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

张　华

摘要：自卫权问题一直是网络空间国际法适用的争论焦点。各国新近发布的网络空间立场文件一致将规模和效果奉为“武力攻击”的判断标准，同时在诸多方面显示出扩大自卫权适用的倾向。但是，网络空间自卫权的适用前提、适用时间和适用对象均存在法律不确定性。将传统武力攻击情境中不无争议的累积性自卫、预先性自卫和针对非国家行为体的自卫引入网络空间不仅缺乏合法性和可行性，而且会加剧网络空间的军事化，导致自卫权的滥用。中国在网络空间国际造法进程中应坚决抵制扩大自卫权适用的主张，强调必要性和相称性原则对自卫权的内在限制，同时提倡联合国安理会在应对跨境网络攻击方面发挥建设性作用，以遏制网络空间的军事化。

关键词：网络空间；自卫权；法律不确定性；国际造法；中国立场

中图分类号：D990　　**文献标识码：**A　　**文章编号：**1000—8691（2021）06—0081—12

网络空间国际法规则的发展一直存在两种路径之争：究竟是应适用现有国际法规则——其中主要是国际习惯法规则，抑或需要制定全新的条约规则？客观理性的答案自然是兼顾两种路径。[①]但实践中，仍有不少国家罔顾现实，坚持现有国际法足以规制网络空间涌现的新问题。近年来，联合国信息安全政府间专家组（以下简称 UNGGE）进程和开放式工作组（以下简称 OEWG）进程为网络空间“建章立制”提供了多边性的讨论平台，取得了令人瞩目的成就。2021 年 3 月和 5 月，首届 OEWG 进程和第六届 UNGGE 进程先后成功达成了最终报告[②]，代表了联合国框架下网络空间国际造法进程的最新进展。与此同时，网络空间国际造法进程出现了不容忽视的“第三条道路”：近年来，各国陆续发布有关国际法适用于网络空间的专题立场文件，大有在网络国际法领域催生新的国际习惯法规则的趋势。众所周知，网络空间适用国际法的讨论源于“网络战”。然而，其中争论最为持久和激烈的自卫权问题始终是网络空间国际造法进程中不可逾越的“红线”。2017

基金项目：本文是 2020 年国家社会科学基金重大项目“网络空间国际规则博弈的中国主张与话语权研究”（项目号：20&ZD204）的阶段性成果。

作者简介：张　华，男，南京大学法学院副教授，主要从事国际公法原理、国际海洋法、网络国际法研究。

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》，《厦门大学学报（哲学社会科学版）》2018 年第 1 期。

② See Open-ended Working Group on developments in the field of information and telecommunications in the context of international security: Final Substantive Report, 12 March 2021, UN Doc. A/AC.290/2021/CRP.2; also Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, 28 May 2021.

年的第五届 UNGGE 进程甚至因为这一问题“无果而终”。可以预料，即使未来联合国框架下的网络空间国际造法进程始终无法就自卫权问题达成共识，各国立场文件对自卫权规则的宣示仍然有可能催生出相关的国际习惯法规则。鉴于国际习惯法的形成构成国际造法的正式路径之一，各国立场文件中有关自卫权的阐述值得思考和深入研究。本文将以各国立场文件为出发点，揭示其中扩大自卫权适用的不良倾向，同时结合相关国际法原理，重点从适用前提、适用时间和适用对象三个方面，对网络空间适用自卫权存在的法律不确定性进行深层次探讨，揭示网络空间扩大自卫权适用的不合理之处，最终服务于中国在网络空间国际造法进程中阐述自卫权适用之立场的需要。

一、各国网络空间立场文件扩大自卫权适用的倾向

在2017年的UNGGE进程中，由于自卫权、反措施和国际人道法在网络空间的适用问题引发了激烈的争议，以致于第五届UNGGE进程最终无法通过报告。网络空间政府间造法进程一度陷入僵局。与此形成鲜明对比，各种半官方和非政府间的网络空间造法进程同期蓬勃发展。其中，北约网络合作防御卓越中心（CCDCOE）特邀国际专家组编写的《网络行动国际法塔林手册2.0版》（以下简称“《塔林手册2.0版》”）于2017年出版，成为网络空间国际造法进程中“专家造法”的典型。[①]

或许是为了摆脱第五届 UNGGE 进程“无果而终”的阴影，又或许是为了响应重新开启的第六届 UNGGE 进程的号召，自 2019 年以来，荷兰、法国、芬兰、新西兰、澳大利亚、德国、瑞士、英国、日本等国陆续发布有关网络空间国际法适用的立场文件，同时爱沙尼亚总统、以色列副总检察长和美国国防部法律顾问以演讲的形式阐明本国有关网络空间适用国际法的最新立场，成为网络空间国际造法进程中备受瞩目的新动向。国家立场文件构成国家实践和法律信念的有力证据，对国际习惯法的形成具有最为直接的作用。[②]因此，在联合国 UNGGE 进程和 OEWG 进程之外，各国试图以发布立场文件的形式对网络空间国际造法进程产生实质性影响——不排除国家立场文件会在这一新兴领域催生出一些具体的国际习惯法规则。

各国立场文件均无一例外地涉及使用武力和自卫权问题，足见自卫权议题实属网络空间国际法适用之焦点。从具体内容来看，各国立场文件以类似措辞表示：判断网络攻击构成国际法上“使用武力”和“武力攻击”的标准为效果标准，亦即网络攻击造成的损害后果如果与传统的动能攻击相当的话，那就可以视为“使用武力”。而只要网络行动在规模和效果方面等同于动能武力攻击的话，那么网络行动就可以构成《联合国宪章》第 51 条意义上的武力攻击，进而产生自卫权。网络空间行使自卫权既可以是网络方式，也可以是动能方式，同时必须遵守必要性和相称性原则。[③]各国立场文件对自卫权适用的表述吸收了此前国际法理论界和实务界的讨论成果，尤其是很大程度上参照了《塔林手册2.0》。虽然总体上表述较为谨慎，但是部分国家也提出了一些扩大网络空间自卫权适用的主张。主要体现为以下三个方面：

（一）网络空间适用“累积性自卫”

由于迄今为止的网络攻击事件均未能达到“武力攻击”的门槛标准，网络空间适用自卫权其实缺乏实践基础。当然，不排除有个别网络攻击事件可能构成使用武力——例如2010年针对伊朗纳坦兹核工厂的“震网”攻击。为尽可能使用自卫权，有一些学者和国家主张“累积性自卫”理论，即单独的网络攻击事件也许不构成武力攻击，但若干网络攻击事件累积起来，可以达到类似武力攻击的程度，进而触发自卫权。这一理论极其危险。法国是迄今唯一在立场文件中明确主

① [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，北京：社会科学文献出版社，2017 年，第 1—3 页。

② [英]马尔科姆·肖：《国际法》，白桂梅等译，北京：北京大学出版社，2011 年，第 65—66 页。

③ See e.g. *Switzerland's Position Paper on the Application of International Law in Cyberspace*, p.4,available at: https://www.eda.admin.ch/dam/eda/en/documents/aussenpolitik/voelkerrecht/20210527-Schweiz-Annex-UN-GGE-Cybersecurity-2019-2021_EN.pdf.

张“累积性自卫”的国家。①

（二）网络空间适用“预先性自卫”

由于恶意代码和数据传输的时间极为迅速，网络攻击的发起和完成几乎是“间不容发”。这一先天性特征似乎预示着预先性自卫(anticipatory self-defence)的适用前提——“迫在眉睫的攻击”(imminent attack)——在网络攻击情境中更加容易成立。迄今为止，网络空间尚未发生现实的武力攻击，却有若干国家在立场文件中过于急切地主张预先性自卫。公然使用“预先性自卫”这一措辞的国家是澳大利亚②和法国③。英国和德国则相对隐晦，虽然并没有在立场文件中公然使用“预先性自卫”这一措辞，但其相关阐述提及“预先性自卫”的适用前提——“迫在眉睫的攻击”。例如，英国表示：考虑攻击之规模和效果的因素包括事实上或预期(actual or anticipated)的伤亡和物理性的财产损害。针对迫在眉睫的（imminent）或正在进行中的武力攻击，可以通过网络方式或动能方式实施自卫权。④德国主张：《宪章》第51条中的自卫权可以针对迫在眉睫的攻击（imminent attack）。这类自卫权同样适用于恶意网络行动。⑤

（三）网络空间自卫权的适用对象包括非国家行为体

迄今为止的网络攻击大多是由非国家行为体发起的。受到“反恐战争”拓展自卫权行使对象的影响，“网络战”讨论中也出现了类似的主张。实际上，网络空间自卫权的行使对象是否包括非国家行为体这一问题一直富有争议。在国际法理论界和实务界尚未形成共识的情况下，有部分国家对此表达了开放的态度。荷兰主张：自卫权适用于国家和非国家行为体。⑥以色列副总检察长施恩多弗（Roy Schöndorf）在阐述以色列有关适用于网络行动的国际法的立场时亦指出：当网络空间使用武力——无论是国家，还是非国家行为体——可以被视为现实或迫在眉睫的武力攻击时，受攻击国可以根据《联合国宪章》第 51 条中的固有自卫权开展行动。⑦

德国和法国虽然支持对特定的非国家行为体——例如ISIS或基地组织行使自卫权，但两国分别从正反两方面表达了对非国家行为体问题的原则性立场。德国以肯定式的措辞表示：非国家行为体的行为可以构成武力攻击。德国曾经就ISIS和基地

① *International Law Applied to Operations in Cyberspace,* 9 September 2019, available at: http://www.defense.gouv.fr/content/download/567648/9770527/file/international+law+applied+to+operations+in+cyberspace.pdf (hereinafter ‘France’s Positon Paper’), para.1.2.2.

② 澳大利亚立场文件中援引总检察长此前有关“anticipatory self-defence”的演讲，主张网络空间同样应适用预先性自卫。See *Australia's Submission on International Law to be Annexed to the Report of the 2021 Group of Governmental Experts on Cyber*, available at: https://www.internationalcybertech.gov.au/sites/default/files/2021-06/Australia%20Annex%20-%20Final%2C%20as%20submitted%20to%20GGE%20Secretariat.pdf (hereinafter ‘Australia’s Positon Paper’), p.3.

③ 法国使用了“preemptive self-defence”这一不太贴切的英文措辞，但从其表述内容来看，法国实质上是在阐释预先性自卫。See France's Position Paper, para.1.2.2.

④ *Application of International Law to States' Conduct in Cyberspace: United Kingdom Statement, 3 June 2021*, available at: https://www.gov.uk/government/publications/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement/application-of-international-law-to-states-conduct-in-cyberspace-uk- -statement (hereinafter ‘UK’s Positon Paper’), p.6.

⑤ *On the Application of International Law in Cyberspace: Position Paper*, March 2021, https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf(hereinafter ‘Germany’s Positon Paper’), p.16.

⑥ *Appendix: International law in Cyberspace , in Letter of 5 July 2019 from the Minister of Foreign Affairs to the President of the House of Representatives on the international legal order in cyberspace*, available at: https://www.government.nl/ministries/ministry-of-foreign-affairs/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace(hereinafter‘Netherlands’Positon Paper’),p.9.

⑦ 以色列副总检察长Roy Schöndorf在美国海战学院2020年12月8日举办的“破坏性科技与国际法”会议上发表主旨演讲，简要阐述了以色列有关适用于网络行动的国际法的立场。See Roy Schöndorf, “Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations”, *International Law Studies*, Vol.97, 2021, p.399.

组织表达过这一观点。[①]法国则以否定式的措辞表示：对于非国家行为体的行为无法直接或间接地归因于一国的，不得针对此类非国家行为体的行为实施自卫权。但在例外情况下，法国针对准国家的武力攻击，可以援引自卫权，例如针对叙利亚境内ISIS的军事干预行动。[②]不过，法国对此问题亦表达了开放式态度，认为“不排除通例会转向承认针对非国家行为体的自卫权”[③]。

就国家战略层面而言，网络空间继陆地、海洋、天空和外空之后，成为极具战略意义的“第五空间”。“网络战”的威胁其实是以美国为首的北约国家集团不断渲染夸大的产物，这些国家的军方将网络空间视为重要的作战场域。但现实情况却是，迄今为止尚无网络攻击严重到“武力攻击”的地步，就连勉强构成“使用武力”的网络攻击都几乎是“乏善可陈”。应对网络攻击的现实需要完全可以通过非武力措施实现，自卫权属于“遥不可及”的“杀手锏”。与此相反，从理论界和实务界的反应来看，“网络战”讨论自20世纪90年代绵延至今，始终将自卫权作为应对网络安全威胁的讨论重点，各国孜孜不倦地谋求以单边军事手段来应对外来网络攻击，难免有舍本逐末之感。这一反差很大程度上是受到了西方国家推动网络空间军事化的影响。[④]在美国“朝前防御”这一进攻型网络安全战略[⑤]的启发下，主要西方国家的网络安全政策军事化色彩不断加重，近期各国立场文件中出现扩大网络空间自卫权适用的倾向不足为奇。

就网络空间国际法的演变而言，近期各国立场文件在网络空间无条件地类推适用物理空间的自卫权规则，甚至引入富有争议的自卫权类型的倾向存在巨大的风险。长期以来，网络攻击能否构成“使用武力”和“武力攻击”一直是国际法理论界和实务界的争论焦点。随着学术讨论的深入和《塔林手册》的出台，学术界的共识逐渐在国家立场文件中“结晶”为效果标准，网络空间适用自卫权的前提条件因此得以一定程度的统一。这一共识可谓各国对日益严峻的网络安全问题的集体法律回应。令人不安的是，部分国家的立场文件无视网络空间自卫权适用前提的法律不确定性，积极主张“累积性自卫”和“预先性自卫”，以及针对非国家行为体的自卫。实事求是地说，在迄今为止网络空间尚无自卫权实践的情况下，过早主张上述自卫权是否合适？以下笔者将就这些方面的法律不确定性进行深入探讨。

二、网络空间自卫权适用前提的法律不确定性

根据《联合国宪章》第51条，自卫权适用的前提是存在“武力攻击”。各国立场文件亦从规模和效果角度考察网络攻击是否严重到“武力攻击”的程度。“规模和效果标准”看似清晰，但本身面临不少解释和适用方面的难题。同时，一系列的网络攻击事件能否累积为“武力攻击”？在网络攻击难以达到“武力攻击”的情况下，自卫权适用前提是否应该向受害国采取武力回应的现实需要妥协——亦即小规模的使用武力亦可以诉诸相称的自卫行动？这些深层次的问题反映出网络空间适用自卫权的前提绝非各国立场文件表面上所显示的那样确定。

（一）“规模和效果标准”的解释与适用问题

从各国立场文件来看，“使用武力”和“武力攻击”的判断标准均为效果标准。就“武力攻击”而言，如果网络攻击的规模和效果严重到“武力攻击”的地步，受害国可以行使自卫权。规模与效果标准看似确定，但仍然存在解释和适用方面的困境。

1. 规模与效果标准是否为现行法？

规模与效果标准源于国际法院在“尼加拉瓜诉美国军事行动案”中的裁决。国际法院区分了“最为严重的使用武力”和“不太严重的使用武力”，前者构成武力攻击，并且在规模和效果方面有别于边境事件。[⑥]但是，国际法院创造的“规模和效果

① Germany's Positon Paper, p.16.
② France's Position Paper, para.1.2.1.
③ *Ibid*.
④ 项登：《全球网络空间军事化问题评析》，《信息安全与通信保密》2018年第1期。
⑤ 根据美国国防部2018年发布的网络战略文件，“朝前防御”（defend forward）战略是指拦截和阻止网络威胁，并通过增强那些支撑国防部任务之计算机系统和网络的安全，美国国防部将反击那些威胁美国军事优势的网络行动。
⑥ *Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. USA),* Merits, Judgment, I.C.J. Reports 1986, p. 14, paras. 191, 195.

标准”并非毫无异议。有不少学者认为，国际法院有关使用武力严重性的区分不无人为之嫌，美国施韦贝尔（Schwebel）法官和英国詹宁斯（Jennings）法官在“尼加拉瓜诉美国军事行动案”中的反对意见，以及国际法学者的批判一定程度地反映了这一点。[①]亦有学者指出，几乎不可能设定武力的门槛标准以界定“武力攻击”这一概念。[②]实际上，国际法院在之后涉及自卫权的裁决中也没有严格坚持“规模与效果标准”。[③]归根结底，规模与效果标准属于国际法理论界和实务界推崇国际法院裁决的产物，充其量只是判断武力攻击的规范性指南，而非现行法。各国立场文件将其奉为圭臬的做法似乎超越了“实然法”。当然，这也不排除立场文件会在此方面促成国际习惯法规则的形成。

2. 效果是否限于物理性后果？

长期以来，“网络战”讨论中一个棘手的问题是：网络攻击的效果评估是否限于物理性后果，抑或还应包括非物理性后果？这一问题一直争论不断。[④]

支持者大多以国家电网、运输、能源、通信、卫生等关键基础设施遭受网络攻击为例，主张非物理性的损害应属于效果标准适用的范畴。例如，有学者认为，关键基础设施的失灵对国家行为能力或居民基本生活条件产生不可立即修复的抑制效果，原则上可以造成必要的破坏性效果，这将成为界定“武力攻击”的理由。[⑤]有学者更是一针见血地指出，产生物理后果本身并非门槛标准，物理后果也并不必然比非物理后果更加严重。物理后果固然因为更加可视和有形而有助于使用武力的判断，但也不能忽视那些导致非物理性后果的网络行动能产生大规模的效果。如果网络行动具有损害目标国生存的直接或间接后果，拒绝将之定性为使用武力是不合逻辑的。[⑥]

从相关国家立场文件来看，大多数国家只是提及物理性的损害后果，所列举的假设性事例也均为造成物理损害的网络攻击。不过，也有个别国家提及非物理性损害。例如，法国在立场文件中主张：如果网络攻击造成大量人员伤亡，或者是重大的物理或经济损害，就应当被归类为“武力攻击”，如网络攻击造成关键基础设施失灵并产生严重后果，或者是可能导致国家活动大面积瘫痪，引发技术或生态灾难，剥夺大量受害者的生命之类的后果，就应当属于这种情况。[⑦]

值得注意的是，荷兰在立场文件中承认：目前，对于未造成人员死亡、物理性损害或破坏，但具有非常严重的非物理性后果的网络攻击能否构成“武力攻击”这一问题，缺乏国际共识。[⑧]这一表述实事求是地反映了非物理性后果在效果评估中的不确定性。

3. 效果是否应考察间接影响和长期影响？

当代国家运行和人类社会的方方面面高度依赖网络和网络化设备。网络攻击一旦发生，其后果往往是攻击者当初无法预料和不可控制的。网络攻击的结果因此具有高度的不确定性和不可预测性。网络攻击的直接后果是指遭受攻击之计算机系统或网络，以及其所控制或互动的系统和设备所承受的不利后果。[⑨]鉴于国家运行和人类社会的高度网络化，网络攻击往往造成间接后果。[⑩]甚至有学者将经济

① See Christian Henderson, *The Use of Force and International Law*, Cambridge: Cambridge University Press, 2018, pp.217–218.

② See Natalino Ronzitti, “The Expanding Law of Self-defence”, *Journal of Conflict & Security Law*, Vol.11, 2006, p.351.

③ 例如，在“石油平台案”中，国际法院并未排除对军用船舶布雷这一行动足以引发自卫权的可能性。See *Oil Platforms* (Iran v. USA), Judgment, ICJ Reports 2003, p. 161, para. 72.

④ 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》，《现代法学》2015 年第 5 期。

⑤ Albrecht Randelzhofer and Georg Nolte, “Article 51”, in Bruno Simma *et al*. (eds.), *The Charter of the United Nations: A Commentary*, Third Edn., Oxford: Oxford University Press, 2012, pp.1419–1420

⑥ François Delerue, *Cyber Operations and International Law*, Cambridge: Cambridge University Press, 2020, pp.297–298.

⑦ France’s Position Paper, para.1.2.1.

⑧ Netherlands’ Positon Paper,p.9.

⑨ See Reese Nguyen, “Navigating *Jus Ad Bellum* in the Age of Cyber Warfare”, *California Law Review*, Vol.101, 2013, p.1098.

⑩ 朱雁新：《数字空间的战争——战争法视域下的网络攻击》，北京：中国政法大学出版社，2013 年，第 78 页。

萧条、社会动乱和政权更迭之类更为间接和长远的影响也视为网络攻击的后果。在讨论制定《塔林手册 2.0》时，有学者认为结果的性质并不重要，后续影响的程度才是关键。这里的典型后续影响，例如针对国家核心功能的网络行动引起严重的国家功能瓦解或对国家稳定的严重和持续后果。[①]如此一来，网络攻击便更有可能被夸大为武力攻击了。

芬兰在立场文件中指出网络空间适用自卫权富有争议的问题之一是：在判断网络攻击是否构成武力攻击时，在何种程度上应考虑攻击的间接影响和长期影响？[②]对此，德国在立场文件中持开放式态度。德国主张：评估网络行动的规模和效果是否严重到将之视为“武力攻击”的程度，这属于在国际法框架下做出的政治决定。物理性财产损害、人员伤亡——包括间接效果，以及严重的领土入侵性属于相关因素。该决定的做出不仅应依据技术信息，而且应评估战略背景，以及网络行动在网络空间以外的效果。[③]德国明确提及“间接效果”和“网络空间以外的效果”，肯定了网络攻击的间接影响和长远影响也属于规模与效果的考虑范畴。这似乎与《塔林手册2.0》中达成共识的“近因标准”相悖。根据“近因标准”，在适用效果标准以评估某一网络行动是否构成武力攻击时，应考虑“一切可以合理预见的网络行动的结果”。[④]一旦无视“近因标准”，将过于间接和长远的影响纳入损害后果的范畴，会导致网络空间自卫权的滥用。

（二）网络攻击的累积效应

由于“武力攻击”的门槛明显高于“使用武力”，在“网络战”的学术讨论中，“事件累积理论”成为主张网络空间适用自卫权的重要依归。“事件累积理论”的意涵是：源于同一主体的一系列“针刺型”（pin-prick）网络攻击单独来看不构成武力攻击，但累积起来会达到武力攻击所需的规模和效果门槛标准，进而触发自卫权。基于“事件累积理论”而产生的自卫权不妨称之为“累积性自卫权”。根据《塔林手册 2.0》第 71 条的评注，国际专家组认为，小规模的网络攻击事件如果是由同一发起人实施，或者由行动协调一致的若干发起人实施，彼此关联，并总体上达到了必要的规模和效果，不排除将这一系列攻击视为“武力攻击”。当然，关键是需要有确定的证据能够证明这些攻击的关联性。[⑤]

“事件累积理论”在近期的国家立场文件中也出现了拥趸。法国明确主张“累积性自卫”，其具体表述如下：“网络攻击孤立来看也许未达到武力攻击的门槛，但如果效果累积达到严重性门槛的话，或者是与构成武力攻击的物理行动一道采取的话，也可以构成武力攻击。这类网络攻击经过协调，并源于同一实体，或者是源于不同的实体但统一行动”。[⑥]对照《塔林手册2.0》第71条的评注部分，可见法国的表述明显受到了《塔林手册2.0》的影响。

“累积性攻击”能否触发自卫权这一问题在国际法上富有争议。国际法院在裁决有关自卫权的案件中其实没有就此问题做出肯定回答，至多只是“闪烁其词”式地提及“累积性攻击”这一情形，但对于此类攻击能否触发自卫权仍然语焉不详。对此，有学者总结道：“迄今为止，国际法院并未对‘累积性攻击’本身是否构成武力攻击做出明确的界定。国际法院的判决表明，小规模攻击的简单叠加不足以转化为能够触发自卫权的大规模累积性攻击。明显存在规避严重性和即时性的风险，国家实践和学者们不太愿意接受事件累积可以构成武力攻击这一主张。”[⑦]另外，从国家实践来看，当美国和以色列主张以遭受“累积性攻击”作为行使自卫权的理由时，往往引发国际社会，尤其是联合国决议的谴责。[⑧]由此可

① 《塔林手册 2.0》，第 345 页。
② *International law and cyberspace: Finland's National Positions*, 15.10.2020,p.6, available at: https://valtioneuvosto.fi/en/-/finland-published-its-positions-on-public-international-law-in-cyberspace.
③ Germany's Position Paper, p.15.
④ 《塔林手册 2.0》，第 345—346 页。
⑤ 《塔林手册 2.0》，第 345 页。
⑥ France's Position Paper, para.1.2.2.
⑦ Albrecht Randelzhofer and Georg Nolte, “Article 51”, pp.1409-1410.
⑧ See Tom Ruys, *'Armed Attack' and Article 51 of the UN Charter: Evolutions in Customary Law and Practice*, Cambridge: Cambridge University Press, 2010, p.169.

见，“累积性自卫”在物理空间尚存在明显的合法性争议，不宜过早地引入网络空间。

究其本质，“事件累积理论”试图在维持“使用武力”和“武力攻击”的区别的基础上，寻求一条中间道路。鉴于网络攻击的隐秘性和私人性，证据获取、攻击溯源和国家归因的难度较大，因此在网络攻击的情境下过于前卫地适用“累积性攻击”理论，难免引发国与国之间的争端。

（三）介于“使用武力”与“武力攻击”之间的网络攻击

自卫权适用的前提在于确定是否存在“武力攻击”。根据国际法院在“尼加拉瓜诉美国军事行动案”中的裁决，网络攻击只有首先构成“使用武力”，然后才有可能构成“武力攻击”。“武力攻击”是在规模和效果方面极为严重的网络攻击。因此，《联合国宪章》第2条第4款“使用武力”和第51条的“武力攻击”之间存在灰色区域。对于那些倾向于采取自卫性军事行动的国家而言，介于“使用武力”和“武力攻击”之间的小规模攻击也有必要采取武力措施进行回应，而不是诉诸非武力性的反措施，因为后者往往无法发挥威慑作用。①

美国和以色列向来淡化“使用武力”和“武力攻击”之间的区别，以为其滥用武力辩护。②在网络空间自卫权方面，美国的立场依旧。2012 年，时任美国国务院法律顾问的高洪柱教授在题为“国际法与网络空间”的演讲中指出，美国长期以来坚持的立场是：自卫权适用于任何非法性的使用武力。不存在有关极度的武力使用构成“武力攻击”，以至于需要采取武力回应的门槛标准。③

但是，从各国发布的立场文件来看，除美国外，所有国家均主张应从规模和效果角度区分“使用武力”和“武力攻击”。这也反映了学术界的主流观点。《联合国宪章》的权威评注指出：《联合国宪章》没有明确禁止小规模的使用武力，并不意味着对此类行为实施自卫权就是被允许的。同样可以认为，《联合国宪章》在自卫权语境中故意没有规定小规模的使用武力，只允许对武力攻击进行回应的自卫，其实已经表达了这样的立场——不允许对小规模的使用武力采取小规模的武力自卫。④高洪柱在演讲中也表示：我们承认，其他一些国家和学者区分“使用武力”和“武力攻击”，并且将触发自卫权的“武力攻击”视为“使用武力”的子集。⑤

如果说“累积性自卫”尚在形式上尊重“使用武力”和“武力攻击”的区别的话，那么蓄意淡化或无视两者区别，进而对小规模使用武力采取军事手段回应将导致滥用武力。有学者试图以相称性原则作为辩解理由，认为可以采取与小规模军事行动相称的武力回应。但是，相称性原则是在自卫权前提条件成立的基础上才能发挥效用，本身并不能为这类滥用武力的行为提供合法性。就必要性原则而言，小规模使用武力即使不能诉诸自卫权，但也至少可以提交安理会讨论，而非动辄使用武力回应。因此，没有必要对小规模网络攻击实施自卫性的军事行动。这种主张只会导致网络空间武力的升级。

三、网络空间自卫权适用时间的法律不确定性

根据《联合国宪章》第 51 条，一国应在遭受武力攻击时行使自卫权。而且按照必要性和即时性的要求，自卫权行使的时间点似乎是明确的。但是，预先性自卫的合法性问题始终困扰着国际法理论界和实务界。网络空间适用自卫权的时间点是否应与物理空间有所不同？抑或更为复杂？部分国家在立场文件中主张网络空间适用预先性自卫，似乎完全忽视了预先性自卫在国际法上的争论，以及网络空间的特殊性。

预先性自卫系针对迫在眉睫的武力攻击而采取自卫行动，在国际法上富有争议。自“9.11 事件”至今，无论是联合国的政治文件，抑或国家实践都显示出预先性自卫的合法性仍然存疑，更勿用奢谈其国际习惯法地位了。⑥然而，德国、法国、英国、

① ［美］沃尔特·夏普：《网络空间与武力使用》，吕德宏译，长春：国际文化出版公司，2001 年，第 39—41 页。
② Christian Henderson, *The Use of Force and International Law*, p.222.
③ Harold Hongju Koh, “International Law in Cyberspace”, *Harvard International Law Journal Online*, Vol.54, 2012, p.7.
④ Albrecht Randelzhofer and Georg Nolte, “Article 51”, p.1403.
⑤ Harold Hongju Koh, “International Law in Cyberspace”, pp.7-8.
⑥ See Christin Gray, *International Law and the Use of Force*, 4th edn., Oxford: Oxford University Press, 2018, p.175.

澳大利亚、美国和以色列在立场文件中却“理直气壮”地主张：一国可以对迫在眉睫的、且具有潜在严重后果的网络攻击行使预先性自卫权。鉴于预先性自卫的“先天不足”和网络攻击的特性，网络空间引入预先性自卫存在以下问题：

首先，预先性自卫极有可能在实践中被滥用为先发制人式自卫。预先性自卫（anticipatory self-defence）经常被混淆为先发制人式自卫(preemptive self-defence)，但两者存在本质不同。预先性自卫针对迫在眉睫的威胁，而先发制人式自卫是指一国针对时间上更为遥远的攻击威胁而行使武力，以防止武力攻击的现实发生。“9.11事件”发生后，先发制人式自卫在小布什政府的《国家安全战略报告》中得到了淋漓尽致的阐释，亦即所谓的“布什主义”。理论上而言，这两个概念不应该发生混淆。但无论是国际法理论界和实务界，抑或是国际法律文件，往往会交替使用这两个概念，以至于这两种截然不同的自卫权经常被混为一谈，或张冠李戴。[①]法国立场文件中使用“preemptive self-defence”来指称“预先性自卫”就是典型例证。可以预料，在网络空间引入预先性自卫，极有可能被某些国家利用为先发制人式军事行动的法律依据。[②]这是网络空间引入预先性自卫的首要法律风险。

其次，预先性自卫最为明显的悖论在于，在网络攻击现实发生之前，如何判断网络攻击在规模和效果上严重到“武力攻击”的程度，并因而需要采取自卫行动？按照上文所述，网络空间自卫权行使的前提是从规模和效果方面考察网络攻击是否足够严重，以至于构成“武力攻击”。在传统的动能攻击中，动能武器潜在的破坏性后果也许可以在获取可靠情报的基础上开展预先评估。网络攻击的后果具有很大的不确定性和不可控性，加之网络攻击先天的隐秘性和情报获取难度大，预先评估其后果不太可行。从上文探讨规模和效果标准的解释和适用问题也可以看出，如果将过于牵强的间接影响和长期影响也纳入后果评估的范围，主张预先性自卫也就显得更加狭隘且脱离现实。更何况在潜在攻击后果不确定的情况下，如何考虑采取必要且相称的自卫行动？是否非武力的方式足够阻止迫在眉睫的网络攻击威胁？

再次，判断网络攻击紧迫性的标准为何？紧迫性的判断标准本身就是有争议的。根据《塔林手册2.0》评注，国际专家组原则上同意预先性自卫亦可以适用于网络空间，理由是对于预期的武力攻击，一国不必任凭对方准备攻击而坐视不理。当武力攻击迫近时，一国就可以行使自卫权。但是，在适用预先自卫权时，专家组存在两种标准之争：即所谓的“将要发生的攻击”标准和“最后可行的机会之窗”标准。前者对预先性自卫施加了相对严格的时间限制。“最后可行的机会之窗”则更加灵活一些，意味着只有在对即将发生的武力攻击进行自卫的“最后机会之窗”出现时，才能实施预先性自卫。[③]无论如何，这两项标准在适用时都存在难以回避的主观性，当事国其实享有较大的自由裁量空间，[④]极易在网络攻击情境中导致自卫权的滥用。

最后，网络空间适用预先性自卫的可行性存疑。姑且不论预先性自卫在国际法上是否存在可靠的法律依据，单就其在网络攻击的情境中如何适用而言，就已经引起了不少质疑。根据以往网络攻击的实例，可能在两种情况下对网络攻击实施预先性自卫：其一，在附属于军事行动的情境中，准备性网络攻击作为传统动能攻击的前奏，预示着传统军事行动迫在眉睫；[⑤]其二，在独立行动的情境中，前期网络攻击预示着另一场可能更具破坏性的网络

① Yoram Dinstein, *War, Aggression and Self-Defence*, 5th edn., Cambridge: Cambridge University Press, 2011, pp.194-195.

② 有学者认为：对目标国家未意识到的网络攻击主张预防性自卫是不可行或不现实的，网络环境中的先发制人自卫将没有任何实际意义。参见[泰]克里安沙克·基蒂猜沙里：《网络空间国际公法》，程乐等译，北京：中国民主法制出版社，2020年，第154页。

③ 《塔林手册2.0》，第351—353页。

④ 有专家认为，“最后可行的机会之窗”的主张依赖一个相当开放的，需要进行解释因而易被滥用的标准。参见《塔林手册2.0》，第353页。

⑤ 例如，2007年以色列在对叙利亚核工厂开展空袭之前，运用网络攻击方式使叙利亚的防空雷达系统无法识别来犯的以色列战机；2008年俄罗斯在开展对格鲁吉亚的军事行动之前，有黑客对格鲁吉亚的政府和银行网站展开了DDoS攻击。

行动迫在眉睫。[①]

在第一种情形中，针对准备性网络攻击实施预先性自卫理论上看似问题不大，但问题在于，是否有确切情报显示网络攻击将伴随着更大规模的军事行动？考虑到在大多数情况下，几乎不太可能识别迫在眉睫的军事行动的整体效果，加上网络攻击具有很强的隐秘性，实际上很难在第一种情形中证立预先性自卫。

在第二种情形中，前期网络攻击预示着后续更严重的网络攻击的紧迫性。前期网络攻击通常通过植入恶意软件来实施。恶意软件的共同特征是以后门有效载荷 (backdoor payload) 的形式允许攻击者在稍后日期访问和控制计算机。除非存在有关后续网络攻击之目的和对象的信息，否则敌对国家植入恶意软件这一行为不能证明随后攻击的时间、类型或严重性。[②]更何况在此情形中行使预先性自卫不符合自卫必要性原则。既然一国已经探知计算机系统中存在恶意软件，那完全可以删除这一软件，大可不必诉诸预先性自卫。根据自卫必要性原则，通过非武力的手段即可消除威胁，当事国又何须“大动干戈”？

当然，上述两种情形都是在假定可以实现国家归因的理想状态下考虑预先性自卫的可行性。实践中，在主张一国应对网络攻击负责时，目标国几乎不可能在网络攻击发生后立即实现归因，更毋庸奢谈在网络攻击尚未发生之前就实现国家归因了。如此，预先性自卫沦为“纸上谈兵”。况且准确的国家归因还取决于证据充分与否。有学者指出：在没有明显迹象时，要令人信服地确立网络攻击的起源、性质、紧迫性，以及反应措施的必要性和相称性是不可能的任务。主张预先自卫的国家至少应就“迫在眉睫的攻击”提供“清晰和令人信服的”证据。[③]当事国在网络攻击的情境中要确保获得“清晰和令人信服的证据”，着实不易。

四、网络空间自卫权适用对象的法律不确定性

传统自卫权适用于国与国之间的关系。但是，过去二十多年以来的“反恐战争”催生出一种颇具影响力的主张——自卫权的行使对象并不限于国家，遭受武力攻击的国家可以对他国境内的非国家行为体行使自卫权。[④]之所以有此主张，很大程度上是因为：一方面，受害国无法将非国家行为体的武力攻击行为归因于领土国；另一方面，领土国又不允许受害国在本国境内武力打击非国家行为体。相应地，受害国试图在国家归因无法奏效或无意开展国家归因的情况下，径自绕开领土国的主权“屏障”，直接针对领土国境内的非国家行为体实施军事行动。一旦无条件地接受这一主张，等于是漠视领土国的主权，同时赋予受害国以无限的自卫权。这一主张大大有利于遭受武力攻击的国家，乃是一种实用主义的态度使然。

在网络空间，绝大多数网络攻击都是由爱国黑客、犯罪团体、恐怖分子之类的非国家行为体实施的。因此，受害国在行使自卫权之前，为避免“殃及无辜”，更加有必要认真对待国家归因问题。但是，和传统动能攻击相比，网络攻击的溯源和归因更加困难。[⑤]网络攻击的隐秘性和瞬时性决定了受害国在搜集证据和识别攻击者身份方面即便不会总是“徒劳无功”，但也很可能是“希望渺茫”。纵使偶尔能够通过技术溯源确定网络攻击者的身份，但在国家归因方面仍然存在不可逾越的法律和事实鸿沟。[⑥]除非有直接证据显示网络攻击者的身份是军事人员或国家机关工作人员，否则作为个体的网络攻击者的行为能否归因于国家尚存在很大的疑问。根据国际法上国家归因的一般规则，通常个人行为只有在受到国家指挥或控制的情形下才可以归因于一国，或者是国家明确将个人行为接受为国家行为，或者是国家授权个人行使政府权力要素。这些规则

① 例如，2010 年伊朗纳坦兹核工厂遭受“震网”攻击就属于类似的情形。尽管这一实践严格意义上不构成“武力攻击”，但表明实践中的确存在这样一种可能：即前期植入恶意软件是为未来某一时间发动一场更加严重的网络攻击做准备。

② 例如，在“震网”攻击事件中，从前期制作恶意软件到最终攻击后果发生大概有两年左右的时间差。

③ Marco Roscini, *Cyber Operations and the Use of Force in International Law*, p.79.

④ See Elizabeth Wilmshurst *et al*., “The Chatham House Principles of International Law on the Use of Force in Self-defence”, *International and Comparative Law Quarterly*, Vol.55, 2006, p.969.

⑤ 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。

⑥ 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。

适用与否取决于证据是否充分。更毋庸讳言有关国家指挥或控制的法律标准在网络攻击情境中尚不确定：究竟是应适用严格的“有效控制标准”，抑或相对灵活的“整体控制标准”？迄今国际法理论界和实务界远未达成一致。①

既然网络攻击的归因难度如此显而易见，自然有不少实用主义者主张非国家行为体可以作为网络空间自卫权的行使对象。学术界的讨论对国家立场文件也产生了一定的影响。诚如上文第一部分所述，荷兰和以色列在立场文件中明确表示可以对从事网络攻击的非国家行为体行使自卫权。法国在坚持国家归因的基础上，原则上反对将非国家行为体作为自卫权的行使对象，但例外允许对ISIS这种近似国家的非国家行为体行使自卫权。德国原则上表示可以对发动网络攻击的非国家行为体行使自卫权，一如其以往对待 ISIS 和基地组织的立场。

非国家行为体对外国的网络攻击行为如果不能归因于领土国的话，本质上应属于执法的范畴。②依据审慎原则，相关国家有义务采取执法措施，以防止或打击其管辖或控制下的非国家行为体的跨境网络攻击行动。③受害国在未获得相关国家同意的情况下，以自卫之名，对后者管辖或控制下的非国家行为体径自使用武力，明显有侵犯他国主权之嫌。出于尊重相关国家主权的需要，受害国的正常反应理当是请求相关国家预防或惩治非国家行为体的不法网络攻击行动。④纵使不能奏效，也只能追究后者因违反审慎义务的国际不法行为责任，动辄使用武力不可取。

值得注意的是，为了论证非国家行为体构成网络空间自卫权的适用对象，近期有西方国家和学者不断主张“不能够或不愿意理论”（unable or unwilling），试图缓和自卫权与主权之间的矛盾，以增强对非国家行为体实施自卫权的正当性。根据该理论，当领土国不能够或不愿意采取措施，以防止其管辖或控制下的非国家行为体发动跨境网络攻击行动时，受害国可以在领土国境内针对非国家行为体行使自卫权。⑤

“不能够或不愿意理论”貌似有理，但毕竟不是现行法。更何况对照一般国际法，该理论既不符合通行的国家归因标准，也不符合自卫必要性原则，同时还存在解释和适用方面的不确定性。⑥领土国不能够或不愿意防止或惩治境内从事跨境网络攻击的非国家行为体，至多违反了审慎原则，没有必要诉诸自卫权，否则无异于要求领土国对其境内发生的一切活动承担绝对责任。这一点在国际法上明显缺乏依据。受害国至多诉诸反措施，而非自卫权。因此，对于西方国家和学者以“不能够或不愿意理论”扩大网络空间自卫权行使对象的危险倾向，国际社会应保持高度警惕。

五、中国关于网络空间适用自卫权的立场表达

中国将网络空间视为国家安全和经济社会发展的关键领域，并将维护网络空间和平与安全、推动构建网络空间命运共同体作为重要的外交使命。

中国近年来一直积极参与联合国框架下的网络空间国际造法进程，始终坚持《联合国宪章》的宗旨和原则——尤其是其中的和平解决国际争端原则和禁止使用武力原则——适用于网络空间，坚决抵制任何试图在网络空间滥用武力的主张。在2017 年的第五届 UNGGE 进程中，中国和俄罗斯、古巴一样对网络空间自卫权、反措施和国际人道法问题持保留态度。2019 年 9 月，中国在向 OEWG 进程提交的立场文件中明确表示：“要审慎对待武装冲突法、诉诸武力法适用于网络空间问题。不应变相承认网络战的合法性，防止网络空间成为新的

① 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。
② 《塔林手册 2.0》，第 347 页。
③ 张华：《论国际法上的审慎原则对网络行动的规制效用——基于<塔林手册 2.0>的思考》，《中国国际法年刊（2018 年）》，北京：法律出版社，2019 年，第 187 页。
④ 在讨论制定《塔林手册 2.0》的过程中，就连那些认为跨境自卫行为合法的专家也认为：受害国应首先要求领土国制止武力攻击行为，也要给领土国以处置相关情况的机会。参见《塔林手册 2.0》，第 349 页。
⑤ See Michael Schmitt and Sean Watts, “Beyond State-Centrism: International Law and Non-state Actors in Cyberspace”, *Journal of Conflict & Security Law*, Vol.21, 2016, p.610.
⑥ 张华：《论网络空间自卫权的行使对象》，《法学论坛》2021 年第 1 期。

战场”[①]。中国对网络空间适用自卫权问题的谨慎态度由此可见一斑。对于近期各国立场文件中扩大自卫权适用的危险倾向，中国在网络空间国际造法进程中可以尝试从以下几个方面进行规范性的立场表达：

（一）抵制网络空间扩大自卫权适用的主张

根据上文有关自卫权适用之法律不确定性的分析，中国在抵制这一不良倾向时可以在国际法技术层面指出：规模与效果标准本身并非国际法上的“现行法”，至多构成评估网络攻击后果严重性的指南。现阶段应避免将非物理性后果、过于间接和长期的影响纳入效果评估范围。针对个别国家淡化或无视“使用武力”与“武力攻击”的主张，应从条约解释角度主张《联合国宪章》第2条第4款中的“使用武力”与第51条中的“武力攻击”之间存在实质性差别。对于“累积性自卫”“预先性自卫”，以及针对非国家行为体的自卫，中国可以指出这些自卫权在动能武力攻击中尚且存在争议，在网络空间争议尤甚，断不可取。

同时，在战略层面，中国还可以指出这些不良倾向的本质和风险：以网络攻击的特殊性提倡引进这些富有争议的自卫权等于是“借尸还魂”，试图利用网络空间国际法规则“混沌不明”的现状，倒逼国际法上诉诸武力的法律向有利于“穷兵黩武”之国家的方向发展。这些富有争议的自卫权类型在过去 20 年的反恐战争中大行其道。事实证明，这非但没有起到维护世界和平与安全的作用，反而导致地区和国际局势更加混乱，沦为北约国家滥用武力的借口。反恐战争的前车之鉴表明：在网络空间应禁止引入这些富有争议的自卫权，以免破坏网络空间的和平属性。

（二）坚持自卫必要性与相称性原则

即使网络攻击构成武力攻击，也并不意味着受害国可以当然诉诸自卫权。自卫权行使受到必要性和相称性原则的限制。具体而言，必要性原则要求自卫措施对于受害国阻止武力攻击是必要的，只有在非武力措施无法奏效或被用尽，且没有其他替代措施的情况下才能最终诉诸自卫行动。必要性很大程度上可以限制对网络攻击行使自卫权。既然自卫是最后诉诸的措施，那么在大多数网络攻击中就无须诉诸自卫权——因为在很多情况下，非武力措施其实完全可以阻止网络攻击。

相称性原则要求自卫措施须与其阻止武力攻击的目的相称。由于自卫措施不具有报复性或惩罚性，不相称的使用武力回应可能构成武力报复。相称性原则因此对自卫行动的规模、范围、强度和持续时间形成限制。[②]当然，相称性并不意味着对等性，亦即自卫措施并不必然要求使用和武力攻击相同的方式。这就意味着，对于网络攻击，既可采取网络方式，亦可采取动能方式行使自卫权。但在有选择余地的情况下，以网络方式行使自卫权可能更加符合相称性原则。

中国可以坚持必要性和相称性原则对网络空间行使自卫权的限制，尽可能压缩自卫权的行使空间。纵使相关国家有行使自卫权的必要，也应优先考虑网络方式，避免造成不相称的攻击后果。

（三）提倡充分发挥联合国安理会的权威职能

根据《联合国宪章》第 51 条的规定，受害国固有的自卫权应尊重联合国安理会的权威。只有在安理会未采取办法之前，受害国才能行使自卫权，并且应立即向安理会报告自卫行动。安理会介入后，受害国不得再行使自卫权。因此，安理会介入与否也是判断自卫必要性的重要考量因素。

理论上，当网络攻击发生时，安理会有权判断网络攻击是否构成对和平之威胁，和平之破坏，抑或是否为侵略行为，并在《联合国宪章》第 41 条或第 42 条框架下通过相关决议，分别授权会员国采取非军事或军事行动。鉴于目前判断网络攻击是否构成武力攻击存在很大的争议，与其让受害国自身，或小型国家利益集团自行界定，还不如由负责维护国际和平与安全的权威机构——联合国安理会——首先做出判断。如果安理会能顺利通过相关决议，授权采取具体行动的话，受害国完全没有必要诉诸自卫权；反之，这也并不妨碍受害国在安理会无法通过决议的情况下，最终诉诸必要与相称的自卫权。从集体应对网络安全威胁的需要来看，提倡联合国

① 《联合国信息安全开放式工作组中方立场文件》，OEWG 官方网站，https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/09/china-submissions-oewg-ch.pdf, accessed on 12 July 2021。

② 《塔林手册 2.0》，第 350 页。

安理会在网络攻击事件中的作用也具有现实意义。

以往网络战的讨论局限于单边诉诸自卫权，完全忽略了联合国安理会集体安全体制的作用。罕见的是，德国立场文件显示出对联合国权威一定程度的尊重，德国主张："评估网络攻击的规模和效果是否严重到足以视为武力攻击的程度，这属于国际法框架下做出的政治决定……此决定不应由恶意网络活动的受害国自由裁量，而是需要依据《联合国宪章》第51条向国际社会——亦即联合国安理会——全面报告。"[①]德国的主张启示：受害国应优先考虑联合国集体安全体制在应对网络攻击方面的作用，切勿径自诉诸单边自卫行动。

中国向来尊重联合国权威。2020年9月18日，中国发布《联合国成立75周年中国立场文件》，主张："安理会要发挥国际集体安全机制作用，承担维护国际和平与安全首要责任……中方坚决反对动辄使用武力或以武力相威胁……任何强制行动都应由安理会授权。"[②]相应地，无论是基于国际战略的考虑，抑或是抑制网络空间自卫权扩大化倾向的需要，中国都可以主张安理会在应对网络攻击事件时发挥建设性的作用，实现网络安全国际规制的多边主义，确保网络空间的和平属性。

[责任编辑：陈慧妮]

（上接80页）特别是中国进行无端攻击和蓄意污蔑，力图通过双重标准和霸权主义色彩鲜明的"两分法"主张，维护其网络霸权地位。这一主张及相关实践，既直接损害网络主权的根本理念，也严重破坏了国际法的权威性与统一性，凸显了网络空间规则博弈和秩序构建的复杂性与紧迫性。

网络主权是中国关于网络空间全球治理和规则制定的核心主张，也是构建网络空间命运共同体、推动网络空间国际规则进程的一个核心议题。以网络间谍国际法规制问题为契机，运用网络主权原则打破"两分法"的掣肘，进而完善网络主权原则的理论体系与实践运用，这为中国更好地参与网络空间国际规则博弈，最大限度地维护本国正当利益提供了动力源泉。

[责任编辑：陈慧妮]

① Germany's Position Paper, p.15.

② 《中国关于联合国成立75周年立场文件》，外交部网站，http://new.fmprc.gov.cn/web/zyxw/W020200910425553975697.pdf。