网络空间中的反措施

陈徽，朱莉欣，安东尼奥·科科（Antonio Coco），
弗朗索瓦·德勒吕（François Delerue）

网络空间国际法中欧专家工作组（EWG-IL），研究小组成果报告（2024）

Geneva Centre for Security Policy
Maison de la paix
Chemin Eugène-Rigot 2D
P.O. Box 1295
1211 Geneva 1
Switzerland
Tel: + 41 22 730 96 00
Contact: www.gcsp.ch/contact
www.gcsp.ch

ISBN: 978-2-88947-023-5（中文版）
ISBN: 978-2-88947-019-8 (English)

关于合作组织

中国现代国际关系研究院

中国现代国际关系研究院（CICIR）是一个历史悠久、研究领域宽泛、功能齐备的复合型国际战略与安全问题研究及决策咨询机构。研究领域覆盖全球所有地区和重大战略性、综合性问题。中国现代国际关系研究院现有研究、行政和辅助人员 300 余人，下设 15 个研究所、若干研究中心以及若干部门。长期开展广泛、深入、高端的国际学术交流，是博士、硕士学位授予单位，主办发行《现代国际关系》、Contemporary International Relations 和《国家安全研究》三本学术期刊。

欧盟“网络直通车”

欧盟“网络直通车”-欧盟网络外交倡议（EU Cyber Direct – EU Cyber Diplomacy）支持欧盟的网络外交和国际数字参与，以加强基于规则的网络空间秩序，并建设具有网络韧性的社会。为此，欧盟“网络直通车”开展研究，支持合作国家的能力建设，并促进多利益攸关方的合作。通过研究和活动，欧盟“网络直通车”定期参与讨论打击网络犯罪和加强全球刑事司法系统的国际合作之未来。

日内瓦安全政策中心

日内瓦安全政策中心（GCSP）是一个旨在促进全球合作、安全与和平的国际基金会。该基金会受瑞士政府支持，由 55 个成员国管理。日内瓦安全政策中心提供了一种独特的 360° 方法来了解和解决全球挑战。该基金会的使命是培养人才，促进对话，通过内部研究提供建议，集思广益，并联合专家制定可持续的解决方案，以建设一个更加和平的未来。

厦门大学

厦门大学创办于 1921 年，长期被列为中国顶尖大学之一。厦门大学设有研究生院、6 个学部以及 33 个学院和 16 个研究院，拥有近 44000 名全日制学生以及 3000 多名专任教师和研究人员，其中有 32 人是中国科学院或中国工程院的成员。

背景

本报告源于一项重大研究和对话项目：中国现代国际关系研究院（CICIR）、欧盟“网络直通车”、日内瓦安全政策中心（GCSP）和厦门大学联合召集的网络空间国际法中欧专家工作组（EWG-IL）。中欧专家工作组旨在搭建一个平台，以支持中欧法律专家共同研究国际法在网络空间的适用问题。研究小组工作的主要目标是为选定的专题提供更深入的分析，并确定中欧之间的共识与分歧，为一轨和一轨半对话进程中的政策讨论创造一个更多以结果为导向与信任驱动的环境。

作者

陈徽，武汉大学网络治理研究院院长助理、助理研究员，数学与统计学院博士后

朱莉欣，西安交通大学科教院网络安全法治研究所所长

安东尼奥 · 科科（Antonio Coco），埃塞克斯大学法学院副教授（高级讲师）

弗朗索瓦 · 德勒吕（François Delerue），西班牙IE大学法学院助理教授

致谢

本中文报告系由英文翻译而来，译者是厦门大学法学院网络空间国际法研究中心童润琪和杨帆，荷兰莱顿大学罗杰 · 克里莫斯（Rogier Creemers）对中译报告做了复核。原报告的欧方合作者得到欧方瑞士外交部赞助，欧方代表非常感谢瑞士外交部的慷慨支持。报告全体作者对审稿人杨帆和利斯 · 维胡尔（Liis Vihul）的建设性反馈和宝贵见解表示感谢，他们的专业知识为本出版物的质量做出了积极贡献。

目录

1. 反措施的概念及其在网络空间中的可适用性

“反措施”一词一般指为对抗或抵消另一行为而采取的措施，[1]它在多个学科中得到了广泛运用，如法律、国防、医学、工程、污染预防和网络安全等领域。[2]然而，具体到国际法中，反措施[3]一词有其独特含义。在过去的一个世纪里，“反措施”逐渐在概念上取代了“报复”（reprisal）。[4]1978 年法美《航空服务协定》仲裁案（Air Services Agreement case）[5]的仲裁庭最早使用了“反措施”一词；国际法院（ICJ）则是在1980年德黑兰人质案（Tehran Hostages case）[6]中首次使用这一术语。

国际法委员会（ILC）于 1949 年将“国家责任法”列为研究专题，[7]并于 2001 年发布了最终版的《国家对国际不法行为的责任条款草案》（ARSIWA）。[8]在编纂有关国家责任的习惯国际法的过程中，国际法委员会花费了大量精力来明确反措施规则以及其它重要原则，例如关于国家行为的归因规范。尽管《国家对国际不法行为的责任条款草案》并未就反措施提出明确定义，但国际社会目前已基本形成广泛共识，认为国际法中的反措施是指一国为应对另一国的不法行为而采取的单边应对举措，这些措施在正常情况下通常是不法的，却因存在特定条件（作为对在先的他国国际不法行为的回应）而得以合法化。

即使过了二十多年，反措施仍然是国际法委员会有关《国家对国际不法行为的责任条款草案》工作中最具争议的内容之一。[9]一方面，反措施有其公认的价值，即在一个缺乏中央权威来维护各国合法权益进而确保国际法得到普遍遵守的国际社会中，它为各国提供了一种维护己方权益和恢复国际秩序的自助手段。另一方面，反措施兼具一定风险，即可能被强国所利用，方便为其开展有争议行动提供口实。国际法委员会的旧任国家责任特别报告员詹姆斯·克劳福德（James Crawford）曾指出，“反措施，尤其是集体反措施，在国际法中仍然存有很大争议，部分原因是因为其与国际关系中的强权政治和‘炮舰外交’的历史息息相关。”[10]

即便如此，本研究小组的中欧专家一致认可并强调反措施在现有国际法框架下依然应当发挥重要作用，均认同反措施是一项牢固确立的习惯国际法制度，可一般性适用于网络

1 A. Stevenson (ed), “Countermeasure”, Oxford Dictionary of English (3rd edn.), Oxford University Press 2015.

2 F. Delerue (2020) Cyber Operations and International Law, Cambridge, Cambridge University Press, p. 434.

3 On countermeasures, see, generally: C. Leben, “Les contre-mesures inter-étatiques et les réactions à l’illicite dans la société internationale” [1982] Annuaire français de droit international 9; O.Y. Elagab, *The Legality of Non-Forcible Counter-Measures in International Law* (Oxford University Press 1988); E. Zoller, *Peacetime Unilateral Remedies: An Analysis of Countermeasures* (Transnational 1984); L.A. Sicilianos, *Les réactions décentralisées à l’illicité: des contre-mesures à la légitime défense* (LGDJ 1990); C. Focarelli, *Le contromisure nel diritto internazionale* (Giuffrè 1994); Y. Matsui, “Countermeasures in the International Legal Order” [1994] The Japanese annual of international law 1; D. Alland, *Justice privée et ordre juridique international: étude théorique des contre-mesures en droit international public (A Pedone 1994); M. Noortmann, Countermeasures in International Law: Five Salient Cases* (Gadjah Mada University Press 2005); M.E. O’Connell, *The Power and Purpose of International Law: Insights from the Theory and Practice of Enforcement* (Oxford University Press 2008); J. Crawford, A. Pellet and S. Olleson (eds), *The Law of International Responsibility* (Oxford University Press 2010) 1127–1214; J. Crawford, *State Responsibility: The General Part* (Cambridge University Press 2013) 684–712.

4 M. Noortmann, *Enforcing International Law: From Self-Help to Self-Contained Regimes* (Ashgate 2005) 35; O’Connell (n 3) 233.

5 *Air Service Agreement of 27 March 1946 between the United States of America and France* (1978) 18 RIAA 417.

6 *United States Diplomatic and Consular Staff in Tehran (United States of America v Iran)* (Judgment) [1980] ICJ Reports 3, 27–28 para 53.

7 ILC (International Law Commission) (1949) “Survey of International Law and Selection of Topics for Codification”, Yearbook of the International Law Commission, 1, pp. 279, 281; Crawford, 2013, pp. 35-44.

8 ILC (International Law Commission) (2001) “Articles on Responsibility of States for Internationally Wrongful Acts”, adopted at the fifty-third session, annexed to UN General Assembly Resolution 56/83, 12 December, A/56/49(Vol I)/Corr4.

9 Crawford, 2013, p. 675.

10 Ibid., p. 684.

空间。因此，一国通过数字化手段在网络空间针对他国不法行为采取的行动，如作为对等回应的黑客攻击或破坏网络系统的行动，均可被认定为网络空间中的反措施。然而，中欧专家亦承认，反措施即使在网络空间也存在被滥用的可能性，因此需要通过明确实体上和程序上的严格要求，以确保其得到妥当适用。

在进一步讨论中，针对目前网络空间是否已自动允许各国采取反措施，中欧专家持有不同看法。

欧方专家认为，作为一般规则，除非另有更具体规定，习惯国际法当然地适用于国家在网络空间中的各项行为，[11]其中自然包括作为习惯国际法的反措施的相关法律规定。在此基础上，国际法委员会在《国家对国际不法行为的责任条款草案》中所总结出的反措施须遵循的相关实体和程序要件，构成了可以默认适用于网络空间的法律规则，它们为防止反措施被滥用提供了重要保障。

中方专家更倾向于另一种理解方式，强调反措施由一套互相紧密联系的规则所组成，涉及许可使用和限制使用之间所保持的复杂与微妙的平衡，2001 年通过的《国家对国际不法行为的责任条款草案》正是国际社会历经多轮谈判后，对其所应保持的平衡状态达成的基本共识。因此中方专家认为，相比于仅表面上确认反措施中各项规则的适用，更重要的在于确保这一制度框架内的每一条规则都能在实质上得到谨慎遵守，并能在网络空间发挥与在传统情形下等同作用，也只有此时网络空间中的反措施才是被允许的。[12]换言之，中方专家观察到，除非对许可使用和限制使用反措施的平衡状态形成了新的共识，否则只有在国家采取反措施的自由程度与防止其在网络空间被滥用所需的限制之间保持同传统情形下基本一致的平衡下，网络空间的反措施才可谓被自动允许。然而，对于在网络空间中各要件如何得以适用，各国目前仍存在争论，因此尚不清楚前述平衡是否、能否保持，以及会否产生新的共识而作出调整。这意味着，目前很难对是否已自动允许各国在网络空间采取反措施给出明确的答案。中方专家强调，根据以上判断，各国未来可以通过明确网络空间适用反措施的要件来促进在网络空间澄清被允许的反措施的样貌。

从实践的角度看，目前从国际法角度发表的有关反措施如何适用于网络空间的立场声明主要源于发达国家，这些声明通常包括受害国针对不法行为采取反措施的可行性。[13]相较而言，区别于发达国家多倾向于为反措施争取许可，发展中国家似乎对此表现担忧，当前在网络空间明确阐述反措施的要件，特别是那些需遵守的限制性要件上还存有较大难度，因此他们尚不愿公开认可网络空间反措施的可行性。例如，在明确对国际法如何适用于网

11 D. Akande et al. (2022) “Drawing the Cyber Baseline: The Applicability of Existing International Law to the Governance of Information and Communication Technologies”, International Law Studies, 99, pp. 4-36.

12 中方专家举了“电子签名”为例进行说明。在判定是否允许在数字环境下使用电子签名时，通常采用功能等同原则。即只有当电子签名能够通过一定的技术手段识别签名者的身份和意图，从而实现与传统手写签名相当的功能时，才被视为具有与传统手写签名相同的法律效力。因此，只有像在联合国国际贸易法委员会《电子签名示范法》中定义的“可靠电子签名”，以及欧盟《电子身份认证和信任服务条例》（eIDAS）中定义的“合格电子签名”才默认被法律认可。”

13 CCDCOE (NATO Cooperative Cyber Defence Centre of Excellence) “Countermeasures”, Cyber Law Toolkit, https://cyberlaw.ccdcoe.org/wiki/Countermeasures.

络空间发表了立场或意见的国家中，伊朗[14]、哈萨克斯坦[15]、肯尼亚[16]、巴基斯坦[17]以及非洲联盟均在网络反措施问题上保持了沉默。此外，巴西似乎对反措施在网络空间的适用持批评态度，甚至质疑国际法委员会当年有关反措施的编纂可能超出了习惯国际法的范畴。[18]

基于这一背景，中方专家结合中国实践，指出各国能否在联合国框架内进行普遍且平等的谈判，以明确界定在网络空间适用反措施的各项要件，[19]尤其是明确那些应当施加一定限制的要件，如强化和平解决国际争端的原则的适用和作用、限制虚假归因等，[20]或将直接影响与中国类似的一众发展中国家对待反措施适用于网络空间的立场与态度。

回溯 2001 年，中国政府在评论《国家对国际不法行为的责任条款草案》时，总体上还是承认了反措施在国际法中所具有的特殊地位的，但也同时指出：“反措施必须伴随对其使用的适当限制，以在承认反措施的合法性和防止其滥用之间取得平衡”。[21]然而，2017 年，中国出于反措施可能在网络空间遭到滥用，连同网络空间军事化等可能加剧国家间冲突情形的担忧，强烈反对在 2017 年联合国信息安全政府专家组（UNGGE）报告中纳入涉及网络反措施的相关内容。[22]尽管如此，鉴于中国当前有着反制外国制裁，包括但不限于网络制裁的迫切需要，《中华人民共和国反外国制裁法》中所罗列的一些反制措施实际上会需要以国际法中的反措施作为理论依据进而提供合法性辩护。[23]因此，中国不太可能完全反对在网络空间适用反措施。事实上，中国也已不再对网络空间适用反措施表示强烈反对，而是保持某种微妙的沉默；因此，相信中国会欢迎国际上加深对网络空间反措施，特别是其中限制性要件的讨论，同时对可能产生的过度解读与发展保持警惕。

鉴此，中欧双方专家一致认为，接下来有关反措施适用于网络空间的实体和程序要件的深入探讨具有重要意义。

14 Iran (2020) “General Staff of Iranian Armed Forces Warns of Tough Reaction to Any Cyber Threat”, NOURNEWS Analytics & News Agency, https://nournews.ir/En/News/53144/General-Staff-of-Iranian-Armed-Forces-Warns-of-Tough-Reaction-to-Any-Cyber-Threat.

15 UNGA (UN General Assembly) (2021) “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”, UN Doc A/76/136, pp. 51-52.

16 Ibid., pp. 52-54.

17 Pakistan (2023) “Pakistan’s Position on the Application of International Law in Cyberspace”, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/UNODA.pdf.

18 United Nations General Assembly (n 15) 21.

19 China (2021) “China’s Positions on International Rules-making in Cyberspace”, https://documents.unoda.org/wp-content/uploads/2021/12/Chinese-Position-Paper-on-International-Rules-making-in-Cyberspace-ENG.pdf; China (2017) “International Strategy of Cooperation on Cyberspace”, Xinhua, 1 March, http://www.xinhuanet.com//english/china/2017-03/01/c_136094371.htm.

20 A.E. Levite et al. (2022) “Managing U.S.-China Tensions Over Public Cyber Attribution”, Carnegie Endowment for International Peace, 28 March, https://carnegieendowment.org/research/2022/03/managing-us-china-tensions-over-public-cyber-attribution#a-chinese-perspective-on-public-cyber-attribution.

21 State Responsibility: Comments and observations received from Government, A/CN.4/515, 2001, p.82.

22 Permanent Mission of the People’s Republic of China to the UN (2017) “Statement by Counsellor Sun Lei of the Chinese Delegation at the Thematic Discussion on Information and Cyber Security at the First Committee of the 72nd Session of the UNGA”, 23 October, http://un.china-mission.gov.cn/eng/chinaandun/disarmament_armscontrol/unga/201710/t20171030_8412335.htm.

23 例如，“查封、扣押、冻结在中国境内的动产、不动产和其他各类财产”以及“禁止或者限制中国境内的组织和个人与其进行有关交易、合作等活动”等的措施，可能与中国在WTO规则或其他双边或多边贸易和投资协议下的国际义务相冲突。因此，反措施可以为采取这类措施提供合法性辩护。相关中文学术论文可参见：张辉，《单边制裁是否具有合法性：一个框架性分析》，《中国法学》，2022年第3期，；霍政欣，《<反外国制裁法>的国际法意涵》，《比较法研究》，2021年第4期。

2. 对网络活动采取反措施的实体要件

一般国际法中确立的反措施的实体要件不仅是为一国明确了可以采取反措施的情形，同时也是对其在采取反措施的过程中必须遵守的限制的规定。这些要件依旧适用于网络活动。

2.1 在先国际不法行为

中欧专家一致认为，只有出现在先的国际不法行为后，国家才有权针对其采取反措施。[24]国际法中的反措施从概念上而言本质上是被动的，不能主动采取，不能作为预先式、预防式或先发制人式地应对（可能、未来或者即将发生的）国际不法行为的依据。

根据此基本原则，造成损害并非判断国际不法行为存在的必要条件。中欧专家一致认为，缺少物理损害并不妨碍国家采取正当的反措施。然而，欧方专家指出，物理损害结果的缺失可能会对评估必要性和相称性产生影响。中方专家补充认为，鉴于国际社会对网络空间中国际不法行为的构成要件尚未达成明确共识，在实际损害发生之前采取反措施更容易引发争端和冲突。

正如国际法委员会所承认的，国家在采取反措施时需要自担风险。中欧专家一致认为，如果一国对在先的行为的不法性判断失误，该国需为其实施的不法反制行为承担责任。[25]仅凭善意坚信国际不法行为在先存在是不够的——必须存在客观上事实性的在先国际不法行为，否则一国针对先前行为所采取的反措施将无法获得正当性，导致其本身是不法的。[26]

欧洲各国在这一问题上的国家立场相当明确，在采取反措施之前，准确的归因和有着正当的反制理由至关重要。[27]对于欧方专家而言，为合法实施反措施所设计的严格的实体和程序要件，正是为了防止滥用。如果一国未能满足这些要件，其采取的反制行为将构成国际不法行为，需自行承担相应责任。

中方专家则指出，若网络空间在先的国际不法行为的存在仅仅依靠一国自行判断，可能存有反措施被滥用的巨大风险。[28]因此，作为实施反措施的必要前置步骤的归因，尚需要进一步的检视和研究，以限制诸如基于虚假指控发起的反措施（只是有关归因的讨论超出了本研究报告的范围，便未再做进一步探讨）。

---

24 "Fundamental prerequisite" per ARSIWA Commentaries Art 49, p. 130, § 2. See *Gabčíkovo-Nagymaros Project* (Hungary/Slovakia) [1997] ICJ Rep 7, 55, para 83; *Naulilaa* (Portugal v Germany) (1928) 2 RIAA 1011, 1027; *Cysne* (Portugal v Germany) (1930) 2 RIAA 1041, 1057. See also Delerue (n 2) 438.

25 ARSIWA Commentaries Art 49, p. 130, § 3.

26 F. Paddeu (2015) "Countermeasures", Max Planck Encyclopedia of Public International Law, para. 18, https://opil.ouplaw.com/display/10.1093/law:epil/9780199231690/law-9780199231690-e1020.

27 Estonia (2019) "President of Estonia: International Law Applies Also in Cyberspace", 29 May UNODA (United Nations Office for Disarmament Affairs) (2021) "Official Compendium of Voluntary National Contributions on the Subject of How International Law Applies to the Use of Information and Communications Technologies by States", A/76/136, August, p. 73.

28 Chinese Delegation to the Open-ended Working Group on ICT Security (2021) "Statement at the Seventh Plenary Meeting on the Application of International Law", 16 December, https://documents.unoda.org/wp-content/uploads/2021/12/Statement-of-China_ICT-OEWG-7th-plenary-meeting_international-law_DEC-16-AM_CHN.pdf.

2.2 反措施的目的

中欧专家一致认为，反措施在国际法中作为一种工具性手段，其目的在于制止国际不法行为并促使责任国履行赔偿义务，而非惩罚责任国。反措施的核心目标是恢复受害国与责任国之间的正当法律秩序。如果反措施成功促使了责任国终止不法行为并履行赔偿义务，受害国即应终止反措施。[29]

事实上，根据《国家对国际不法行为的责任条款草案》第 49 条第 1 款，受害国仅能采取反措施以促使责任国履行该条款第二部分的义务，包括终止正在进行的不法行为并向受害国提供赔偿。因此，反措施是一种强制各国遵守国际法的工具，其重点在于恢复法律秩序和纠正不法行为，而非实施报复。[30]

2.3 反措施的对象

根据《国家对国际不法行为的责任条款草案》第 49 条第 1 款和第 2 款，反措施只得针对责任国，不得针对第三方。[31]仅在受害国与实施在先国际不法行为的责任国之间，反措施才能起到排除不法性的作用。[32]

然而，这并不意味着反措施不会对第三国或其他第三方产生附带影响。例如，中止贸易协定可能会间接影响责任国的贸易方，从而导致相关企业亏损甚至破产。在某些情况下，这种间接影响可能难以避免。[33]问题在于，反措施对第三国和其他第三方的间接影响是否应纳入相称性的评估范围。欧方专家倾向于将其纳入考虑；中方专家则认为，鉴于网络空间无边界特征所带来的扩散效应和放大效应，需强化限制，强调受害国在选择应对措施时，应优先采取对其他国家造成附带影响最小的措施，或者尽可能采取必要手段减轻潜在的附带影响。

中欧专家一致认为，如果有害的网络行动源自第三国（例如位于第三国境内的受控僵尸服务器），受害国只有在声称该第三国实施了国际不法行为的情况下，才能对其采取反措施。例如，若第三国未能履行其审慎义务，致使其领土或其控制下的基础设施被用于侵犯其他国家的权利，即可能构成国际不法行为。[34]此时，在满足相关实体性和程序性要求的前提下，受害国可以对该第三国采取反措施。

如若不然，采取反措施的国家要对实施在先国际不法行为的责任国以外的国家造成的损害负责。如果反措施损害了第三国的权利，受害国——同时也是反措施的实施国——将因违反其对第三国的国际义务而承担责任，[35]其有义务终止相关不法行为，提供不再实施的

29 ARSIWA Commentaries Art 49, pp. 130-131, § 7.

30 ARSIWA Commentaries Art 49, p. 130, § 1. In this sense, among other states: New Zealand, The Application of International Law to State Activity in Cyberspace, 1 December 2020, 3.

31 ARSIWA Commentaries Art 49, p. 130, § 4.

32 ARSIWA Commentaries Art 22, pp. 75-76, § 5, citing *Cysne* (n 22) at 1055-1056) and *Gabcíkovo-Nagymaros Project* (n 22), p. 55, para. 83.

33 ARSIWA Commentaries Art 49, p. 130, § 5. In this respect, it must be noted that, per Denmark's national position, this 'does not necessarily exclude that actions may in some circumstances be directed against non-State actor as part of countermeasures.' See Government of Denmark, "Denmark's Position Paper on the Application of International Law in Cyberspace"(4 July 2023).

34 *Corfu Channel* (United Kingdom v. Albania), Judgment, 9 April 1949, ICJ Reports (1949) 4, at 22.

35 Paddeu, 2015, para. 41.

保证，并提供赔偿。而且在这种情况下，因该国际不法行为而受到损害的各个国家都有权根据自身所受损害的程度，采取与之相称的反措施。

2.4 禁止的反措施

中欧专家一致认为，根据《国家对国际不法行为的责任条款草案》第 50(1)(a)条，反措施不得达到使用武力的程度。国际法委员会已有指出，实施反措施需遵守禁止使用武力原则，这一规定得到了大量文献和司法判决的广泛支持。许多国际法律文书也明确阐述了该原则，例如《关于各国依联合国宪章建立友好关系和合作的国际法原则宣言》。[36]无论所涉国际不法行为的严重程度如何，受害国都不能援引反措施来为其使用武力的行为开展合法性辩护，即使反措施系通过网络手段实施。[37]中方专家指出，将反措施限制在武力门槛之下，对于防止其被滥用特别是被用作军事干预手段尤为重要。

中欧专家还指出，《世界人权宣言》第 50 条规定了一些不能假借反措施之名而中止的义务，其中包括保障基本人权的义务。中方专家指出，尽管国际法没有明确定义基本人权，但可将这些人权理解为涉及《世界人权宣言》所规定的生命权、自由权和安全权的核心部分。[38]网络空间出现的一些有关网络人权的探讨与诠释可能会给传统人权带去新的理解，[39]或可能足以成为一项新的人权（例如，网络言论自由可以被认为是自由权或更具体的言论自由权的又一新表现形式），[40]或作为某种附带权利促进基本人权的实现。[41]然而，网络空间是否已有出现新型人权且达到单独成为基本人权的地步仍值得怀疑。在此方面，专家们特别审议了各方热议的“互联网接入权（right to internet access）”，但认为至少从现阶段的国家实践来看，由于该权利在特定情况下仍不时受到限制，因此很难说其已构成一项基本人权。

欧方专家指出，根据国际法委员会对这一问题的相关评论，其所讨论的基本人权似乎是那些在紧急情况下不能被削弱、或对生存至关重要的权利。[42]因此目前而言，若要说基本人权包括互联网接入权，多少还是有些牵强的。值得一提的是，任何克减人权的反措施都还必须尊重必要性和相称性才有可能是合法的。

中欧专家进一步指出，《国家对国际不法行为的责任条款草案》第 50 条还列出了其他一些不能通过反措施中止的义务。这些义务包括禁止报复的人道主义义务[43]、一般国际法强制性规范（强行法）下的义务[44]、以及为保护外交或领事代表、房舍、档案和文件不

36 ARSIWA Commentaries Art 50, p. 132, § 5. Citing *Corfu Channel*, (n 32) at 35; and Military and Paramilitary Activities in and against Nicaragua, p. 127, para. 249. See, e.g., Security Council resolutions 111 (1956) of 19 January 1956, 171 (1962) of 9 April 1962, 188 (1964) of 9 April 1964, 316 (1972) of 26 June 1972, 332 (1973) of 21 April 1973, 573 (1985) of 4 October 1985 and 1322 (2000) of 7 October 2000. See also General Assembly resolution 41/38 of 20 November 1986.

37 M. Roscini (2014) Cyber Operations and the Use of Force in International Law, Oxford, Oxford University Press, pp. 105-107; H. Lahmann (2020) Unilateral Remedies to Cyber Operations: Self-Defence, Countermeasures, Necessity, and the Question of Attribution, Cambridge, Cambridge University Press, p. 130; Delerue, 2020, pp. 442-443.

38 UNGA (United Nations General Assembly) (1948) “Universal Declaration of Human Rights”, Article 3.

39 E.g. it could be argued that freedom of online speech could be a new manifestation of the right to liberty and of the right to freedom of expression.

40 E.g. a right to internet access.

41 E.g. a right to cybersecurity, which could more fully safeguard the right to liberty and security.

42 ARSIWA Commentaries Art 50, p. 132, §§ 6-7.

43 ARSIWA Commentaries Art 50, § 8, p. 132.

44 ARSIWA Commentaries Art 50, pp. 132-133, § 9.

可侵犯而制定的义务[45]。这一规定确保了即使在实施反措施期间，国际法的基本原则和规范仍应予以维护。

此外，受害国和责任国之间必须遵守可适用的争端解决程序所规定的义务，以确保相关争端解决程序得到遵守并发挥公正、有效地解决争端的作用。[46]在一些特别法体系中，反措施也可能被特别禁止，例如欧盟法和世界贸易组织的法律体系内均一般性禁止采取反措施。[47]

2.5 必要性和相称性

《国家对国际不法行为的责任条款草案》第 51 条规定，除需满足必要性之外，[48]针对国际不法行为采取的反措施还必须是相称的。 这意味着反措施应与所遭受的损害和在先国际不法行为的严重程度相当。相称性需要从定量（所遭受的损害）和定性（如所保护的利益和被侵犯的义务的严重程度）两个方面进行评估。[49]相称性还需要考虑各有关权利，包括受害国的权利、责任国的权利、以及其他相关国家的立场。[50]普遍认为，在对反措施的相称性进行评估时，往往需要做大致估算。[51]国际法委员会指出，相称性要求是确保反措施合法且不会不必要地加剧冲突的关键。[52]

中方专家指出，在实践中如何确定反措施的相称性仍然是一个有争议的问题，因为在结合不同的定性和定量判断时很难进行有效比较，即使按照国际法院在加布奇科沃-大毛罗斯项目案（Gabčíkovo-Nagymaros Project case）等案件中采用的标准，具体运用于实践中仍然不够明确。

中欧专家一致认为，反措施并非只允许不履行与在先国际不法行为所违反义务相同或与之密切相关的义务。[53]采取反措施甚至可能意味着可以不履行多项义务。[54]一些国家已经承认，针对网络行动的反措施可以采取非网络形式，而网络形式的反措施也可以用于应对非网络环境下的不法行为。[55]

中欧专家均指出，采取“同类（in-kind）”反措施——即不履行与被指控的责任国违反义务相同或密切相关的义务，可能更容易确定其相称性。[56]然而，中方专家提醒，这一立场也还值得进一步审视。即使“同类”反措施施加的实际损害相当，不同国家对损害的感知程度也是有所不同的。例如，对网络发达国家和欠发达国家而言，同样导致互联网服

45 ARSIWA Commentaries Art 50, pp. 133-134, §§ 14-15.

46 ARSIWA Commentaries Art 50, p. 133, §§ 12-13.

47 Paddeu, 2015, para. 22. See Article 55 ARSIWA on the point.

48 ARSIWA Commentaries Art 51, p. 135, § 7.

49 ARSIWA Commentaries Art 51, p. 135, § 6.

50 ARSIWA Commentaries Art 51, p. 135, § 6. See also Paddeu (2015) para 23.

51 *Air Service Agreement* (n 5), 443 para. 83.

52 ARSIWA Commentaries Art 51, p. 135, § 7.

53 ARSIWA Commentaries Art 22, pp. 75-76, § 5, *Cysne* (n 22) at 1055-1056) and *Gabcíkovo-Nagymaros Project* (n 22), p. 55, para. 83. See also ARSIWA Commentaries p. 129, § 5.

54 ARSIWA Commentaries Art 49, p. 130, § 6.

55 “Countermeasures” (*International cyber law: interactive toolkit*, 20 May 2024) https://cyberlaw.ccdcoe.org/wiki/Countermeasures accessed 9 June 2024. See e.g. the positions of Canada, Germany, Italy, Japan, Norway, Sweden, Switzerland, the United Kingdom, and the United States.

56 Air Service Agreement, 1978, p. 443, para. 83

务中断的网络攻击带来的影响截然不同，因此它们可能针对同类被违反的义务采取不同的反措施以确保相称性。考虑到责任国未必会对违反同类义务抱有类似程度的被侵害感，理解这一点将尤为重要。例如，中英两国在面对同样侵犯网络主权的行为时，中国作为一个高度重视网络主权的国家，采取的应对方式很可能完全不同于不认可网络主权构成一项约束性规则的英国。归根结底，为敦促责任国纠正其不法行为，反措施所施加的压力源于责任国对损害的感知与认知程度而非实际损害本身。采取“同类（in-kind）”反措施只是为讨论符合相称性原则的思路提供了一个方便参考的起点，而不是解决问题的终点。

欧方专家指出，相称性可以确保反措施不超过必要限度，旨在促使责任国履行其义务，而非施加惩罚。中方专家则强调，反措施应限于为恢复责任国与受害国之间的法律关系所必要的范围。从这个角度来看，在评估相称性时，重点应侧重于反措施是否足以实现其恢复正当法律秩序的目标，而不是判断其是否足以施加同等的伤害。

2.6 暂时性与可逆性

中欧专家一致认为，反措施是一种促使责任国终止国际不法行为并履行赔偿义务的工具。因此，反措施必然应当是暂时性的，其效果也必须“尽可能”可逆。[57]使用“尽可能”这一措辞意味着，在可以选择多种合法有效的反措施时，受害国应优先采取那些能够在实现目的后恢复履行被中止的相关义务的措施。[58]

57 Arts 49(2-3), and 53 ARSIWA.

58 ARSIWA Commentaries Art 49, p. 131, § 9.

3. 对网络活动采取反措施的程序要件

《国家对国际不法行为的责任条款草案》第 52(1)(a)条规定，在采取反措施之前，受害国应当要求责任国终止在先的国际不法行为并履行赔偿义务，这种事先沟通有时被称为“催告”（sommation），已经得到了普遍实践和相关司法判决的支持。这一程序要求具有某种绝对性，因为第 52 条规定的减损情形不包括其在内，因而可以确保责任国拥有做出行为纠正的机会，进而允许其得以终止在先的不法行为并提供赔偿，避免争端升级。[59]虽然在实践中具体如何遵守这些规定存在争议，但中欧专家都认为，这一程序要件应适用于与网络行动有关的反措施，以确保被指控的责任国意识到其行为的不法性并有机会纠正它。

3.1 优先诉诸争端解决程序

在讨论中，对于在采取反措施之前是否应优先诉诸“任何”可用的争端解决程序，中欧专家产生了分歧。

欧方专家遵循国际法委员会在《国家对国际不法行为的责任条款草案》中的立场。根据第 52(1)(b)条的规定，在实施反措施之前，通常只需先提议谈判。此外，第 52(3)条要求，如果国际不法行为已经停止，且争端正在由有权作出具有约束力裁决的机构审理，则应中止反措施或避免采取反措施。这一规定旨在确保反措施是暂时性的，同时尊重司法程序的权威。然而，根据第 52(4)条，如果责任国未能真诚参与争端解决程序时，受害国又将得以继续采取反措施，这一规定旨在防止争端解决程序被不当滥用为阻碍采取反措施的工具，鼓励各方为解决争端而做出真正实际的努力。

相比之下，中方专家的立场倾向于更进一步，其认为第 52(1)(b)条中之所以规定在采取反措施之前，“受害国应将采取反措施的决定通知责任国并提议与该国进行谈判”，核心目的是鼓励优先通过争端解决程序和平解决争端（毕竟提议谈判总归是一项相对简单易行的和平解决争端的努力）。然而，鉴于越来越多的国家主张，在将反措施适用于网络空间时，应对某些程序要件进行调整，尤其是在紧急情况下排除第 52(1)(b)条的适用。对此，中方专家基于本报告第一部分中提出的保持许可与限制间平衡的观点，建议进一步强化第 52(1)(b)条后半部分的要求，以弥补在紧急情况下，免除事前通知义务可能导致的程序性限制不足。中方专家据此指出，强化后的限制应当是在责任国实施在先的国际不法行为后，受害国应优先诉诸“任何”可用的争端解决程序，而非直接采取反措施来解决争端。这一观点并不要求当事国穷尽尝试所有可用的争端解决程序，而仅要求做出必要的努力以防止争端加剧的方式和平解决争端。这一主张之所以具有可行性，是因为提议谈判始终是一种简单且可以普遍适用的争端解决方法，即使在紧急情况下也不会必然减损需要发起的紧急反措施的有效性。[60]

59 ARSIWA Commentaries Art 52, p. 136, §§ 4-5.

60 C. Tomuschat (1994) “Are Counter-measures Subject to Prior Recourse to Dispute Settlement Procedures?”, European Journal of International Law, 5, pp. 84-87.

3.2 事先通知的要求

在将反措施适用于网络空间时，事先通知（采取反措施的决定）的程序性要求仍然适用。这一要求是促使责任国自行纠正其错误行为并推动双方秉持善意和平解决争端的必要步骤。考虑到网络活动的溯源难度，事先通知还为各方提供了进一步澄清事实、避免误判的机会。

根据《国家对国际不法行为的责任条款草案》第 52(1)(b)条，采取反措施的国家必须将其决定通知责任国，并提出与该国进行谈判的意向。针对该条的评注指出，这一规定为责任国提供了在反措施实施之前履行其义务的又一次机会。[61]

受害国没有义务具体说明其计划或拟采取的反措施，尽管做出更具体的说明可能会更有效地促使被指控的责任国履行义务。[62]

值得指出的是，《国家对国际不法行为的责任条款草案》第 52(1)条第(a)款和(b)款提及的两种通知之间并无固定的时间顺序，这意味着二者可以同时进行，也可以在时间上前后接近。[63]

3.3 紧急反措施

根据《国家对国际不法行为的责任条款草案》第 52(2)条，在必要时，受害国可以采取紧急反措施以维护其权利，这也构成了第 52(1)(b)条规定的通知义务的例外。此种情况下，受害国无需事先通知被指控的责任国，也无需提出谈判要求。然而，这一例外不能免除第 52(1)(a)条受害国“催告”责任国终止其在先国际不法行为，并要求赔偿损害的程序性要求，因为这是合法实施反措施的基本程序。

“紧急”一词既涉及实质性判断，也涉及程序性判断。然而，对于网络情形下何谓“紧急”，相关讨论和共识仍然有限，因此在程序上如何适用“紧急反措施”仍缺乏定论。欧方专家认为，“免除事先通知”适用于为保障受害国权利而采取紧急反措施的情形，它既是为保障受害国在实质争端中受到侵犯的权利，也是为保障受害国得以顺利采取反措施的权利。[64]具体而言，如果事先通知可能减损反措施的预期目标，例如可能泄露反措施所依赖的机密方法或影响实施反措施的能力，那么受害国可以在不通知责任国的情况下直接采取紧急反措施。由于在网络情形下，威胁可以迅速出现并快速造成严重损害，因此只要紧急反措施能够符合必要性和相称性要求，并且在紧急情况解除后及时终止并向责任国追发通知，这种措施就可以是正当的。一些国家已明确支持该规则适用于与网络行动相关的反措施。[65]

61 ARSIWA Commentaries Art 52, p. 136, § 5.

62 Paddeu, 2015, para. 27.

63 ARSIWA Commentaries Art 52, p. 136, § 5.

64 ARSIWA Commentaries Art 52, p. 136, § 6.

65 Costa Rica (2023) “Position on the Application of International Law in Cyberspace”, 21 July, pp. 4-5, § 14;Netherlands (2019) “International Law in Cyberspace”, 26 September, pp. 7-8;France (2019) “International Law Applied to Operations in Cyberspace”, 9 September, pp. 7-8;Israel (2020) “Israel’s Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations”, 8 December;UNODA (United Nations Office for Disarmament Affairs) (2021) “Official Compendium of Voluntary National Contributions on the Subject of How International Law Applies to the Use of Information and Communications Technologies by States”, A/76/136, August, p. 73;Sweden (2022) “Position Paper on the Application of International Law in Cyberspace”, July, p. 6;UK (United

中方专家也认为这一针对紧急情况的例外并不排除《国家对国际不法行为的责任条款草案》第 52(1)(a)条的适用，即受害国在采取反措施之前仍应通知责任国，以“催告”其履行国际义务。[66]紧急反措施仅得在必要情况下实施，尽管在网络空间中如何界定“必要”仍需进一步研究。各国无疑会选择通过网络形式的紧急反措施来达成预期效果，但为防止滥用，在多大程度上允许基于情况“紧急”而免除通知要求仍值得进一步审视。在此背景下，中方专家指出，网络空间中的反措施通常具有隐蔽性，因此即使是紧急反措施，也必须要求其能够被责任国所知晓，以确保能够感知反措施所施加的压力，进而促使产生纠正不法行为的动力，实现反措施的基本目标。因此，中方专家建议，即便《国家对国际不法行为的责任条款草案》第 52(2)条允许通知例外的存在，也应理解为仅仅是免除了“事先”通知的义务，受害国仍应在紧急反措施实施的同时或随后发出该通知。

Kingdom) (2018) “Cyber and International Law in the 21st Century”, 23 May;UK (United Kingdom) (2021) “Application of International Law to States’ Conduct in Cyberspace”, 3 June.

66 ARSIWA Commentaries Art 52, p. 136, § 6.

4. 受害国以外的国家采取的措施

中欧双方确认，受害国以外的国家采取反措施并未被一致接受为现行法，这一问题仍然具有高度争议。

各国在2001年审议《国家对国际不法行为的责任条款草案》时，未能就国际法是否允许受害国以外的国家采取反措施达成共识。作为妥协，《国家对国际不法行为的责任条款草案》仅允许受害国以外的国家依据第 48 条而 “对另一国援引责任”和依据第 54 条采取“合法措施”。[67]第 54 条的评注指出，尚不确定现行国际法是否允许“为普遍或集体利益而采取的反措施”，因此“纳入一项保留条款，保留立场并将此问题的解答交由国际法的进一步发展决定。”[68]

受害国以外的国家采取的反措施可能涉及三种不同的形式：

(1) 非受害国针对责任国违反对世（*erga omnes*）义务所采取的反措施。
(2) 非受害国针对责任国违反对所有缔约国整体的（*erga omnes partes*）义务所采取的反措施。
(3) 非受害国应受害国请求而采取的反措施，无论责任国所违反的义务性质如何。

值得注意的是，以上这些有关不同形式的反措施的定义尚未统一，不同术语被同时使用且存有交叉混用的情形。但至少在本报告中，我们理解第一种和第二种形式的反措施有时被称为“第三方反措施”或“为一般或集体利益采取的反措施”，而第三种形式的反措施通常被称为“集体反措施”或“代理反措施”。[69]本报告将相应地使用上述的术语表达。

近年来，关于受害国以外的国家针对网络行动采取反措施的问题，已有一些学者和国家发表了评论。自 2012 年以来，若干国家公开发布了关于国际法适用于网络空间的立场声明。在 33 份国家立场文件中，只有 10 个国家（奥地利[70]、加拿大[71]、哥斯达黎加[72]

67 一些学者认为，这里的说法可以包含反措施，因为反措施的不法性是被排除了的。See, generally, L.A. Sicilianos, “Countermeasures in Response to Grave Violations of Obligations Owed to the International Community” in J. Crawford and others (eds), *The Law of International Responsibility* (Oxford University Press 2010) 1145–1146; M. Longobardo, “The Contribution of International Humanitarian Law to the Development of the Law of International Responsibility Regarding Obligations *Erga Omnes* and *Erga Omnes Partes*” (2018) 23 Journal of Conflict and Security Law 383, 388.

68 ILC (International Law Commission) (2001) “Commentary to the Articles on State Responsibility”, Yearbook of the International Law Commission, Vol. 2(II), p. 139, para. 6 to Article 54.

69 M. Jackson and F.I. Paddeu (2024) “The Countermeasures of Others: When Can States Collaborate in the Taking of Countermeasures?”, American Journal of International Law, 118, p. 231.

70 Austria (2024) “Position Paper of the Republic of Austria: Cyber Activities and International Law”, p. 9.

71 Canada (2022) “International Law Applicable in Cyberspace”, para. 37, https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx.

72 Costa Rica (2023) “Position on the Application of International Law in Cyberspace”, p. 5.

、丹麦[73]、爱沙尼亚[74] 、法国[75]、爱尔兰[76]、新西兰[77]、波兰[78] 和英国[79] ）对受害国以外的国家采取的反措施发表了评论。可以发现，在提及这个问题的那些声明中，有些关注第三方反措施，有些关注集体反措施，还有一些二者都关注，且他们的态度不尽相同：

> 第三方反措施：波兰、爱尔兰、哥斯达黎加和奥地利认为其是被允许的，丹麦似乎也赞成。
>
> 集体反措施：爱沙尼亚、爱尔兰和哥斯达黎加认为其是被允许的，新西兰似乎也赞成。法国和加拿大反对。

2019 年 5 月，爱沙尼亚在其关于国际法和网络空间的立场声明中首次提出受害国以外的国家是否可以采取反措施的问题。[80]有趣的是，爱沙尼亚当时的立场侧重于讨论集体反措施。换言之，爱沙尼亚关注的是实力较弱的受害国能否请求其他国家协助，并代表其采取反措施的可能性。即便在爱沙尼亚最新的一份立场文件中，也是既讨论第三方反措施，也讨论集体反措施。由于集体反措施在网络事务之外的讨论中很少被提及，因此网络空间出现的此类主张便显得格为重要。看待集体反措施的这一发展动向恰恰如同对世义务的发展历程，正如一些学者所认为的那样，正是有了确保对世义务能够得到有效履行的需要，才愿意承认第三方反措施是必要的。[81]然而，中方专家对此指出，由于当前尚缺乏一份明确的对世义务清单，也缺乏对其如何适用于网络空间的明确指引，承认第三方反措施的问题变得更具挑战性。特别是从更广的范围内考虑到，已有一些学者认为，自 2001 年通过《国家对国际不法行为的责任条款草案》后，一些国家在某些情况下发展出的实践可能足以从形式上被认定为第三方反措施。[82]

鉴于对受害国以外的国家采取反措施的问题发表过立场声明的国家数量有限，目前又没有足够的国家实践能补充说明帮助理解，中欧专家一致认为，现有这些不尽相同的立场并不能够表明现有国际法的演变，更合理的推论应当是：迄今为止尚未允许受害国以外的国家采取反措施，包括在网络空间。

一个至关重要的问题是，如何将受害国以外的国家采取反措施与提供援助或协助进行

---

73 J.M. Kjelgaard and U. Melgaard (2023) "Denmark's Position Paper on the Application of International Law in Cyberspace", Nordic Journal of International Law, pp. 446-455.

74 Kersti Kaljulaid (2019) "Opening Address at the 11th Annual Conference on Cyber Conflict of the NATO Cooperative Cyber Defence Centre of Excellence", https://president.ee/en/official-duties/speeches/2525-president-republic-opening-cycon-2019; United Nations General Assembly, 28.

75 France (2019) "International Law Applied to Operations in Cyberspace", ministère des Armées, p. 7.; France (2021) "International Law Applied to Operations in Cyberspace", United Nations Office for Disarmament Affairs, Paper shared by France with the Open-ended working group established by resolution 75/240, https://documents.unoda.org/wp-content/uploads/2021/12/French-position-on-international-law-applied-to-cyberspace.pdf.

76 Ireland (2023) "Position Paper on the Application of International Law in Cyberspace", Department of Foreign Affairs, p. 6, para. 26, https://www.dfa.ie/our-role-policies/international-priorities/international-law/internationallawandcyberspace/.

77 New Zealand (2020) "The Application of International Law to State Activity in Cyberspace", p. 4, https://www.mfat.govt.nz/assets/Peace-Rights-and-Security/International-security/International-Cyber-statement.pdf.

78 Poland (2022) "The Republic of Poland's Position on the Application of International Law in Cyberspace", Ministry of Foreign Affairs of the Republic of Poland, https://www.gov.pl/web/diplomacy/the-republic-of-polands-position-on-the-application-of-international-law-in-cyberspace.

79 S. Braverman (2022) "International Law in Future Frontiers", UK Attorney General's Office, https://www.gov.uk/government/speeches/international-law-in-future-frontiers.

80 Kaljulaid, 2019.

81 G. Gaja (2013) "The Protection of General Interests in the International Community: General Course on Public International Law (2011)", 364 Collected Courses of the Hague Academy of International Law, p. 130.; C.J. Tams (2005) Enforcing Obligations *Erga Omnes* in International Law, Cambridge University Press, pp. 198–251.; M. Dawidowicz (2017) Third-Party Countermeasures in International Law, Cambridge University Press, p. 11.

82 T. Dias (2024) Countermeasures in International Law and Their Role in Cyberspace, Chatham House, Research Paper, pp. 39–42.

区分，准确做出这一区分在网络空间面临着更大挑战。在某些情况下，非受害国提供的援助可能被视为助长了国际不法行为，甚至可能被认定为构成了国际不法行为本身，从而需要承担相应的国家责任。考虑到能力建设活动正如火如荼兴起，如何处理这一问题就显得尤为关键。毕竟对于某些能力建设活动——例如对某国提供支持以帮助其发展网络能力并用于网络行动——而言，不排除其在特定情况下助长了受助国实施国际不法行为，或因自身就违反国际义务而成为国际不法行为。中欧双方一致认可上述观察到的问题。

Building Peace Together

Geneva Centre for Security Policy
Maison de la paix
Chemin Eugène-Rigot 2D
P.O. Box 1295
1211 Geneva 1
Switzerland
Tel: + 41 22 730 96 00
Contact: www.gcsp.ch/contact
www.gcsp.ch

ISBN: 978-2-88947-023-5 (中文版)
ISBN: 978-2-88947-019-8 (English)