“尼加拉瓜案”中被国际法院提出，但是国际法院仅是用以区分最严重的和不太严重的使用武力的情况，其具体的定义并不清楚。（《塔林手册 2.0 版》的编写由北约“网络合作防御卓越中心”发起，由国际专家组在 2012 年完成的《塔林手册 1.0 版》基础上完成，是国际上第一项对“网络战”的国际法问题进行大规模集体研讨的成果。武汉大学黄志雄教授是这个国际专家组的成员之一。）

③ 这些因素最早由施密特提出，但他当时只提出了七项因素，未涉及“军事性”因素。See Michael N. Schmitt，“Computer Network Attack and the Use of Force in International Law：Thoughts on a Normative Framework”，（1999）37 *Columbia Journal of Transnational Law* 885，pp. 888 – 889. 施密特强调：这些因素不是绝对准确的，一个行为是否属于“使用武力”归根结底取决于国家自己。这些因素也不是决定性的和穷尽的，不应当被呆板适用。对于哪些因素更重要一些、不同因素的比重是多少这些问题，都应当充分结合背景情况考虑。See Michael N. Schmitt，“Cyber Operations and the Jus Ad Bellum”，（2011）56 *Villanova Law Review* 569，p. 577.

④ 《塔林手册 2.0 版》专家组中的一些专家就指出：网络行动导致的市场瘫痪可以引发灾难性后果，这足以将其定性为武力攻击。参见《塔林手册 2.0 版》规则七十一之十二。

⑤ 直接影响指影响目标系统或网络。间接影响指影响与目标系统交互的系统以及使用目标系统的人。See Stephen Dycus，“Congress's Role in Cyber Warfare”，（2010）4 *Journal of National Security Law & Policy* 155，p. 163.

⑥ Debra Wong & Brian M. Hoffstadt，“Countering the Cyber-Crime Threat”，（2006）43 *American Criminal Law Review* 201，p. 202.

⑦ Richard & W. Downing，“Shoring Up the Weakest Link：What Lawmakers Around the World Need to Consider in Developing Comprehensive Laws to Combat Cybercrime”，（2005）43 *Columbia Journal of Transnational Law* 705，p. 709.

⑧ 这部手册由哈佛大学“人道主义政策与冲突研究”项目组在世界范围内遴选的三十多名学者在 2009 年编写完成，旨在对现行空战和导弹战法律规则进行整合，但手册本身没有法律约束力。

的行动。[①] 这个定义忽略了网络攻击可能带来的物理效果，也没有将其与传统武力攻击完全区分开来。[②]

另一种逐渐兴起的定义将“网络攻击”理解为：基于政治或国家安全目的而采取的破坏计算机网络功能的任何行动。[③] 该定义对网络攻击的影响进行了最大化的考量，但也正是这种最大化考量使得该定义过于宽泛。而且它仅仅关注到了政治或国家安全目的，却排除了基于其他目的而发动的网络攻击。

《塔林手册2.0版》则认为：网络攻击是一种可合理预见的会导致人员伤亡或物体毁损的网络行动。[④] 该定义最大的特点是将标准定位在行动的效果上，即任何一种可以预期的会造成损害的网络行动均构成网络攻击。但由于其未对“效果”的范围作出界定，因此实践中的可操作性不强。

以上是“网络攻击”定义本身会产生的各种争论。但是，跳脱出定义本身，实践中各国面临的任务是：首先对一个网络行动定性。

根据上文，我们可以将一个国家行为分为三类，然而，这种理论上看似泾渭分明的分类在实践中并不能帮助一个国家区分“使用武力”和“武力攻击”，虽然国际法院早在“尼加拉瓜案”中就提出了区分标准——“规模和效果”。但时至今日，这个标准的具体内涵是什么仍然有非常大的争议。若再将这个问题置于网络空间中，模糊地带只会更多。[⑤]

（二）应对违反禁止使用武力原则之行为的困境

近年来，西方学者认为，国家与适格的非国家行为体在网络空间极其容易违反禁止使用武力原则，[⑥] 所以极有必要讨论自卫权或人道主义干涉。笔者认为，既然该原则在网络空间应当得到遵守，那么紧接着思考遵守的对立面确实是有必要的。[⑦] 但在这样的思考之前，有两点基本立场需要阐明：第一，禁止使用武力原则是所有国家应遵守的义务，网络空间亦不例外，如何履行和监管履行该义务是国际社会应首先关注的重点。第二，面对违反该原则的行为，国际社会应至少形成一个共识：无论是自卫还是所谓的人道主义干涉，都不能允许不受控制地使用武力。[⑧] 具体到网络空间，一旦“网络攻击”得以确认，基于传统习惯国际法和战时法规的内容，三大原则就必须予以深入讨论：（1）区分原则；（2）比例原则；（3）中立原则。[⑨]

---

① 《空战和导弹战国际法手册》规则一。该定义参考的是美国军方对计算机网络攻击的定义。See JOINT CHIEFS OF STAFF, Joint Doctrine for Information Operations, Joint Publication 3 - 13 (13 February 2006), GL - 9, GL - 6, GL - 5.（计算机网络攻击是指扰乱、剥夺、削弱或破坏存储在计算机和计算机网络中的信息、或对计算机和网络本身采取这些行动的作战行动。）

② 朱雁新：《数字空间的战争：战争法视域下的网络攻击》，中国政法大学出版社2013年版，第81—83页。

③ Oona A. Hathaway, “*The Law of Cyber-Attack*”, (2012) 100 *California Law Review* 817, pp. 826 - 827.

④ 《塔林手册2.0版》规则九十二。

⑤ 《塔林手册2.0版》也仅仅是关注到了这个问题，鉴于专家组内部争议较大，手册没有给出可行观点。

⑥ 黄志雄：《国际法视角下的“网络战”及中国的对策——以诉诸武力权为中心》，载《现代法学》2015年第5期，第156页。

⑦ 对立面是指：一旦禁止使用武力原则被违反，传统战时法即应当被适用。

⑧ 史久镛：《国际法上的禁止使用武力》，载《武大国际法评论》2017年第6期，第7页。

⑨ Heather H. Dinniss, *Cyber Warfare and the Laws of War* (New York: Cambridge University Press, 2014), p. 280.

1. 区分原则[①]

区分原则要求国家区分平民和战斗人员、民用物体和军事目标。国家也只能使用可控制、可预测、可区分的武器进行战争。[②] 然而，如今攻击对象的愈发重合以及网络空间天然的无法区分性使得区分原则的适用举步维艰。

第一，网络空间天然的无法区分性。在传统武装冲突中，犯罪、间谍、攻击等行为可以通过“特征和规模”加以区分。但是在网络空间中，上述行为在某些阶段是完全相同的。[③] 这就给所有国家提出了一个新的任务，即如何在监测活动中准确区分网络行动并针对不同类别的网络行动启动不同的反制措施。

第二，平民和战斗人员难以区分。在传统习惯国际法和战时法背景下，只有三类人允许受到合法攻击：战斗人员、直接参与敌对行动的平民以及拥有持续作战职能的平民。[④] 但在网络空间中，平民和战斗人员的界限变得异常模糊，尤其是当受到国家支持的个人也加入到网络攻击中时。

为了解决这个问题，《塔林手册 2.0 版》采取了“地位或行为”标准。基于这个标准，一个受到国家支持而参与到网络攻击中的个人也会因为他的行为而失去了免受攻击的权利。但是，这样的结论引发了一些质疑。

一方面，这个标准导致的结论过于宽泛。如果将“行使战斗人员的行为”作为标准之一，即意味着自发抵抗的民众也免于保护。[⑤] 这样的结论显然无法被广泛接受，因为民众在战时出于家国情怀而作出的自发抵抗行为是不可避免的，无论是基于传统战争视角还是网络战争视角。

另一方面，这个标准仍然无法解决网络战争的天然障碍。网络战争的最显著特征之一就是不受时间和空间的限制。[⑥] 这意味着不论是平民还是战斗人员都可以不加区分地参与到战争中去，这会导致区分原则在实践中的可执行性大打折扣。

第三，民用物体和军事目标难以区分。武装冲突的一大表现就是大规模袭击对方国家的基础设施，这些基础设施又被分为民用物体和军事目标。[⑦] 然而，现实情况是：那些常常被用来开展重要的民用业务的基础设施也越来越多地被用来开展网络间谍、实施网络攻击、进行战略沟通等

---

① 《日内瓦公约第一附加议定书》第 48 条：为了保证对平民居民和民用物体的尊重和保护，冲突各方无论何时均应在平民居民和战斗人员之间、在民用物体和军事目标之间加以区别，因此，冲突一方的军事行动仅以军事目标为对象。

② Oona A. Hathaway，“The Law of Cyber-Attack”，（2012）100 *California Law Review* 817，p. 823.

③ Gary D. Brown，“International Law Applies to Cyber Warfare：Now What”，（2017）46 *Southwestern Law Review* 355，p. 358.

④ Oona A. Hathaway，“The Law of Cyber-Attack”，（2012）100 *California Law Review* 817，p. 853.

⑤ 《塔林手册 2.0 版》规则九十六规定了四类可以作为网络攻击的目标：（1）武装部队的成员；（2）有组织武装团体成员；（3）正在直接参加敌对行动的平民；（4）在国际武装冲突中参加自发抵抗之民众的人员。这么区分的依据正是“地位或行为”标准。前两类人员的可攻击性是基于他们的“地位”，后两类人员则是基于他们的“行为”。

⑥ 按照盖里·布朗的总结，网络战争的三大特征分别是：（1）不受时间和空间的限制；（2）网络攻击手段的非垄断性；（3）网络行动的不可区分性。Gary D. Brown，“International Law Applies to Cyber Warfare：Now What”，（2017）46 *Southwestern Law Review* 355，p. 358.

⑦ 所谓军事目标，是指凭借其性质、位置、目的或用途对军事行动产生有效贡献，而且在当时情况下对其全部或部分毁坏、缴获或失去效用可提供明确的军事利益的物体。详见《塔林手册 2.0 版》规则一百，这个定义参考的是《日内瓦公约第一附加议定书》第 52 条第 1 款。该定义采用的是“性质、位置、目的、用途”标准，任何一个物体只要符合其中任何一个标准，即可被认定为军事目标。该标准与上述提及的“地位或行为”标准存在着类似的问题，即导致的结论或许过于宽泛。

一系列一国政府或民众想要做的重大事项。[①] 这对保护民用物体的实践造成了巨大挑战，尤其是对于网络空间而言，意图找到纯粹的民用网络基础设施，无异于海底捞针。[②] 为了回应这个问题，《塔林手册》专家组提出：所有军民两用的网络基础设施全部属于军事目标。[③] 但是按照专家组这样的思路，那么世界上还有哪些网络基础设施是绝对不属于军事目标的呢？

2. 比例原则[④]

该原则已被广泛接受为习惯国际法，适用于国际性和非国际性武装冲突。[⑤] 对于适用“比例原则”，[⑥] 有必要深入理解民用物体中的附带“损害”。

第一，对民用物体中附带“损害”的理解。网络攻击中，其对民用物体的附带损害究竟应当从什么角度加以衡量是我们需要着重思考的问题。目前，主要有三种观点。

一种观点认为：若网络攻击产生的实际损害后果与传统战争手段可能会产生的损害后果相当，则这样的损害后果即为适用比例性原则时应当考虑的后果。[⑦] 这无疑会受到战争中指挥官的欢迎，因为该思路将网络攻击与传统战争相挂钩，通过比对二者的损害后果就可得出结论，而指挥官对后者会产生的损害后果往往深谙于心。但是，该思路忽略了网络攻击或许根本不会产生传统战争会产生的损害的事实。例如，一场网络攻击直接导致了对方国家的通讯、医疗、银行系统瘫痪，这样的瘫痪必然会影响到平民的正常生活。[⑧] 但在现有研究水平基础上，若让指挥官比较其与直接用炸弹轰炸通讯公司、医院、银行所造成的后果孰轻孰重，显然是强人所难。

另一种观点认为：将所有未经授权的电脑入侵或网络系统入侵，且这些入侵导致电脑或系统中数据的更改的，认定为附带损害。[⑨] 这种思路要求我们在适用比例原则时，务必将某一行为对电脑或网络系统可能产生的所有影响全部纳入考虑范围。这样的观点过于超前，因为比例原则禁止的是那些“过于超出”预期的附带损害后果，远非这种观点下的所有后果。

还有一种观点提议：将“丧失功能”纳入判断附带损害后果的因素中。[⑩] 它强调：就民用物体的附带损害后果而言，其范围大小并无法量化，但其往往与预期的具体和直接的军事利益成正

---

① Cordula Droege，“Get Off My Cloud：Cyber Warfare，International Humanitarian Law，and The Protection of Civilians”，（2012）94 *International Review of the Red Cross* 533，p. 533.

② 随着网络通讯技术的普及，95% 的军用通讯设备在某些阶段也为民用通讯设备。See Vida Antolin-Jenkins，“Defining the Parameters of Cyberwar Operations：Looking for Law in All the Wrong Places?”，（2008）51 *Naval Law Review* 132，p. 133.

③ 参见《塔林手册 2.0 版》规则一百零一。专家组为了证明该观点，使用了一个类比：在传统战争中，攻击者在面对着军用车辆和民用车辆同时使用的公路网时，也并不会确切知道敌方军队将使用哪一条公路，只要该公路网中的某一条公路相当有可能被使用，整个公路网即可以作为被攻击的军事目标。类似地，计算机网络没有理由被区别对待。

④ 《日内瓦第一附加议定书》第 51 条：一次攻击行为若预计造成平民的附带伤害、附带死亡、民用物体的附带损害或者以上三种后果混合的情况，过于超出预期取得的具体、直接的军事利益，则该行为应当被禁止。

⑤ 朱文奇：《国际人道法》，商务印书馆 2018 年版，第 98 页。

⑥ 武汉大学李雪平、黄解放也称之为“相称性”。参见史久镛：《国际法上的禁止使用武力》，载《武大国际法评论》2017 年第 6 期，第 7 页。

⑦ Eric Talbot Jensen，“Cyber Attacks：Proportionality and Precautions in Attack”，（2013）89 *US Naval War College International Law Studies Series* 198，p. 211.

⑧ Stephen Petkis，“Rethinking Proportionality In the Cyber Context”，（2016）47 *Georgetown Journal of International Law* 1431，p. 1457.

⑨ William A. Owens & Kenneth W. Dam，*Technology*，*Policy*，*Law and Ethics Regarding U. S. Acquisition and Use of Cyberattack Capabilities*（The National Academies Press，2009），pp. 253 – 254.

⑩ 《塔林手册 2.0 版》专家组最终采纳了这一说法，详见于规则九十二、一百一十三。

比关系，换言之，若预期的具体和直接的军事利益足够大，那么大范围的附带损害也可能是合法的；相反，若预期的军事利益微不足道，那么再小的附带损害都应被禁止。[①] 这种观点确实很好地反映了网络攻击的特殊性，但却将指挥官的主观决定权无限放大。不过综合而言，这种观点确实最容易被接受。

第二，对“损害”类别的理解。任何损害都可以包括直接和间接两方面。具体到网络空间，网络攻击的直接损害指“立即的、第一序列的、未受干涉实践或机制改变的后果”；间接损害包括“延迟的第二、第三或更高序列的行动后果，往往通过中介事件或机制造成”。[②] 值得注意的是，根据《日内瓦公约第一附加议定书》给出的概念，比例原则旨在使武装行动的目标成果与预估的可能造成的损害间保持平衡，[③] 这就决定了该原则中的损害必须是前瞻性的，[④] 也就是说，比例原则不适用于事后评价。

3. 中立原则[⑤]

时至今日，学界对“网络活动同样应尊重中立原则”的观点已没有争议，[⑥] 但是其在具体适用时也需要面对诸多探索。

第一，违反中立原则的可能情形有哪些。首先可以确定的是，交战国若对中立国发动网络攻击，或者是中立国发动网络攻击，这是最直接的违反中立原则的情形。一方面，为了共同维护中立国的中立地位，所有交战国都有义务避免对中立国的网络攻击；另一方面，一旦中立国主动对其他国家发起网络攻击，便可当然视为其对中立地位的主动放弃。其次，根据《海牙第五公约》第 4 条的规定，交战国滥用[⑦]中立国网络空间的行为也属违反中立原则的应有之意，因为这些滥用行为直接损抑的是中立国作为主权国家对其网络空间的管辖权。[⑧]

第二，网络中立的内涵是什么。[⑨] 有些学者认为：网络中立要求中立国负有阻止交战国的电子数据在其网络空间中传输的义务。[⑩] 但是中立国负担这样的义务是否过重？毕竟网络空间本就交联互通，交战国完全可以通过一系列服务器和计算机掩盖数据来源以帮助传输。还有一些学者认为：应当采纳一种“以意识为基础的”中立观（intent-based neutrality）。[⑪] 在这种观念下，交

① 《塔林手册 2.0 版》规则一百一十三之八。

② See JOINT CHIEFS OF STAFF, Joint Publication 3 – 60: Joint Targeting (13 April 2007), chapterI – 9. 前文介绍过关于直接影响和间接影响的另一组概念，两组概念的实质相同，但是在“比例原则”处采用此处的概念更为直观，有助于理解。

③ 姜世波：《网络攻击与战争法的适用》，载《武汉大学国际法评论》2014 年第 2 期，第 56 页。

④ 所谓前瞻性，即要求网络攻击的实际强度和规模必须与预估的强度和规模成比例，前者不能高于后者。

⑤ 提到中立原则，首先需要研究的文件就是《海牙第五公约》。该公约第 1 条禁止交战国侵犯中立国领土。第 2 条禁止交战国的部队和装载军火或供应品的运输队通过中立国领土。第 4 条禁止交战国在中立国领土上设立无线电台或与交战国陆、海军联系的任何通讯装置或者利用战前交战国在中立国领土上设立的纯为军事目的、并且还没有公开为公众通讯服务的任何此类设施。

⑥ 肖凤城：《中立法研究》，人民出版社 2016 年版，第 213 页。

⑦ 所谓“滥用”，不仅包括第 4 条中列举的行为，还包括诸如交战国将中立国的网络空间作为媒介的行为。参见朱雁新：《数字空间的战争：战争法视域下的网络攻击》，中国政法大学出版社 2013 年版，第 174 页。

⑧ 需要注意的是，中立国侦测并阻止这些滥用行为具有相当大的困难，详见下文。

⑨ 《海牙第五公约》并没有对网络中立的内涵作出任何规定。

⑩ Joshua E. Kastenberg, “Non-Intervention and Neutrality in Cyberspace: An Emerging Principle in the National Practice of International Law”, (2009) 64 *Air Force Law Review* 43, p. 56.

⑪ Jeffrey T. G. Kelsey, “Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare”, (2008) 106 *Michigan Law Review* 1427, pp. 1448 – 1449.

战国只有在蓄意利用中立国网络系统传输网络武器时才会违反国际人道法，也就是说，中立国没有义务去预防交战国非蓄意下的网络武器传输行动，只要其不放任蓄意行动，其中立性就没有被破坏。[①] 但是它的实践性与客观性又有多强呢？毕竟这种观点将义务违反与否的决定权交由中立国自主论证。第三种观点认为：中立国不得在明知的情况下允许交战国利用位于其领土或在其排他性控制下的网络基础设施行使交战权利。[②] 这是一种“实际的”中立观，即只有当中立国已实际知悉了有关情况后，[③] 才产生对应的义务。这虽然是《塔林手册》采取的观点，但是其也面临着两个问题，一是它无法解决国与国之间，尤其是中立国与交战国之间的网络发展的差距问题。这些差距会产生一个国际社会需要面对的更加棘手的问题：网络攻击发起国（组织）的识别问题。一旦交战国的网络发展水平超越了中立国，例如，中立国的计算机正在成为僵尸电脑而被交战国用于网络攻击，[④] 就会发生中立国完全不知晓其中立地位受到威胁的情况。更严重的是，有些时候即便中立国知晓情况，碍于技术限制，其也无法归属攻击的来源。[⑤] 二是由于“知悉与否”由中立国自主论证，很有可能出现中立国实际并不中立的情况。

第三，《海牙第五公约》的例外性规定研究。公约第 8 条规定：中立国没有义务禁止或限制交战国使用属于它或公司或私人所有的电报或电话电缆以及无线电报器材，只要中立国保证该举措对交战双方公正不偏地予以适用。[⑥] 基于该条规定，我们产生的疑问是：第 8 条是否包括当下的现代通信技术（网络技术）？虽然有支持第 8 条包括现代通信技术的声音，[⑦] 但必须考虑到：在制定该公约时，起草人显然没有想到人类在未来甚至可以利用网络发动战争。即便电报、电话电缆和无线电报器材被写进公约，但它们之所以被起草人考虑是因为这些工具都可以为交战国攻击的开展提供便利，而非它们自身拥有的攻击性。[⑧] 因此，对第 8 条仍应当慎重解释之。

---

① “以意识为基础的”中立观也得到了其他一些国内外学者的赞成。See Danielle Higson，“Applying the Law of Neutrality While Transiting the Seas of Cyberspace”，（2006）6 *National Security Law Brief* 1，p. 30；黄德明主编：《国际人道法若干问题研究》，武汉大学出版社 2013 年版，第 96 页。

② 《塔林手册 2.0 版》规则一百五十二。

③ 需要考虑“推定知悉”的情况，它是指：中立国理应知道交战国正在其领土或在其排他性控制下的网络基础设施行使交战权利的情形。但“推定知悉”是否意味着中立国负有义务仍然存在很大争议。参见《塔林手册 2.0 版》规则一百五十二之五。

④ 姜世波：《网络攻击与战争法的适用》，载《武汉大学国际法评论》2014 年第 2 期，第 56 页。

⑤ 技术上领先的攻击者几乎可以从任何地区的计算机介入网络从而实施形态各异的网络攻击。并且攻击者完全具备扫除攻击、掩盖或混淆攻击的痕迹。参见丁丽柏、朱静：《〈塔林手册〉对网络攻击中“武力”的界定及反思》，载《河北法学》2018 年第 12 期，第 86 页。

⑥ 《海牙第五公约》第 8 条。

⑦ 斯考特认为：第 8 条的例外性规定适用于现代通信技术。See Roger D. Scott，“Legal Aspects of Information Warfare：Military Disruption of Telecommunications”，（1998）45 *Naval Law Review* 57，p. 62. 朱雁新认为：从本质上讲，计算机网络与电报、电话电缆、无线电报器材都是信息传递媒介，因此可以将第 8 条扩大解释使其包括现代通信工具。参见朱雁新：《数字空间的战争：战争法视域下的网络攻击》，中国政法大学出版社 2013 年版，第 186 页。美国政府也持类似观点，他们认为任何国际条约都未对其信息行动的开展（information operations）制造障碍。See Department of Defense Office of General Counsel，an Assessment of Internaitonal Legal Issues in Information Operations（MAY 1999），p. 34.

⑧ 与电报、电话电缆和无线电报器材不同的是，个人、国家完全可以利用网络技术直接发动攻击。

三　对禁止使用武力原则适用于网络空间的困境应对

作为网络空间国际治理中最为重要的内容之一，诉诸武力权和战时法规一直都是西方国际法学界关注的热点问题。[①] 但是客观而言，国内学界对这些问题的关注十分有限，这直接导致了中国尚未对各种网络空间议题形成体系化认识和应对策略。反观美国，其政界和学界不断利用各种场合和方式输出自身观点，[②] 更是反复提出新理念和新词汇来完善其有关网络空间国际法的主张，[③] 并根据形势的变化和新的需要对既有主张和理论作出新的解释，这使得美国关于网络空间国际法的一整套理论得以在稳定中不断得到澄清和新的发展，并借此产生了不可忽视的全球影响力。[④]

鉴于诉诸武力权和战时法规仍将是今后一段时间网络空间国际规则博弈中的焦点问题之一，中国有必要对相关议题作出回应。具体而言：

第一，网络空间国际治理体系应当建立在现有国际法基础之上。[⑤] 涉及到具体规定，始终不能脱离以《联合国宪章》为核心的国际法基本原则，[⑥] 始终不能动摇联合国在国际法体系和全球治理机制中的核心地位。[⑦] 在此基础之上，学界需要关注网络空间之外已经存在且具有习惯法地位的实然法，并对这些规则应当如何适用于网络空间加以澄清和发展，而不是倡导新的应

① 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》，载《厦门大学学报（哲学社会科学版）》2018 年第 1 期，第 2 页。

② 从 2011 年美国政府出台《网络空间国际战略》，到 2012 年的“高洪柱演讲”，再到 2016 年的“依根演讲”以及两个版本的《塔林手册》的编写，这些都体现了美国政府意图左右网络空间规则制定的野心。

③ 黄志雄：《网络空间负责任国家行为规范：源起、影响和应对》，载《当代法学》2019 年第 1 期，第 68 页。

④ Elaine Korzak，“The 2015 GGE Report：What Next for Norms in Cyberspace?”，https：//www. lawfareblog. com/2015 - gge - report - what - next - norms - cyberspace（last visited March 20，2019）.

⑤ 王铁崖认为，《联合国宪章》及 1970 年《国际法原则宣言》等宪章性国际法文件所包含的国际法基本原则，是现行国际秩序和国际法体系不可或缺的重要组成部分。参见王铁崖：《国际法》，法律出版社 1981 年版，第 64 页。徐宏认为，当前，《联合国宪章》所确立的国际秩序框架、安全机制、行为规范和价值理念是现代国际法和国际关系的基石。参见徐宏：《人类命运共同体与国际法》，载《国际法研究》2018 年第 5 期，第 9 页。张辉认为，国际法存在和发展的根基从共存和有限合作为基本特征的国际社会，转变为国家间存在广泛而重要的共同利益从而更紧密合作的国际共同体。当今时代即使在社会制度迥异的国家间，也是你中有我、我中有你的关系，虽然国家间价值观、文化传统差别很大，但存在着共同珍视和向往的价值，对这些价值的追求催生了《联合国宪章》等一系列国际法文件的诞生。参见张辉：《人类命运共同体：国际法社会基础理论的当代发展》，载《中国社会科学》2018 年第 5 期，第 53—55 页。上述观点均提及《联合国宪章》等宪章性国际法文件对现代国际法和现代国际法体系的基础性意义，因此，笔者认为，第二次世界大战后《联合国宪章》的诞生和联合国的建立，标志着国际法进入了新的发展阶段，现代国际法基础也应当以《联合国宪章》为基石。

⑥ 《联合国宪章》第一次明确和系统地规定了七项国际法基本原则。以此为基础，联合国大会先后通过了一系列载有国际法基本原则的决议，其中，特别是 1970 年《国际法原则宣言》郑重明确地宣布了七项国际法基本原则，要求“所有国家在其国际行为上”予以“严格遵守”。这七项原则是：不使用武力威胁或使用武力、和平解决国际争端、不干涉任何国家内政、各国依宪章彼此合作、各民族权利平等与自决、各国主权平等、善意履行宪章义务。至此，一个由若干原则构成的国际法基本原则的体系初步形成。由于国际法基本原则是被作为整体的国际社会认定为指导国际关系的一般准则，因此，这个体系的形成，无疑也为国际造法提供了一般国际法的根据。参见古祖雪：《国际造法：基本原则及其对国际法的意义》，载《中国社会科学》2012 年第 2 期，第 142 页。

⑦ 张晓君：《尊重国际法权威 维护国际秩序》，载《求是》2018 年第 20 期，第 25—27 页。

然法。[①]

当前，网络已发展成为各国以信息化方式运作的金融、商贸、交通、通信、军事、思想文化等系统的神经中枢，网络也已经成为与土地及其他有形资本一样重要的权力资源，对国家实力、国家安全和国际关系发展起着关键性作用。[②] 可以预见到的是，随着网络空间地位的急速加强，网络空间国际治理体系的构建势在必行。[③] 以美国为首的西方发达国家再一次不出意料地走在了最前端并试图以“先行者”的身份主导网络空间的治理秩序。以《塔林手册 2.0 版》为例，虽然手册自身反复强调其不具有法律约束力，未受到政治影响，但是已经有越来越多的政府高级别官员在很多场合援引该手册观点，很多学者甚至将其视为构建网络空间国际治理体系的蓝本。[④] 对此，一方面，我们可鼓励更多的学者投身到与“网络空间治理”有关的研究中；另一方面，我们应当高度重视当前碎片化的网络空间制度，可坚持在以《联合国宪章》为核心的国际法基本原则之上形成中国网络空间治理路径。

第二，有关“网络行动的定性问题研究”仍亟待学界探索。笔者认为，对于判断一个网络行动是否达到了“使用武力”的门槛或“武力攻击”的门槛的问题，虽然短时期内很难形成一套统一标准，但至少要确保客观性与全面性。

首先，网络行动定性务必遵循客观标准。如前文所述，在各种议题上，诸多观点的共性都是放大了国家的主观性。与传统使用武力行为必然会产生物理效果不同，网络空间未必与物理损害有必然联系。为了帮助受攻击国判断自身处境，更为了帮助其他国家或机构考察和审视受攻击国的判断，客观性起到了很大的可量化作用，这也是为什么笔者在上文提出一国或可以通过对比在遭受到某一网络行动前后其呈现的经济数据来辅助判断该行动是否属于“使用武力”。当今中国，庞大的网络系统已经融入到金融、商贸等关键领域，网络更直接捆绑着绝大多数公民的日常生活，在这种背景下，坚持客观性标准，突出“经济因素”在网络行动定性中的重要地位，具有重大现实意义。

其次，网络行动定性离不开全面考察。认定一个网络行动决不能仅考察一个或几个因素，而是应当以全面的态度综合考察，这是由网络空间的特征决定的。

一方面，网络空间不受时间和空间限制。这使得发起网络攻击无需再像发动传统武装冲突一样需要依赖客观环境。另一方面，网络行动手段具有非垄断性。非垄断性意味着只要掌握了网络技术，任何国家均可对网络空间的和平与安全产生威胁，此外，发起网络行动的主体也不再局限于国家，有关组织甚至是个人均可以随时随地发起具有针对性的行动。最后，网络行动具有很强的不可区分性。这会给遭受到网络行动的国家造成巨大的识别困难。今天的网络行动是普遍的，而片面定性这些网络行动的后果之一就是“使用武力”行为的泛滥，这是不可取的。鉴于此，

① 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》，载《厦门大学学报（哲学社会科学版）》2018 年第 1 期，第 4 页。

② 黄志雄：《国际法在网络空间的适用：秩序构建中的规则博弈》，载《环球法律评论》2016 年第 3 期，第 10 页。

③ 网络空间国际治理体系的构建最直接地体现在立法呼声的不断增强上。立法形式主要包括多边公约、双边协议、联合国大会决议等等。

④ Eric Talbot Jensen，“The Tallinn Manual 2.0：Highlights and Insights”，（2017）48 *Georgetown Journal of International Law* 735，p. 778.

尽可能多地考察各种因素，包括经济因素、时间因素、影响范围、技术水平、国际关系等等，[①] 有助于更恰当地理解一个网络行动的性质。

第三，中国应当积极推动构建网络空间命运共同体。近年来，西方不免过度渲染了“网络战”的威胁，这种渲染给人们营造出一种错觉：网络战场已经形成，网络战亦可随时爆发。但我们不禁发问：网络战在哪呢？如同“费米悖论”[②] 一样，从未发生网络战的事实让我们陷入沉思：很多理论研究是否是在舍本逐末？

互联网发展至今，已经与人类的日常生活息息相关，一个和平安宁的网络空间符合所有国家的根本利益。在这样的背景下，国际社会本应摒弃“零和”思维，致力于共同构建和谐的网络空间秩序，但是不少西方国家却将注意力放在了“如何通过解释让行使自卫权在网络空间也变得顺理成章”，这展示了这些国家鲜明的网络军事化倾向和霸权主义思想。对此，我们应当认识到：

首先，网络军事化违背了《联合国宪章》的首要宗旨。人的安全主要有两方面内容。其一是免受诸如饥饿、疾病和压迫等长期威胁的安全；其二是在家庭、工作或社区等日常生活中对突如其来的、伤害性的骚扰的保护。[③] 作为一个旨在增进各国人民福祉的国际组织，联合国更加侧重于应对“对人的安全普遍性的挑战”。[④] 与人类生活休戚相关的网络空间一旦遭到恶意攻击，势必会危害到人类的普遍安全，[⑤] 并违背《联合国宪章》规定的“维持国际和平及安全”的首要宗旨。[⑥]

其次，《联合国宪章》第 2 条第 4 项是研究核心。[⑦] 任何战争和武装冲突从本质上讲都是不公正的，这决定着禁止使用武力原则这项义务始终应当得到各国的遵守。只有在最为罕见的情况下，追求武力的政策才有可能服务于“上善”，因此，最好不要根据例外来制定额外规则。[⑧] 西方学界目前的主流倾向恰恰是根据例外来制定规则，具体而言，就是利用《联合国宪章》第 51

① 时间因素是指一国在判断某一网络行动的性质时，有必要考察当时的内政状况、国内局势，通过比对网络行动的发动时机和本国国内局势的发展势态以辅助判断该网络行动的目的。影响范围是指有必要考察该网络行动的辐射范围和所辐射地区的发展水平。技术水平是指通过考察支撑该网络行动的技术手段的特征和先进程度，辅助判断行为主体。国际关系是指考察该网络行动下的时代背景，尤其是双边关系。

② 1951 年，著名物理学家费米在与友人讨论外星文明时提出一个疑问：“外星人都在哪里呢?”，这句话就是“费米悖论”。简单地说，“费米悖论”是指：一方面，人类可以通过现有科学理论证明外星文明确实存在；但是另一方面，迄今为至人类又从来没有发现过外星文明的任何痕迹。这样的矛盾让人们开始怀疑探索外星文明的意义。

③ United Nations Development Programme（UNDP），（New York：Oxford University Press，1994），http：//hdr. undp. org/sites/default/files/reports/255/hdr_ 1994_ en_ complete_ nostats. pdf（last visited March 16，2019）.

④ 参见柳建平：《安全、人的安全和国家》，载《世界经济与政治》2005 年第 2 期，第 59 页。

⑤ 以中国为例，2018 年，国内企业、公共服务机构甚至是政府机关均有遭遇勒索病毒攻击的情况，生产系统数据被加密破坏，重要业务系统陷入崩溃。参见腾讯安全发布的《2018 上半年互联网黑产研究报告》。从世界范围看，2018 年 2 月，知名代码托管网站 GitHub 遭遇史上大规模 Memcached DDoS 攻击，流量峰值高达 1. 35 Tbps；6 月，韩国加密货币交易所遭黑客攻击，引发比特币近三个月最大跌幅；俄罗斯在世界杯期间遭到将近 2500 万次网络攻击。

⑥ 《联合国宪章》序言开宗明义：“我联合国人民同兹决心，欲免后世再遭今代人类两度身历惨不堪言之战祸……并为达此目的……集中力量，以维持国际和平及安全。”《联合国宪章》第 1 条第 1 项规定联合国的首要宗旨为：“维持国际和平及安全；并为此目的：采取有效集体办法，以防止且消除对于和平之威胁，制止侵略行为或其他和平之破坏；并以和平方法且依正义及国际法之原则，调整或解决足以破坏和平之国际争端或情势。”

⑦ 诚如著名国际法学者路易斯·亨金所言：《联合国宪章》第 2 条 4 项是国际法最重要的规范，它是国际法律制度首要价值的浓缩和体现，是国家独立自主的保护神。See Louis Henkin，*International Law*：*Politics and Value*（Martinus Nijhoff Publishers，1995），p. 113.

⑧ 史久镛：《国际法上的禁止使用武力》，载《武大国际法评论》2017 年第 6 期，第 8 页。

条（自卫权）和第53条（联合国集体安全机制下的使用武力）扩大诉诸武力权的范围。[①]

再次，推动各国共同制定普遍接受的网络空间国际治理原则是维护《联合国宪章》各项宗旨，是构建网络空间命运共同体的应有之意。从海洋空间治理到民用航空合作，从南极的和平开发再到外太空的国际协作，这些国际实践表明，对新领域、新空间的有序治理离不开各国的共同参与。笔者认为，构建网络空间命运共同体的最终目标是通过打造一个普遍安全、持久和平、开放包容的网络平台实现各国的共同繁荣。这需要国际社会在尊重各国主权、领土完整和政治独立，尊重人权和基本自由，尊重各国历史、文化、社会制度的多样性的基础上，通力合作。

虽然当前的网络空间合作面临诸多挑战，但是制定一般法律原则的思路并非不可能。上个世纪中期，人类在“如何规范各国在外太空的行为”这一问题面前，遇到了与今天类似的境况，但是《关于各国探索和利用包括月球和其他天体的外层空间活动所应遵守原则的条约》（以下简称《外层空间条约》）和后续一系列条约的签订，[②] 展示出人类在处理新空间问题上的智慧，即在联合国的积极推动下，宣布若干基本法律原则，首先确保新空间的和平稳定。[③] 在网络空间的治理问题上，类似地，也可以首先确定一些基本法律原则，例如：各国不得在网络空间实施有悖于国际和平与安全目标的行动；各国不得利用信息通信技术和信息通信网络干涉他国内政，破坏他国政治、经济和社会稳定；在利用网络空间时产生的任何争端，都以和平方式解决，不得使用武力或以武力相威胁等。[④]

结　语

网络空间虽是一个新兴领域，但是诉诸武力权和战时法在网络空间的适用却是一个被长期讨论的焦点议题，虽然其中存在诸多争议，但是各国在网络空间应当遵守禁止使用武力原则这一基本原则性立场不应被突破。

对网络空间的国际治理问题，始终不能脱离以《联合国宪章》为核心的国际法基本原则，始终不能动摇联合国在国际法体系和全球治理机制中的核心地位。对网络行动的定性问题，客观性和全面性标准有助于提升定性手段的可量化程度以及防止“使用武力”的泛滥。对一些国家的网络军事化倾向，应当鲜明地指出它们对《联合国宪章》首要宗旨的违背和对《联合国宪章》

① 不使用武力原则是联合国集体安全制度的核心，自卫权只是例外，但是近年来，大谈网络战、自卫权等例外的论调不绝于耳，不使用武力原则却备受冷落，这使得网络空间面临滑向军事化的风险，必须受到国际社会的高度关注。详见《中国代表在网络空间首尔会议上的发言》，载《中国国际法年刊》（2013），法律出版社2014年版，第681页。

② 除《外层空间条约》外，还包括《营救协定》《责任公约》《登记公约》和《月球协定》。

③ 以《外层空间条约》的诞生为例，联合国起到了关键作用。1958年，美苏两国分别向联合国提出了关于外层空间和天体的建议。在经历了多次讨论之后，所有国家一致认为外层空间只能是用于和平的目的，一般意义上的主权国家的法律原则上也适用于外层空间，但是外层空间不能够成为国家主权所要求的对象。1961年，联合国大会通过了关于探索和利用外层空间的基本原则，1966年，联合国大会正式通过《外层空间条约》。

④ 实际上，包括中国在内的一些国家已经在尝试推动确立一些网络空间的基本原则。中国和俄罗斯等国在2011年向联合国大会提交了“信息安全国际行为准则”草案；综合国际社会的意见和形势发展，上海合作组织成员国更新了该草案并在2015年1月将新版“准则”作为联大正式文件散发。“准则”旨在明确各国在信息空间的权利与责任，推动各国在信息空间采取建设性和负责任的行为，促进各国合作应对信息空间的共同威胁与挑战，以便构建一个和平、安全、开放、合作的信息空间，确保信息通信技术和信息通信网络的使用促进社会和经济全面发展及人民福祉的目的，并与维护国际和平与安全的目标相一致。

第 2 条第 4 项的错误认识。

对中国而言，推动构建网络空间命运共同体不仅有利于共同繁荣目标的落实，也有助于维护国际和平与安全。为实现这一目标，中国应汲取人类在曾经的“新活动空间”中所达成的合作经验，积极推动网络空间中的基本法律原则早日确立。

The Principle of Prohibition of Use of Force in Cyberspace

Wang Meili and Chen Yu

Abstract: International legal issues concerning cyberspace have caught more and more scholars' attention, among which the most hot issues include the re-understanding of the principle of prohibition of use of force from the perspective of cyberspace. At present, most western scholars focus on how to expand the scope of jus ad bellum and are inclined to promote the international community to expand the interpretation of it. This is in sharp contrast to China's attitude of opposing the arms race in cyberspace and actively promoting the construction of a community of shared future in cyberspace. In view of this, on the basis of making full use of the United Nations platform, it is necessary for China to put forward its position towards jus ad bellum and jus in bello, centering on the basic principles of international law with United Nations Charter at its core. Besides, China should actively address western misconceptions and take the lead in making cyberspace order.

Keywords: Cyberspace, Cyber Attack, Cyber War, Prohibition of the Use of Force

（责任编辑：李西霞）