网络空间累积性自卫的理论解构与因应思考

张　磊*

摘　要：近年来，一些国家和国际组织相继主张网络攻击的累积效果可视同武力攻击。构成武力攻击是合法诉诸自卫权的前提条件，这种由攻击的累积效果触发自卫权的模式被称为累积性自卫。累积性自卫概念包含行为主体的同一性或协同性、攻击行为的关联性、复合义务的追溯性、不法行为的持续性和以效果标准评估是否构成武力攻击等要素。国际法上对累积效果的考察起源于事件累积理论或“针刺理论”，后在《国家对国际不法行为的责任条款草案》第15条“复合行为违反国际法义务”中得以确认，并在“爱尔兰诉英国案”“伊朗诉美国石油平台案”等司法判例中得以应用。国内刑法中的聚合原则为累积性自卫提供了一定法理依据。累积性自卫充分适应网络空间的虚拟性、大多为低烈度攻击和代理人攻击以及关联性攻击等属性，但也具有累积因子的不法性与严重性存在分歧，累积模式采用线性或加权迭加的任择性，累积效果的计量周期与关联性不明，以及模糊、主观的累积门槛等内在缺陷。中国秉持“不鼓励或将冲突合法化”的基本立场，可以从累积性自卫的法律内涵存在较大不确定性，“政治决定”赋予无限自由裁量权，以及违背善意履行国际义务原则与和平解决国际争端原则等三方面，明确反对网络空间自卫权被扩大解释的倾向。

关键词：自卫权　累积性自卫　诉诸武力权　使用武力　网络空间国际法

一　问题的提出

近年来，网络空间国际规则博弈越发激烈，各国围绕“自卫权”等焦点议题展开持续讨论。[①] 2017年，第五届联合国信息安全政府专家组（United Nations Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security）关于自卫权、反措施以及国际人道法适用于网络空间等议题的谈判破裂，未就实质性报告达成一致。[②] 2019

* 张磊，武汉大学国际法研究所博士研究生。本文系2020年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。如无特别说明，本文网络资料的最后访问时间统一为2024年1月30日。

① 在围绕国际法如何适用于网络空间的讨论中，“自卫权”是焦点议题之一。参见王玫黎、陈雨：《论网络空间中的禁止使用武力原则》，载《国际法研究》2019年第4期，第31页。

② 2017年第五届联合国信息安全政府专家组未达成最终报告，参见“Developments in the Field of Information and Telecommunications in the Context of International Security”，https：//www. un. org/disarmament/ict – security/。

年以来，美国、德国、澳大利亚、以色列、荷兰等国分别发表立场文件[①]或以其他形式，[②] 主张在网络空间“移植”适用物理空间极富争议的预先性自卫（anticipatory self-defense）、先发制人的自卫（preemptive self-defense）等概念，法国[③]、新加坡[④]以及北大西洋公约组织（下文简称北约）[⑤] 进一步提出网络攻击的累积效果可视同武力攻击，试图促成自卫权在网络空间的合法化。

目前，网络空间累积性自卫（cumulative self-defense）理论研究尚处于萌芽阶段，相关内容大多是政府立场文件或战略政策，缺乏学理性的深入解释与论证。涉及考察网络攻击累积效果的研究多聚焦于恶意网络攻击的分级分类与针对性反应。例如，尼古拉斯·萨古里亚斯（Nicholas Tsagourias）首次提出“轻微网络挑衅的累积可能会上升到出于自卫目的的武力攻击的程度”，并提醒应当关注低烈度网络攻击背后的基本策略、累积效应以及可能的自卫还击。[⑥] 西科范德梅尔（Sico van der Meer）对小规模网络攻击与战略级网络攻击作出区分，指出“同一行为体在长时间内发起的许多小型网络攻击综合起来可能被视为一种战略威胁”。[⑦] 托比亚斯·利贝特劳（Tobias Liebetrau）强调应该从中观和微观层面对网络攻击作出反应：在中观层面，对长期积累的、相互关联和协调的网络攻击建立战略指导框架；在微观层面，对恶意网络攻击进行分级分类，并明确不同级别反应措施的门槛和触发点（thresholds and trigger points）。[⑧] 这些研究对小规模网络攻击与达到武力攻击门槛的网络攻击作了较为清晰的界定，但对累积性自卫概念的阐述缺乏深入论证。

鉴此，本文拟从跨学科视角明晰网络空间累积性自卫的含义，厘清其概念要素与理论依据，揭示其理论优势与内在缺陷，并尝试基于中国立场提出适当的因应思考，为中国参与网络空间国际规则博弈提供一定的理论支撑。

---

① See Report of the United Nations General Assembly, *Official Compendium of Voluntary National Contributions on the Subject of How International Law Applies to the Use of Information and Communications Technologies by States Submitted by Participating Governmental Experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly Resolution 73/266*, A/76/136, 13 July (2021).

② U. S. Department of Defense, “DOD General Counsel Remarks at U. S. Cyber Command Legal Conference”, https://www.defense.gov/News/Speeches/Speech/Article/2099378/dod-general-counsel-remarks-at-us-cyber-command-legal-conference/; Roy Schöndorf, “Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations”, (2021) 97 *International Law Studies* 395, p. 399.

③ See France Diplomacy, “International Law Applied to Operations in Cyberspace”, https://documents.unoda.org/wp-content/uploads/2021/12/French-position-on-international-law-applied-to-cyberspace.pdf.

④ See Report of the United Nations General Assembly, *Official Compendium of Voluntary National Contributions on the Subject of How International Law Applies to the Use of Information and Communications Technologies by States Submitted by Participating Governmental Experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly Resolution 73/266*, A/76/136, 13 July (2021), p. 83.

⑤ See NATO, “Brussels Summit Communiqué”, https://www.nato.int/cps/en/natohq/news_185000.htm.

⑥ See Nicholas Tsagourias, “Cyber Attacks, Self-defense and the Problem of Attribution”, (2012) 17 *Journal of Conflict & Security Law* 229, p. 231.

⑦ See Sico van der Meer, “Responding to Large-scale Cyberattacks: A Toolbox for Policymakers”, (2022) 7 *Journal of Cyber Policy* 175, p. 176.

⑧ See Tobias Liebetrau, “Cyber Conflict Short of War: A European Strategic Vacuum”, (2022) 31 *European Security* 497, p. 511.

二　累积性自卫的含义与要素

2017 年，澳大利亚发布《网络空间国际参与战略》指出，应当注意反复发生的低级恶意网络行为的累积效果（cumulative effect）对国际和平、安全与稳定的威胁。[①] 在对同年出版的《网络行动国际法塔林手册 2.0 版》（下文简称《塔林手册 2.0 版》）规则 71“对武力攻击的自卫”的评论中，有少数专家指出，由同一发起人（或行动协调一致的若干发起人）实施的相互关联的小规模事件，如果在总体上达到了必要的规模与效果，则可视为一次复合的武力攻击（a composite armed attack）。[②] 这是学术界首次对网络攻击的累积效果进行讨论。2021 年，法国发布《国际法适用于网络空间的立场声明》强调，网络攻击的累积效果达到严重性门槛（threshold of gravity）可能视同武力攻击。[③] 同年，新加坡在其立场文件中也指出，一系列的或协同的网络攻击可能构成武力攻击，即使单个网络行动未达到武力攻击的门槛。[④] 值得注意的是，北约在 2021 年 6 月发布的《布鲁塞尔峰会公报》、2022 年 4 月发布的《网络防御总结文件》以及 2023 年 7 月发布的《维尔纽斯峰会公报》中也申明，重大恶意网络活动的累积效果可能相当于武力攻击。[⑤] 至此，网络攻击的累积效果可视同为武力攻击的观点从学者倡议、少数国家的个体表述扩散到国际组织的确认，政治影响力与国际法示范效应进一步扩大。这种由网络攻击的累积效果触发自卫权的模式，有学者称之为累积性自卫。[⑥]《联合国宪章》第 51 条规定，“联合国任何会员国受武力攻击时，在安全理事会采取必要办法，以维持国际和平及安全以前，本宪章不得认为禁止行使单独或集体自卫之自然权利”。这些国家或国际组织的官方文件虽未明确提及累积性自卫这一概念，但“视同武力攻击”正是诉诸自卫权——禁止使用武力原则的合法例外的重要前提条件。

由上得见，笔者认为，根据法国、新加坡和北约官方文件的表述，网络空间累积性自卫的含义可总结为：一系列由同一实体单独或不同实体协同实施的、针对特定对象的关联性网络攻击，所造成损害的规模与效果达到类似于物理动能“武力攻击”的严重性后果，可能触发《联合国宪章》第 51 条所确认的单独或集体自卫权。

上述定义包含了如下要素：

1. 行为主体的同一性或协同性。可评估由同一实体单独实施的或不同实体协同实施的一系

---

① See Australian Government, *Australia's International Cyber Engagement Strategy*, 2017, p. 45.

② 参见〔美〕迈克尔·施密特等：《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 345 页。

③ See France Diplomacy, “International Law Applied to Operations in Cyberspace”, https://documents.unoda.org/wp-content/uploads/2021/12/French-position-on-international-law-applied-to-cyberspace.pdf.

④ See Report of the United Nations General Assembly, *Official Compendium of Voluntary National Contributions on the Subject of How International Law Applies to the Use of Information and Communications Technologies by States Submitted by Participating Governmental Experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly Resolution 73/266*, A/76/136, 13 July (2021), p. 83.

⑤ See NATO, “Brussels Summit Communiqué”, https://www.nato.int/cps/en/natohq/news_185000.htm; NATO, “Cyber Defence”, https://www.nato.int/cps/en/natohq/topics_78170.htm; NATO, “Vilnius Summit Communiqué”, https://www.nato.int/cps/ru/natohq/official_texts_217320.htm?selectedLocale=en.

⑥ 参见张华：《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》，载《云南社会科学》2021 年第 6 期，第 82 页。

列网络攻击行为的累积效果。协同实施的主体间具有从属关系、合作关系、雇佣关系或资助关系等实质联系。

2. 攻击行为的关联性。单独或协同实施的一系列攻击应具有对象、意图、主体、影响或后果等直接关联性。特殊情况是，如果网络攻击配合构成武力攻击的物理动能攻击同时进行，则无论该（一系列或单独的）网络攻击是否达到武力攻击门槛，都可能触发自卫权。[①] 需要注意的是，一系列攻击行为可能同时发生，也可能具有时间参差性。联合国国际法委员会在对《国家对国际不法行为的责任条款草案》（下文简称《国家责任条款草案》）第 15 条“复合行为违反国际法义务”的评注中强调，复合行为（composite acts）不影响实施行为的时间因素，一系列的作为或不作为可以同时发生，也可以在不同的时间相继发生。[②]

3. 复合义务（composite obligation）的追溯性。《国家责任条款草案》第 15 条的评注提出行为的累积性质构成一种复合义务，“有必要将复合义务与复合行为所违反的简单义务区分开来……如果义务本身是根据行为的累积性质来定义的，那么累积行为构成不法行为的本质是不同的”。[③] 同时，评注强调了复合义务的追溯性，“一旦发生了足够数量的作为或不作为，从而产生了复合行为的结果，则违约行为可追溯到该系列行为中的第一个行为。第一个作为或不作为的地位是模棱两可的，直到发生了足以构成不法行为的系列行为”。[④]

4. 不法行为的持续性。《国家责任条款草案》第 14 条“违背义务行为在时间上的延续”第 2 款规定，有持续性的一国行为违背国际义务时，该行为延续的时间为该行为持续、并且一直不遵守该国际义务的整个期间。[⑤] 若持续性不法行为停止，对复合义务的累积性评估也应终止。《国家责任条款草案》第 14 条的评注指出，如果一项持续性不法行为已经停止，例如释放人质或从非法占领的领土上撤出部队，则该行为被视为今后不再具有持续性，即使该行为的某些影响可能继续存在。[⑥] 但是，若持续性不法行为被打断，并不一定不违反复合义务。国际法委员会认为，一系列作为或不作为被打断，以致从未完成，这一事实并不一定阻止已发生的这些作为或不作为被归类为复合不法行为——如果这些作为或不作为合在一起足以构成违背义务的行为。[⑦]

5. 以效果标准评估是否构成武力攻击。实证主义路径的规模与效果标准（scale and effect），也称“效果标准”，是评估使用武力与武力攻击的主流标准。根据“动能等效理论”，若网络攻

---

① 法国在《国际法适用于网络空间的立场声明》中指出，如果网络攻击与构成武力攻击的物理行动同时进行，则单独进行时未达到武力攻击门槛的网络攻击可以归类为武力攻击，这些攻击必须是协调的，来自同一实体或不同实体的协同行动。See France Diplomacy，“International Law Applied to Operations in Cyberspace”，https：//documents. unoda. org/wp – content/uploads/2021/12/French – position – on – international – law – applied – to – cyberspace. pdf.

② See Report of the International Law Commission，*Commentaries to the Draft Articles on Responsibility of States for Internationally Wrongful Acts*，A/56/10，10 November（2001），p. 149.

③ See Report of the International Law Commission，*Commentaries to the Draft Articles on Responsibility of States for Internationally Wrongful Acts*，A/56/10，10 November（2001），p. 147.

④ See Report of the International Law Commission，*Commentaries to the Draft Articles on Responsibility of States for Internationally Wrongful Acts*，A/56/10，10 November（2001），p. 149.

⑤ See Report of the United Nations General Assembly，*Responsibility of States for Internationally Wrongful Acts*，A/56/83，12 December（2011），p. 4.

⑥ See Report of the International Law Commission，*Commentaries to the Draft Articles on Responsibility of States for Internationally Wrongful Acts*，A/56/10，10 November（2001），p. 140.

⑦ See Report of the International Law Commission，*Commentaries to the Draft Articles on Responsibility of States for Internationally Wrongful Acts*，A/56/10，10 November（2001），p. 149.

击累积造成损害的规模与效果达到动能武力攻击的程度，则可认为网络攻击构成武力攻击。[①] 攻击的效果可以从客观和主观两方面审视：在客观方面，如果破坏程度和伤亡巨大，则使用武力构成武力攻击；在主观方面，国际社会必须承认使用武力是武力攻击。[②]

三　累积性自卫的理论依据

累积性自卫的基础理论模型是军事学或国际政治理论中的“事件累积理论”或“针刺理论”（nadelstichtaktik theory）。事件累积理论曾分别在 1978 年欧洲人权法院“爱尔兰诉英国案”（*Ireland v. The United Kingdom*）、2003 年国际法院“伊朗诉美国石油平台案”（*Islamic Republic of Iran v. United States of America*）中被应用，并在《国家责任条款草案》中得以确认。值得一提的是，事件累积理论与刑法中的聚合原则（the principle of aggregation）也有密切的理论联系。基于军事学、国际政治理论、国际法和国内法的跨学科视角辨析累积性自卫的理论依据，有利于廓清理论缘起与发展脉络，并通过比较分析突出其理论优势。

（一）累积性自卫的理论依据

1. 事件累积理论

事件累积理论在实践中诞生于 20 世纪 60 至 70 年代。[③] 一些国家认为，尽管恐怖组织的每一次恐怖主义行为可能没有上升到触发《联合国宪章》第 51 条自卫权的程度，但恐怖袭击活动的综合后果之和超过了这一门槛。这一理论的核心逻辑是，对一系列不法行为的自卫行为不应通过对孤立袭击的即时反应的有限范围来判断，相反，自卫行为应该被视为对全部后果的回应。[④]

在事件累积理论的基础上，又逐渐衍生出了累积威慑理论（the theory of cumulative deterrence）、累积性网络威慑理论（the theory of cumulative cyber deterrence）等丰富的理论成果。2004 年，多伦·阿尔莫格（Doron Almog）首次提出累积威慑这一概念。[⑤] 累积威慑范式考虑了零星的、短暂的武力爆发，将暴力作为对立双方之间“认知过程”的组成部分。这种间歇性的战略互动旨在引导被威慑方了解威慑方的“红线”。[⑥] 有学者将累积威慑范式引入网络领域，进而提出累积性网络威慑理论以充分适应网络空间大多为低烈度攻击的特点。累积威慑范式并非不切实际地寻求防止网络攻击的发生，相反，它认为某些网络攻击行为不仅是不可避免的，并且通过在很长一段

① 动能等效理论和规模效果论源自《塔林手册 2.0 版》规则 69：如果网络行动的规模和效果相当于使用武力的非网络行动，则构成使用武力。目前规模效果论已成为审视网络攻击是否构成“胁迫”、达到使用武力或武力攻击门槛的主流标准。参见〔美〕迈克尔·施密特等：《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 335 页。

② See Davis Brown, “Use of Force against Terrorism after September 11th: State Responsibility, Self-Defense and Other Responses”, (2003) 51 *Cardozo Journal of International and Comparative Law* 401, p. 410.

③ See Frans Osinga & Tim Sweijs, *Deterrence in the 21st Century—Insights from Theory and Practice* (Springer, 2021), p. 237.

④ Michael McLaughlin, “Deterring the Next Invasion: Applying the Accumulation of Events Theory to Cyberspace”, http://opiniojuris.org/2023/03/02/deterring-the-next-invasion-applying-the-accumulation-of-events-theory-to-cyberspace/.

⑤ See Doron Almog, “Cumulative Deterrence and the War on Terrorism”, (2005) 34 *Parameters* 4, p. 6.

⑥ See Doron Almog, “Cumulative Deterrence and the War on Terrorism”, (2005) 34 *Parameters* 4, p. 6.

时间内反复攻击对手来塑造和限制这些行为，有时甚至与其攻击行为不相称。①

事件累积理论产生于动荡的国际区域环境以及由此形成的“持续交手”的战略文化，最终被视为合法诉诸武力的“政治或法律借口”。正如弗兰克（Thomas M. Frank）所描述的，“自卫概念仍是自私性和侵略性行为的一个方便盾牌……《联合国宪章》第51条的适用正有效且危险地变得不受节制”。②

2.《国家责任条款草案》与司法判例

攻击的累积效果可视同武力攻击这一评估标准的重要依据来自于《国家责任条款草案》的确认和国际法院在“伊朗诉美国石油平台案”、欧洲人权法院在“爱尔兰诉英国案”中的司法判决。《国际法院规约》第38条第1款被广泛承认为关于国际法渊源的最权威和最完全的表述。③该款（d）项规定：在第59条规定之下，司法判例及各国权威最高之公法学家学说，作为确定法律原则之补助资料者。④《国家责任条款草案》作为国际法编纂的一项成果，虽然尚未形成具有法律约束力的文书，⑤但被国际法院、各国政府文件以及学术界广泛援引；司法判例亦是确定法律原则的重要补助资料，二者为累积性自卫理论提供了一定法理支撑。此外，联合国信息安全政府专家组和联合国信息安全开放式工作组（Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security）通过的年度报告中、⑥以及《塔林手册2.0版》等学者倡议⑦和多数国家关于国际法适用于网络空间的立场文件中都已申明，以《联合国宪章》为基础的国际法（包括国家责任法）适用于网络空间。可见累积性自卫理论类推适用于网络空间亦有充分的法理依据。

《国家责任条款草案》第15条“复合行为违反国际法义务”规定：（1）一国通过被一并定义为不法行为的一系列作为和不作为违背国际义务的情事，开始于一作为和不作为发生的时刻，该作为和不作为连同其他的作为和不作为看待，足以构成不法行为；（2）在上述情况下，该违背义务行为持续的时间为一系列作为和不作为中的第一个开始发生到此类行为再次发生并且一直不遵守该国国际义务的整个期间。⑧《国家责任条款草案》第15条的评注指出，“这些行为涉及某种行为的总和（aggregate），而不是单独行为本身”，并强调仅限于严重国际不法行为——“国际法中一些最严重的不法行为是根据其复合性质来定义的”，同时进行了非穷尽式列举，如种族灭绝、种族隔离或危害人类罪的行为、制度性的种族歧视行为、贸易协定禁止的

---

① See Uri Tor, “Cumulative Deterrence as a New Paradigm for Cyber Deterrence”, (2017) 40 *Journal of Strategic Studies* 92, p. 95.

② See Thomas M. Frank, “Who Killed Article 2 (4)？or: Changing Norms Governing the Use of Force by States”, (1970) 64 *The American Journal of International Law* 809, p. 811.

③ See Malcolm N. Shaw, *International Law* (Cambridge University Press, 8th edn, 2017), p. 340.

④ See ICJ, *Statute of The International Court of Justice*, Article 38, para. 1.

⑤ See Maurizio Arcari, “The Future of the Articles on State Responsibility: A matter of Form or of Substance?”, http://www.qil-qdi.org/the-future-of-the-articles-on-state-responsibility-a-matter-of-form-or-of-substance/.

⑥ 联合国信息安全政府专家组和联合国信息安全开放式工作组在多份年度报告中提及。例如参见 Report of the United Nations General Assembly, *Final Substantive Report of Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security*, A/AC.290/2021/CRP.2, 10 March (2021), p. 6。

⑦ 参见〔美〕迈克尔·施密特等：《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116页。

⑧ See Report of the United Nations General Assembly, *Responsibility of States for Internationally Wrongful Acts*, A/56/83, 12 December (2011), p. 5.

系统性的歧视行为等。[①]《国家责任条款草案》强调的复合行为与累积性自卫评估“行为效果的累积”在法律意义上是一致的，因为行为通常具有瞬时性（持续行为是瞬时行为的简单物理组合），只有行为效果才能固化行为的性质。

司法判例也多次提及累积效果与复合义务。在“爱尔兰诉英国案”中，爱尔兰指责北爱尔兰非法对待被拘留者，认为这种做法相当于酷刑或不人道或有辱人格的待遇。欧洲人权法院在判决中表示：“不符合《欧洲人权公约》的做法包括相同或类似的违约行为的累积，这些违约行为数量足够多、相互关联，不仅构成孤立的事件或例外，而且构成一种模式或制度。”[②] 国际法院在“伊朗诉美国石油平台案”的判决中指出，“没有证据表明伊朗在其与伊拉克交战时进行的布雷是专门针对美国的……即使这些事件累积起来，且保留了伊朗的责任问题，但在法院看来，这些事件似乎并不构成对美国的武力攻击。”[③] 需要注意的是，该案并非是旗帜鲜明地反对攻击的累积效果可能构成武力攻击，而是客观地揭示鱼雷对商船造成的损害的累积效果与规模尚且不足以达到武力攻击的门槛。

3. 刑法上的聚合原则

刑法上的聚合原则与国际法关注累积损害的复合义务有密切的理论联系。例如，一名男性一次跟踪女同事回家可能会引起同事的愤怒，但不会违反刑事法规，如果此人多次跟踪同事回家，并发表威胁性言论，给同事造成可能受到身体伤害的合理恐惧，那么不法行为的总和会使系列行为构成跟踪罪。这也被称为规范聚合（normative aggregation），即当两项或两项以上的指控（其单独的规范权重不足以确定责任）被聚合，并且所有指控的组合权重足够时，就会发生这种情况。[④]

刑法上的持续侵害与正当防卫的关系，与各国认定持续的网络攻击构成武力攻击并可合法诉诸自卫权的逻辑基本一致，即持续侵害的危险被评估为“行凶”，类似于网络攻击的累积效果被视同为武力攻击。在一些持续侵害案件中，违法侵害由不同的、但有关联的个人共同实施的系列违法行为组合而成，且持续较长时间。若系统性地、整体地评估这一系列行为，可以认为，受害人所遭遇的持续积累的不法侵害，从质与量的角度看已足以被评估为“行凶”。[⑤] 受害人的反击造成对方死伤的，不能轻言防卫行为“明显超过必要限度”（即比例性），要考虑“累积升高”的不法侵害危害人身安全的严重性，从而肯定受害者的特殊防卫权。对于网络活动而言，如果一系列行为可归咎于一个国家，则规范性聚合可能是适当的。如果国家行为的后果总体上构成违反国际义务，则单独恶意网络活动不必构成独立的不法行为。

笔者认为，聚合原则已经事实上成为一项国际法渊源意义上的一般法律原则。一般法律原则是确定各国法律体系中所共有的法律原则的存在和效力的国际法表现形式，[⑥] 其顺应国际社会的

---

① See Report of the International Law Commission, *Commentaries to the Draft Articles on Responsibility of States for Internationally Wrongful Acts*, A/56/10, 10 November (2001), p. 146.

② See *Ireland v. The United Kingdom*, Judgment, European Court of Human Rights Reports 5310/71 1977, p. 64, para. 159.

③ See *Oil Platforms* (*Islamic Republic of Iran v. United States of America*), Judgment, I. C. J. Reports 2003, p. 192, para. 64.

④ See Michael McLaughlin, “Deterring the Next Invasion: Applying the Accumulation of Events Theory to Cyberspace”, http://opiniojuris.org/2023/03/02/deterring-the-next-invasion-applying-the-accumulation-of-events-theory-to-cyberspace/.

⑤ 参见周光权：《论持续侵害与正当防卫的关系》，载《法学》2017 年第 4 期，第 4 页。

⑥ 〔英〕詹宁斯、瓦茨修订：《奥本海国际法》（第 9 版第 1 卷第 1 分册），王铁崖等译，中国大百科全书出版社 1995 年版，第 21 页。

要求，反映国际社会的本然之理，具有高度的价值共识。[①] 对累积性危险行为的处罚在世界各国的实践中已经普遍存在，[②] 无论是大陆法系国家还是英美法系国家。例如，德国刑法学者洛斯（Loos）将贿赂罪视为“危险行为的累积最终导致侵害”。[③] 在此基础上，1986 年，德国学者库伦（Kuhlen）针对德国《刑法》第 324 条第 1 款“水污染犯罪”首倡了累积犯（Kumulationsdelike）的概念。[④] 日本立法也注重考察有害性的复合积累、重叠和连锁作用，以防止社会发生不可逆转的深刻事态。[⑤] 中国刑法学者认为，两个以上相互独立的行为，单独不能导致结果的发生，但合并在一起造成了结果的发生，应该肯定相互独立的行为与结果直接的因果关系。[⑥] 美国刑法学者范伯格（Feinberg）亦曾提出累积性侵害的概念，强调由群体行为引起的侵害，但群体中的任何个人的行为自身都不足以引起侵害。[⑦] 可见，聚合原则反映了诸多国家保护集体法益的立法、司法和行政方法论以及共同意志，作为构成法律秩序的指导原则，为法律规则的解释与适用确立了方向。在国际司法实践中，如果针对特定事项缺乏既定的规则，一般法律原则可以直接予以适用。[⑧]

（二）累积性自卫的理论优势

根据上文对理论依据的辨析可见，累积效果主要适用于多发的低烈度损害场景，而网络空间与这种评估模式契合度极高。

网络空间具有诸多独特属性，致使物理空间传统的自卫权理论无法有效适应。首先，网络空间具有虚拟性，网络攻击的损害难以度量。恶意行为体发起的网络攻击不具有可视性，无法对违反国际义务的行为直观取证，这与物理空间形成鲜明对比。例如，在 1986 年“尼加拉瓜诉美国军事行动与准军事行动案”（*Nicaragua v. United States of America*）中，国际法院提及，如果攻击“越过国际边界”则可构成武力攻击。[⑨] 网络攻击造成的直接损害通常仅限于计算机及其网络的二进制数据清除或系统暂时失能，而这类损害难以度量。目前国际社会认可程度较高的“近因标准”[⑩] 注重考察网络攻击造成的具有“实质联系”的间接损害，如人员伤亡、经济财产损失等后果，以弥补网络攻击直接损害难以度量的缺陷。其次，网络攻击大多为低烈度攻击、代理人攻击以及关联性攻击。目前存在的网络攻击多是低烈度攻击，[⑪] 能达到使用武力级别的网络攻击极

---

① 黄晔：《论作为国际法渊源的一般法律原则》，载《法律方法》2021 年第 3 期，第 410 页。

② 参见张志钢：《论累积犯的法理——以污染环境罪为中心》，载《环球法律评论》2017 年第 2 期，第 165 页。

③ See Loos, Zum Rechtsgut der Bestechungsdelikte, in: FS – Welzel, 1974, S. 879 und 891f.

④ See Kuhlen, Der Handlungserfolg der Strafbaren Gewasserverunreinigung, GA 1986, 389, 389f.

⑤ 参见〔日〕关哲夫：《现代社会中法益论的课题》，王充译，载赵秉志主编：《刑法论丛》（第 12 卷），法律出版社 2007 年版，第 338 页。

⑥ 参见《刑法学》编写组：《刑法学》（上册·总论），高等教育出版社 2019 年版，第 130 页。

⑦ 参见〔美〕范伯格：《刑法的道德界限——对他人的损害》（第一卷），方泉译，商务印书馆 2013 年版，第 255 页。

⑧ 黄晔：《论作为国际法渊源的一般法律原则》，载《法律方法》2021 年第 3 期，第 415 页。

⑨ See *Military and Paramilitary Activities in and against Nicaragua* (*Nicaragua v. United States of America*), Judgment, I. C. J. Reports 1986, p. 103, para. 195.

⑩ 《塔林手册 2.0 版》中确认了“近因标准”：在适用规模与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”。参见〔美〕迈克尔·施密特等：《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 345 页。

⑪ See Beatrice Walton, “Duties Owed: Low-Intensity Cyber Attacks and Liability for Transboundary Torts in International Law”, (2017) 126 *The Yale Law Journal* 1242, p. 1464.

其有限,[①] 几乎不存在达到武力攻击门槛的网络攻击。同时,网络空间充斥着意图一致、彼此关联的代理人攻击。小泽淳(Jun Osawa)指出,“在过去 10 年中,国家已开始将网络作为服务于其国家利益的手段……可以发现网络攻击经常发生在国际矛盾或冲突事件之后,一些国家为了干涉邻国的内政而发动网络攻击。”[②]

然而,累积性自卫理论通过对持续的低烈度网络攻击造成损害的规模与效果的定性与定量评估,可以有效适应网络空间的虚拟性、损害难以度量、低烈度攻击和代理人攻击以及关联性攻击多发等特性,充分弥补物理空间传统自卫权理论“水土不服”的弊病。除此之外,累积性自卫理论可在一定程度上降低“武力攻击”的适用要求,增强对恶意行为体的拒止威慑(deterrence by denial)。泽夫毛兹(Zeev Maoz)将威慑视为“一种政策——通过这种政策,人们试图拔出剑以吓退潜在攻击者。只要不使用剑,它就会起作用。”[③] 麦克劳克林(Michael McLaughlin)也曾强调了事件累积理论应用于网络空间的意义,“(网络空间)存在着以牺牲国际和平与安全为代价的不断被利用的灰色地带。将事件积累理论应用于此类战役可能会重塑其他国家寻求实施低强度网络战的考量”。[④]

四 累积性自卫的内在缺陷

累积性自卫理论是在物理空间传统自卫权理论优势的基础上发展出的、适应网络空间独特属性的新理论。但这一理论也存在一些突出的内在缺陷,需要进一步完善。

(一) 累积因子:不法性与严重性程度存在分歧

累积因子(accumulation factor)[⑤] 的复合效果达到武力攻击的严重性门槛可能视同武力攻击。然而,各国、国际组织立场以及学界研究对累积因子的严重性程度、不法性存在巨大分歧。

存在扩大解释自卫权倾向的观点认为,任何轻微的、低烈度的网络攻击,只要具备主观伤害的意图,不论是否违反国际义务,都应视作累积因子。但各国对低烈度累积因子的形容略有不同。澳大利亚《网络空间国际参与战略》提出,警惕“反复发生的低级(low-level)恶意网络行

① 2010 年以色列和美国对伊朗核设施发起的震网(Stuxnet)病毒攻击导致伊朗核工业倒退 10 年,被普遍认为是使用武力级的网络攻击。See Andrew C. Foltz, “Stuxnet, Schmitt Analysis, and the Cyber Use of Force Debate”, https://apps.dtic.mil/sti/pdfs/ADA618715.pdf.

② See Jun Osawa, “The Escalation of State Sponsored Cyberattack and National Cyber Security Affairs: Is Strategic Cyber Deterrence the Key to Solving the Problem?”, (2017) 24 *Asia-Pacific Review* 109, p. 113.

③ See Doron Almog, “Cumulative Deterrence and the War on Terrorism”, (2005) 34 *Parameters* 4, p. 7.

④ Michael McLaughlin, “Deterring the Next Invasion: Applying the Accumulation of Events Theory to Cyberspace”, http://opiniojuris.org/2023/03/02/deterring-the-next-invasion-applying-the-accumulation-of-events-theory-to-cyberspace/.

⑤ 累积因子的概念常见于生物医学和环境保护领域,用于计量有害因素的沉积。由于各国、国际组织立场以及学术研究中对应计入累积效果的事件、行为不法性及严重性程度存在分歧,本文拟用累积因子这一概念统摄相关参数,系指一系列不法或未达不法程度的网络攻击中的独立事件、行为。Abdul G. Khan, “Relationships between Chromium Biomagnification Ratio, Accumulation Factor, and Mycorrhizae in Plants Growing on Tannery Effluent-polluted Soil”, (2001) 26 *Environment International* 417, p. 418.

为的累积影响”;[①] 欧洲一些学者表明,“轻微网络挑衅的累积可能会上升到能引发自卫的武力攻击的程度”,[②] 或者“较小的网络攻击单独看起来可能没有那么大的破坏性,但综合起来也可能被视为一种战略威胁”。[③] 然而,低烈度攻击的累积能否构成武力攻击仍存在较大争议。在2005年厄立特里亚-埃塞俄比亚求偿委员会关于“埃塞俄比亚诉诸战争权求偿案”(*Jus ad Bellum-Ethiopia's Claims between the Federal Democratic Republic of Ethiopia and the State of Eritrea*)的1—8号裁决中,委员会认为,两小股部队在边界交火,即使导致人员伤亡,也不构成《联合国宪章》中规定的“武力攻击”。其他一系列事件是相对轻微的事件,它们不具有《联合国宪章》第51条意义上的构成一个国家武力攻击另一个国家的规模。[④] 也有中国学者对低烈度攻击的代数累积表示反对,“一系列轻微攻击的数量总和并不一定在性质上就构成引起自卫权的武力攻击”,[⑤] 即简单的代数迭加无法反映每一例累积因子以及复合行为的性质。

倾向于保守适用自卫权理论的观点主张,具有一定严重性的网络攻击(违反禁止威胁或使用武力原则)才可视为累积因子,以避免合法诉诸武力权被滥用。如北约在《布鲁塞尔峰会公报》中强调“重大恶意累积网络活动的影响”,[⑥] 一些欧洲学者警告应关注“长期积累的对欧洲社会造成重大危害的相互关联和协调的网络行动”。[⑦] 这类观点采用了国际法院在“尼加拉瓜诉美国军事行动与准军事行动案”中对武力性质的区分,最严重的武力形式是《联合国宪章》第51条所指的武力攻击,不甚严重的武力形式是《联合国宪章》第2条第4款的使用武力。[⑧] 根据这一观点,只有每一例网络攻击造成损害的规模与效果达到使用武力门槛,才可进而累积评估其规模与效果是否构成武力攻击。某单一网络攻击行为,即使构成侵犯主权或违背禁止干涉原则,但造成损害的规模与效果低于使用武力门槛,那么根据和平解决国际争端原则和善意履行国际义务原则(下文简称善意原则),都不足以累积其复合义务。

此外,还有一些观点对累积因子性质的认定模棱两可,如法国和新加坡,并未对何种性质和程度的攻击可视作累积因子作出明确限定。但模棱两可的态度或可解释为所有网络攻击(无论规模大小)都可评估其累积效果是否构成武力攻击。

(二) 累积模式:线性或加权迭加的任择性

在数学语境中,常见的累积模式有线性迭加(linear superposition)和加权迭加(weighted superposition),二者各有千秋。累积模式的高度任择性不仅体现在线性与加权模式的选择,也包

---

① Australian Government, *Australia's International Cyber Engagement Strategy*, 2017, p. 45.

② See Nicholas Tsagourias, "Cyber Attacks, Self-defense and the Problem of Attribution", (2012) 17 *Journal of Conflict & Security Law* 229, p. 233.

③ See Sico van der Meer, "Responding to Large-scale Cyberattacks: A Toolbox for Policymakers", (2022) 7 *Journal of Cyber Policy* 175, p. 179.

④ See *Jus ad Bellum-Ethiopia's Claims 1 - 8 between the Federal Democratic Republic of Ethiopia and the State of Eritrea*, Judgment, Eritrea Ethiopia Claims Commission Reports 2005, paras. 11 - 18.

⑤ 参见余民才:《国际法上自卫权实施机制》,中国人民大学出版社2014年版,第235页。

⑥ See NATO, "Brussels Summit Communiqué", https://www.nato.int/cps/en/natohq/news_185000.htm.

⑦ See Tobias Liebetrau, "Cyber Conflict Short of War: A European Strategic Vacuum", (2022) 31 *European Security* 497, p. 511.

⑧ See *Military and Paramilitary Activities in and against Nicaragua* (*Nicaragua v. United States of America*), Judgment, I. C. J. Reports 1986, p. 101, para. 191.

括确定线性跨度（space）或公差（common difference）[①] 以及加权权秩（weight）。这意味着各国在不同网络攻击场景下可以自由选择论辩依据，从而极大增强了政治与法律承诺履行的不确定性。

线性迭加源于迭加原理（the superposition principle），也称为迭加性质，强调对于所有线性系统，两个或多个激励因素（stimuli）引起的净反应是每个激励因素分别引起的反应的总和。[②] 就网络攻击造成损害的规模与后果而言，线性迭加的适用性仅限于经济与金融损失、人员伤亡的统计等，但对于损害的性质与意义无法充分评估。例如，倘若网络攻击造成 6G 科研数据的抹除且无法恢复，如果使用迭加法仅能评估其损失的设备价值和科研成本，无法充分体现其国家级战略意义上的损失。

加权迭加强调不同累积因子的权秩不同，对结果所作贡献也不同。[③] 如果用 W_i（x）表示每一个累积因子的权秩，E_i（x）表示每一个累积因子造成损害的规模与效果，函数 F（x）表示网络攻击的累积效果，则三者关系见如下公式：

$$F(x) = \sum_{i=1}^{n} W_i(x)\, E_i(x)$$

以不同的权秩衡量累积因子的性质与意义，可以有效弥补线性迭加的缺陷。然而不可忽视的是，权秩的赋值具有较强的个体特性、主观性，若仅以加权迭加作为累积模式，亦不能保证评估网络攻击复合义务的客观、公正与公平。

（三）累积效果：计量周期与关联性不确定

累积效果的计量周期（如第一次攻击和持续时间的认定）以及累积因子的关联性（如直接伤害、间接伤害以及长远伤害的评估）仍然存在一定分歧和不确定性。

识别第一轮攻击即是国际法意义上的“第一枪规则”（first shot rule）。战争的触发点是发动或进行战争，这是第一枪规则之适用所固有的行为模式。[④] 远东国际军事法庭把发动战争和进行战争同等对待，认为发动战争就是开始战争，在这个意义上，它涉及实际进行战争。[⑤] 被视为“第一枪”的网络攻击究竟是一系列攻击中的第一例（不论程度与性质，只要具备主观伤害意图即可），还是谨慎限定在达到使用武力门槛的某一例网络攻击，仍然存在较大分歧。就持续时间的认定而言，又涉及对武力攻击“严重性门槛”的评估，其模糊性、主观性与政治性极大阻碍了对最后一例累积因子的确认。国际法委员会在对《国家责任条款草案》的评注中也指出，第 15 条第 1 款将复合行为“发生”的时间界定为最后一个作为或不作为发生的时间，而该作为或不作为与其他作为或不作为合在一起足以构成不法行为，但不一定是一系列行为中的最后一个……作为或不作为必须是一系列不法行为的一部分，但该条并不要求必须实施了一系列完整不

① 线性跨度相当于等差数列中的公差。

② See “Superposition Principle”, https://en.wikipedia.org/wiki/Superposition_principle.

③ 例如有学者提出用加权迭加来评估地震波的影响，每条迹线（trace）的质量不同，其对最终迭加迹线的贡献也不同。更好的迭加方法是在迭加之前根据特定标准对每条迹线进行加权。See Jianyong Xie & Wei Chen, et al., “Application of Principal Component Analysis in Weighted Stacking of Seismic Data”, (2017) 14 *IEEE Geoscience and Remote Sensing Letters* 1213, p. 1215.

④ See Olaoluwa Olusanya, *Identifying the Aggressor under International Law: A Principles Approach* (Peter Lang AG, 2006), p. 57.

⑤ See *Annexed to the Judgement of the International Military Tribunal for the Far East*, Judgment, International Military Tribunal for the Far East Reports 1948, p. 33.

法行为才属于复合不法行为的类别，只要发生的行为数目足以构成违背义务行为。[①]

在评估网络攻击的规模与效果方面，各国在立场文件中都肯定了直接损害的重要意义，但德国、澳大利亚、波兰等国也强调了附带间接损害的不可忽视性，挪威、法国、荷兰、新西兰等国更是存在扩大解释武力攻击门槛的倾向，指出造成严重的经济与金融后果的攻击也可能视同武力攻击。值得注意的是，德国明确提及“网络空间以外的效果”，将网络攻击的长远影响纳入规模与效果的考虑范畴。这似乎与《塔林手册 2.0 版》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”，将过于间接和长远的影响纳入损害范畴，会导致网络空间诉诸武力权的滥用。[②]

（四）累积门槛：模糊性、主观性与政治性

法国、新加坡和北约都强调了武力攻击的严重性门槛，然而“门槛”一词本质上是一种心理预期，是对成本与收益的综合权衡，具有较强的模糊性、主观性和政治性。

门槛的模糊性建构了一种攻击者与受害者之间的动态不完全信息的非合作博弈（non-cooperative game）。非合作博弈是“假定每个博弈者都独立行动，不同任何行为者进行合作，也不同他人进行信息传递”。约翰·豪尔绍尼（John C. Harsanyi）认为，只有义务（协议、承诺、威胁）是有约束力并且可强制执行的，才会出现合作博弈。更进一步，如果博弈者之间形成了有约束力的契约，那么它也应该是一个非合作博弈的结果。[③] 模糊的门槛有利于强化对攻击者的拒止威慑，然而在持续攻击下，受害者通常倾向于不断降低自身承受最大成本的心理底线，最后在反复妥协中可能会导致博弈信誉的丧失从而使威慑效力大打折扣。明确的门槛继承了法律底线思维，显著提升了相关规则的政治和法律约束力。然而攻击者倾向于在严重性门槛下的灰色地带通过各种方式（如转换身份、变更攻击方式与目标等）持续发起进攻性网络行动（offensive cyber operations），并控制累积效果不越过“红线”，使得受害国无法合法诉诸武力，最终相当于“豁免”了国家责任。

严重性门槛的主观判断具有浓重的政治现实主义色彩。法国在立场文件中表示，“针对违反国际法的网络攻击采取的措施并不是系统性的，而是根据自由裁量的政治决定采取的”。[④] 德国在立场文件中强调，“评估武力攻击的门槛是一种政治决定”。[⑤] 北约也重申，“关于网络攻击何时导致援引《北大西洋公约》第 5 条的决定，将由北大西洋理事会根据具体情况作出”。[⑥] 由此

---

① See Report of the International Law Commission, *Commentaries to the Draft Articles on Responsibility of States for Internationally Wrongful Acts*, A/56/10, 10 November (2001), p. 149.

② 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》，载《云南社会科学》2021 年第 6 期，第 86 页。

③ See Drew Fudenberg & Jean Tirole, *Game Theory* (The MIT Press, 1991), pp. 65 – 70.

④ See France Diplomacy, “International Law Applied to Operations in Cyberspace”, https://documents.unoda.org/wp-content/uploads/2021/12/French-position-on-international-law-applied-to-cyberspace.pdf.

⑤ See Report of United Nations General Assembly, *Official Compendium of Voluntary National Contributions on the Subject of How International Law Applies to the Use of Information and Communications Technologies by States Submitted by Participating Governmental Experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly Resolution 73/266*, A/76/136, 13 July (2021), p. 31.

⑥ See NATO, “Brussels Summit Communiqué”, https://www.nato.int/cps/en/natohq/news_185000.htm.

可见，对严重性门槛的判断可能是由这些国家综合权衡国际或地区局势、相互依赖的经贸关系、国家网络实力乃至综合国力对比等因素作出的决定，体现了唯权力论的政治现实主义。

网络攻击“严重性”的标准具有不确定性。根据《联合国宪章》第 51 条，自卫权是由武力攻击所引起的。这一规定表明，达到武力攻击门槛的使用武力应当具有最严重的性质，如造成人员伤亡或重大财产损失。联合国原子能委员会曾把《联合国宪章》第 51 条“武力攻击”门槛具化到“非常严重”这一标准，“在考虑违反条约的问题时，还必须记住，这种违反必须在性质上非常严重才引起第 51 条所承认的自卫权利”。① 环境法和经济法领域的“严重性”强调造成重大资源损失与高额经济成本。环境法领域的“无损害原则”适用于造成严重损害的跨界事件，即对其他国家的人类健康、工业、财产、环境或农业等产生真正的有害影响。② 这种影响必须以事实和客观标准来衡量。“严重性”将取决于价值决定（value determinations）和当时的情况，例如可用的科学证据、人类对某一物体的欣赏以及损害的概率和程度等。③ 美国在反垄断领域特别积极地适用效果理论，对效果理论的经典论述体现在 1945 年“美国诉美国铝业公司案”（*US v. Aluminum Co. of America*）中。在该案中，法院宣布：任何国家甚至可以对外国人在国外的行为施加责任，只要该行为在其边界内产生了受该国谴责的后果。④ 效果理论的适用有两大要件：“必须存在目的”和“效果必须严重”，⑤ 而根据美国法院的标准，“受谴责”是“效果严重”的充分不必要条件。然而，网络空间的虚拟性使“严重性”的界定更加复杂，例如，计算机及其云空间存储的重要数据的价值如何衡量，对一些国家建立的“数据大使馆”以及太平洋岛国提出的“元宇宙国家”的网络攻击是否涉嫌武力攻击甚至侵略，都是需要进一步探讨的问题。⑥

五　对累积性自卫的思考

累积性自卫理论现已在北约元首峰会达成共识，其与日俱增的政治与法律影响力不容忽视。同时，北约合作网络防御卓越中心（Cooperative Cyber Defence Centre of Excellence）主导的《塔林手册 3.0 版》正在紧锣密鼓地研讨、修订和增补中，最迟将于 2025 年经过各国专家讨论、政府代表评议后正式推出。尽管《塔林手册 2.0 版》对少数专家提出的“复合的武力攻击”未达成共识，但经过 8 年的实践发展，尤其在北约元首峰会集体确认的基础上，本轮修订极有可能成为诉诸武力权部分讨论的重中之重。鉴此，有必要在深刻解构的基础上对累积性自卫理论提供适当的法律建议。

---

① See Report of U. N. Atomic Energy Commission, Doc. AEC/18/Rev. I (1946), p. 24.

② See David Keane, “The Innocence of Satirists: Will Caricatures of the Prophet Mohammad Change the ECHR Approach to Hate Speech?”, https://www.ejiltalk.org/the-innocence-of-satirists-will-caricatures-of-the-prophet-mohammad-change-the-echr-approach-to-hate-speech/.

③ See Duncan B. Hollis & Tsvetelina J van Benthem, et al., “Information Operations under International Law”, (2022) 55 *Vanderbilt Journal of Transnational Law* 1217, p. 1265.

④ See *United States v. Aluminum Co. of America et al.*, U. S. Court of Appeals for the Second Circuit - 148 F. 2d 416 1945, p. 443.

⑤ See Malcolm N. Shaw, *International Law* (Cambridge University Press, 8th edn, 2017), p. 689.

⑥ 爱沙尼亚、卢森堡、印度等已建立“数据大使馆”，以协调数据跨境流动和数据本地化问题的分歧；图瓦卢等濒临淹没的太平洋岛国计划建立“元宇宙国家”以应对气候危机。

（一）基本立场

与诉诸武力权相关的国际法问题是目前网络空间最复杂、最敏感、争议最大的问题之一。[①] 不同于西方国家极力促成自卫权在网络空间的合法化，中国素来审慎对待武装冲突法和诉诸武力概念适用于网络空间等问题，杜绝变相地承认网络战的合法性，防止网络空间成为新的战场。[②] 关于现有国际法适用于网络空间的问题，中国始终坚持维护网络空间和平这一大方向，始终以“不鼓励或将冲突合法化”为前提，坚决反对任何鼓励或可能将网络冲突合法化的建议。[③] 同时强调，各国应坚持通过对话合作解决网络争端，共同防范和应对网络攻击，而不是随意降低国家责任门槛，甚至确立带有惩戒性质的国家责任。[④]

累积性自卫同西方国家提出的预先性自卫、先发制人的自卫以及预防性自卫等概念一样，本质上是为其滥用武力、发起网络战编织的冠冕堂皇的借口。鉴此，中国应明确反对存在扩大解释自卫权倾向的累积性自卫理论的适用。

（二）表达内容

1. 法律内涵存在较大不确定性

西方国家仅提出累积性自卫的理论框架，未对其法律内涵作出明确澄清。笔者认为，累积性自卫的法律内涵存在较大不确定性，主要体现在四个方面。

第一，可累积的网络攻击事件或行为的不法性或严重性程度存在分歧。在实践中极易出现任何低烈度网络攻击甚至尚未构成侵犯主权的网络攻击（即未造成明显损失的轻微攻击）都被累积到复合效果中。

第二，对网络攻击事件或行为采取线性迭加抑或加权迭加的累积模式具有任择性，可能出现违反国际义务的国家采取简单代数迭加以压缩累积效果，而受害国主张加权迭加以强化不法性和国家责任的情形。反之亦然，义务违反国可能采取加权迭加并对每一例事件或行为赋予较低权秩以压缩累积效果，而受害国采取线性迭加并赋予较大线性公差以强化不法性与国家责任。

第三，可累积的网络攻击事件或行为的计量周期和关联性存在争议。一些国家可能追溯到较长时间跨度前的网络攻击，同时合并参考其造成损害的非合理预期的规模与效果。

第四，武力攻击的“严重性门槛”具有模糊、主观的特性，虽有利于法律规则灵活、弹性地适用，却也显著限制了对累积终点的有效评估。概念中不确定的法律内涵势必引发规则适用的分歧与争端，不仅不能抑制滥用武力，反而可能使情势更加复杂。

---

① 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。

② 参见《联合国信息安全开放式工作组中方立场文件》，联合国裁军事务厅网站，https：//unoda - web. s3. amazonaws. com/wp - content/uploads/2019/09/china - submissions - oewg - ch. pdf。

③ 参见中国代表团在联合国信息安全开放式工作组首次会议上关于国际法适用的发言，联合国裁军事务厅网站，https：//documents. unoda. org/wp - content/uploads/2021/12/Statement - of - China _ ICT - OEWG - 7th - plenary - meeting_ international - law_ DEC - 16 - AM_ CHN. pdf。

④ 参见中国代表团在联合国信息安全开放式工作组首次会议上关于国际法适用的发言，联合国裁军事务厅网站，https：//documents. unoda. org/wp - content/uploads/2021/12/Statement - of - China _ ICT - OEWG - 7th - plenary - meeting_ international - law_ DEC - 16 - AM_ CHN. pdf。

值得一提的是，对累积模式的选择和对累积效果的评估在具体实践中也有走向“情境主义路径”的可能性，即是以效果标准为主，结合个案分析和情境分析进行定量与定性的综合判断。[①] 如德国、芬兰、罗马尼亚、挪威、新西兰、美国等国强调结合事件背景、行为体身份、攻击目标、意图等进行个案分析。[②] 对此，笔者认为，中国或可主张在进行个案分析时，目前至少可以考虑严重性、即时性和直接性三项因素，其他更为宽泛的因素（如军事性和国家参与）在国家归因环节再加以考虑。但必须强调的是，这些因素只具有指导性意义，不具有法律约束力。[③]

2. “政治决定”赋予无限自由裁量权

德国、法国以及北约等指出，判断是否构成武力攻击是一种根据具体情况自由裁量的政治决定，即无论在法律层面是否构成武力攻击，国家都可根据对国际形势、权力格局等因素的评估作出是或否的判断。这是典型的以政治凌驾法律、违背国际契约精神的观点。以政治决定判断武力攻击就等于变相地承认受害国享有无限的自由裁量权，使之可以无视目前国际法上关于归因、国家责任等法律框架，并根据法律以外的因素进行归因和判断。这种做法不能也不可能实现国际法意义上的关于国家责任的目标。[④]

3. 违背善意原则与和平解决争端原则

对每一例网络攻击事件或行为（尤其是几乎未造成损失的轻微攻击）进行累积势必塑造紧张的、“有怨必报”的国际政治气氛。在国际争端的解决中，无视善意原则与和平解决争端原则将使相关讨论变得毫无意义，甚至不断侵蚀和破坏各国艰难构建的国际法律体系。鉴于有关累积事件或行为的不法性与严重性程度的认定存在分歧，对所有网络攻击不加区分地进行累积，违背了《联合国宪章》等确认的善意原则以及和平解决国际争端原则。同时，有可能间接促进累积性反措施、累积性反报等惩戒性理论的生成，一定程度上会在国际社会制造持续紧张的敌对政治气氛，进而促进网络空间的军备竞赛。[⑤]

质言之，累积性自卫理论存在显著的扩大适用自卫权的倾向，中国应审慎对待、密切关注其理论与实践发展，尤其应在《塔林手册 3.0 版》制定进程或联合国信息安全开放式工作组等政府间多边进程中充分表达中国立场，防止其发展成为一项习惯国际法规则。

六　结语

当前，各国围绕“自卫权”等焦点议题的讨论进展缓慢，难以达成共识。在这一背景下，西方国家针对网络攻击大多为低烈度攻击、代理人攻击以及关联性攻击等特性，提出了适应网络空间“本土特质”的累积性自卫理论，希冀寻求自卫权如何适用于网络空间的折衷主张。然而，

① 参见张华：《网络空间适用禁止使用武力原则的法律路径》，载《中国法学》2022 年第 2 期，第 296 页。

② See Report of the United Nations General Assembly, *Official Compendium of Voluntary National Contributions on the Subject of How International Law Applies to the Use of Information and Communications Technologies by States Submitted by Participating Governmental Experts in the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security established pursuant to General Assembly Resolution 73/266*, A/76/136, 13 July (2021).

③ 参见张华：《网络空间适用禁止使用武力原则的法律路径》，载《中国法学》2022 年第 2 期，第 301 页。

④ 参见田立：《论恶意网络行动归因中对“控制”标准的法律解释和适用》，载《武大国际法评论》2023 年第 3 期，第 56 页。

⑤ 参见焦园博：《论军民融合趋势下网络武装冲突适用区分原则》，载《国际法研究》2023 年第 4 期，第 60 页。

累积性自卫目前仍然仅是一个理论框架，其法律内涵尚待澄清。究其本质，累积性自卫与预先性自卫、先发制人的自卫等概念一样，是西方国家为其在网络空间滥用武力张目的“皇帝的新衣”。中国在参与《塔林手册3.0版》等学者倡议或联合国信息安全开放式工作组等多边讨论进程时，或可从法律内涵的不确定性、“政治决定”的无限自由裁量权以及违背善意原则与和平解决争端原则等三个方面阐明立场，警惕累积性自卫扩大解释自卫权的倾向，同时呼吁就累积性自卫的理论与实践发展进行深入讨论，以维护网络空间的和平、安全与繁荣。

Theoretical Deconstruction and Practical Response of Cumulative Self-Defense in Cyberspace

Zhang Lei

Abstract: In recent years, some countries and international organizations have proposed that the cumulative effects of cyber attacks can be considered as an armed attack. Constituting an armed attack is a prerequisite for legitimate recourse to the right of self-defense, and this model of self-defense triggered by the cumulative effects of attacks is known as “cumulative self-defense”. The theory of cumulative self-defense has elements such as the identity or synergy of the actors, the correlation of attack behavior, the traceability of composite obligations, the continuity of unlawful behavior, and the evaluation of whether it constitutes an armed attack based on effectiveness standards. The research of cumulative effects in international law originated from the theory of event accumulation or nadelstichtaktik theory, which was later confirmed in Article 15 of *the Draft Articles on the Responsibility of States for Internationally Wrongful Acts*, which states that composite acts violate international legal obligations, and applied in judicial precedents such as *Ireland v. United Kingdom* case and *Iran v. United States* case. The principle of aggregation in domestic criminal law has actually become a general principle of law in the sense of international law resource, providing some theoretical basis for the theory of cumulative self-defense. This theory fully adapts to the virtual nature, low intensity attacks, multi-agent attacks, and multi-correlation attacks of the cyberspace, but it also has inherent shortcomings such as the divergence of illegality and severity of accumulation factors, the selectivity of linear or weighted superposition of cumulative modes, the unclear measurement period and correlation of cumulative effects, and the ambiguity, subjectivity, and political nature of cumulative thresholds. Based on the basic position of the Chinese government that “does not encourage or legalize conflicts”, it may be clarified from three aspects. There is significant uncertainty in the legal connotation of this theory. Besides, “political decision-making” grants unlimited discretion. The theory goes against the principles of good faith and peaceful resolution of international disputes. We need to clearly oppose its tendency to expand the interpretation of the right of self-defense.

Keywords: The Right of Self-defense, Cumulative Self-defense, *Jus ad Bellum*, Use of Force, International Law in Cyberspace

（责任编辑：郝鲁怡）