G D P
全球发展展望
Global Development Perspective

中国社会科学院世界经济与政治研究所 经济发展研究中心 国际经济与战略研究中心

Working Paper No. 15.010

October 1, 2015

任琳 龚伟岸

网络安全的战略选择[1]

【内容提要】 随着网络空间的迅速扩张及其对社会各领域的全面渗透，网络空间不断增长的财富、战略价值以及世界经济社会运行对网络空间的深度依赖，使网络空间整体安全问题的重要性日益凸显，网络安全已成为国际社会面临的又一全球性公共问题。网络安全问题虽然属于国家安全范畴内的非传统安全领域，但国家对于安全的偏好没有改变，对安全追求的逻辑路径依旧。从理论的角度看，由于体系压力以及国家对于安全的追求，会选择制衡的战略，但在现实中，制衡经常缺位或迟到。受到非传统安全环境影响，地缘战略里分而治之、领土补偿、加强军备、联盟以及平衡手的存在等制衡方式和作用意义同时发生了变化。更细分到网络安全领域，由于其沟通机制的不同，威慑效果不同，行为体的多样，行为判断的困难等特殊性，导致在网络安全领域，国家选择追随或合作将成为更优选择。

【关键词】 制衡战略；网络威慑；网络安全；合作治理

【作者简介】 任琳，中国社会科学院世界经济与政治研究所助理研究员（北京 邮编：100732）；龚伟岸，腾讯公司（广州 邮编：510000）。

【DOI】 10.14093/j.cnki.cn10-1132/d.2015.04.00X

[1] 本文已发表于《国际安全研究》，2015，第 5 期。

【中图分类号】D815.5【文献标识码】A【文章编号】2095-574X（2015）04-000X-00

网络安全问题虽然属于国家安全范畴内的非传统安全领域，但国家对于安全的偏好没有改变，对安全追求的逻辑路径依旧没变。理论上，迫于体系压力的国家出于对安全的追求，会选择制衡的战略。但在网络安全领域，由于文化、意图；综合实力，地理位置等原因，制衡战略经常缺位或迟到。由于其沟通机制的不同、威慑效果不同、行为体的多样、行为判断的困难等特殊属性的限制，网络资源大国选择合作战略则更具获益可能。

一　制衡是安全领域中的最重要战略选择

战略学中几种常见的策略有：制衡、追随和合作，国家的行为也常常表现出对某种战略方式的偏好。在网络空间战略中，各国的战略偏好可能发生更为显著的变化。本节首先回顾传统战略领域的国家偏好，为分析网络空间战略偏好提供参照。

在国际政治舞台上，当国家面临他国权力急剧上升的情境时，往往倾向于采取制衡战略以确保自身安全。现实主义主张无政府状态下，制衡策略是行为体（主要是国家）确保其安全乃至生存而采取的常见战略回应。[2] 正如乔治·凯南（George Kennan）认为的，美国的安全来自制衡战略，即通过在各种力量之间谋求平衡，遏制敌对和其他不可靠力量。所谓制衡策略就是让这些力量“在彼此的争斗中，消耗它们的偏执、暴力和狂热，否则它们也许会用这些来对付我们”“挑动它们之间的斗争，使得它们相互毁灭，在自相残杀中筋疲力尽，从而让致力于实现世界稳定的建设性力量保有生存下去的可能”。[3]

（一）传统安全领域中制衡战略的逻辑

国际体系压力，迫使国家选择权力制衡战略。肯尼思·华尔兹（Kenneth Waltz）

* 本研究接受国家社会科学基金（青年项目）“新安全观视野下新兴国家参与全球治理的制度性权力建构及其路径选择”（项目编号为：14CGJ012）的资助。作者感谢《国际安全研究》匿名审稿专家的审稿意见，文责自负。

[2] Joseph M. Grieco, “Realist International Theory and the Study of World Politics,” in Michael W. Doyle and G. John Ikenberry, eds. , *New Thinking in International Relations Theory*, Boulder, Colorado: West view, 1997, p. 169.

[3] 亨利·基辛格：《凯南的时代》，美国《纽约时报》网站，2011 年 11 月 10 日文章。参见 www. nytimes.com, Nov10th 2011, last accessed on 15Feburary 2015.

认为，在国际政治中，无政府状态下的国家以维持生存为基本目标，必须考虑其在国际体系格局中所处的位置，防止其他国家获得过度的权力优势，威胁本国的生存与安全。[4] 每当某一行为体（主要是国家）的权力增长从体量和增速上来说都可能危及整个体系的权力平衡之际，国际体系内其他相关度、脆弱度较高的国家就倾向于单独或联合起来对该国发起制衡，[5] 因为仅仅指望霸权的自我克制是不可靠的，[6] 所以国际格局中的均势（balance of power）现象一再出现。而“制衡”（balancing）和遏制权力挑战者，则是国家为实现“均势”（balance of power）而采取的重要策略。[7]

因此，新现实主义者认为，无论平衡的权力是不是行为体的目的，国家都会采取制衡的策略。国家采取“制衡而非追随”的策略是体系压力所诱导。[8] 在国际安全领域经常采取制衡的策略，汉斯·摩根索（Hans Morgenthau）曾经归纳了常见的制衡手段，“这些方式主要包括分而治之、领土补偿、加强军备、联盟以及平衡手的存在等，这些都是制衡的具体表现形式”。[9]

制衡往往是区域性的战略设计。制衡主要是基于地理临近性和投放能力的限制，或是作为不具备地理毗邻性的国家在该区域内建立同盟关系，从而增加制衡战略的“辐射”范围。例如亚太地区向来是美国制衡战略的重心之一。后冷战时期，历届美国政府高度重视亚太地区，长期在该地区贯彻制衡战略。克林顿执政时期，主要表现为美国在全球经济战略上的东移；小布什执政时期，制衡主要是在政治军事领域内展开，表现为“（军事）战略东移”；到奥巴马执政时期，美国政府提出了“重返亚太”战略。这意味着美国政府对亚太地区的高度敏感和关注，尤其是随着中国实力的不断上升，美国对华政策不断调整，即便是实力不及

---

[4] 刘丰：《制衡的逻辑：结构压力、霸权正当性与大国行为》，北京：世界知识出版社 2010 年版，第 10 页。

[5] 韦宗友：《制衡、追随与冷战后国际政治》，载《现代国际关系》，2003 年第 3 期，第 56-57 页。

[6] 杰克·利维（Jack Levy）认为，均势生成有三种途径：霸权的自我克制；霸权遭遇制衡联盟而收缩；霸权在战争中被打败。参见 Colin Elman, “Introduction: Appraising Balance of Power Theory,” in John Vasquez and Colin Elman, eds., *Realism and the Balancing of Power: A New Debate*, New Jersey: Prentice Hall, 2002, pp. 10-12。

[7] Jack S. Levy, “Balances and Balancing: Concepts, Propositions, and Research Design,” in John Vasquez and Colin Elman, eds., *Realism and the Balance of Power: A New Debate*, New Jersey: Prentice Hall, 2002, pp. 128-153; Susan B. Martin, “From Balance of Power to Balancing Behavior: The Long and Winding Road,” in Andrew K. Hanami, ed., *Perspectives on Structural Realism*, New York: Palgrave, 2003, pp. 61-82.

[8] 刘丰：《制衡的逻辑：结构压力、霸权正当性与大国行为》，北京：世界知识出版社 2010 年版，第 10 页。

[9] [美] 汉斯·摩根索：《国家间政治——寻求权力与和平的斗争》，徐昕等译，北京：中国人民公安大学出版社 1990 年版，第 232-244 页；刘丰：《大国制衡行为：争论与进展》，载《外交评论》，2010 年第 2 期，第 112 页。

的地方也要实现“离岸制衡”。奥巴马的“重返亚太”战略与往届美国政府的“亚太制衡”战略有所区别，其亚太战略表现为“多层次再平衡”，包括安全领域、经济政策和军事领域的全方位、多维度制衡战略，这在侧面说明亚太地区是美国的战略重心，在美国的对外政策中具有高度的敏感性。近年来，在全球公域（极地、海洋、网络和太空）等新生领域内，美国也没少论证其制衡战略的必要性和有效性。[10]

传统安全领域内的制衡战略具有什么样的实际效果呢？制衡的种类很多，以“离岸制衡”为例，第一，制衡可以增强霸权国（美国）的相对实力，通过制衡消耗其他大国的实力，一旦东亚、欧洲陷入安全竞赛，处于离岸位置的霸权国（美国）免于争端的同时，还“隐形”地增加了自身实力。第二，制衡战略可以使大国免于被永久性联盟关系所捆绑，获得更大的政策灵活度。第三，产生威慑效果，震慑潜在挑战者。[11] 制衡的核心在于均势，均势并非自发形成，而是通过了一系列的制衡手段最终达成。制衡的目的是权力或者说是相对的实力优势。

（二）制衡战略在实际应用中的修正

在传统安全领域的现实情境中，制衡的缺位（Absence of Balancing）与迟到现象经常发生，在面对体系中其他国家谋求权力或扩张权力的局面，国家有时会选择制衡，有时则会放弃制衡。[12] 学者们从多个维度对制衡的缺位进行了研究，使制衡作为一种战略工具更具现实操作意义，而非停留在纸面。

1. 威胁制衡论

国际体系的失衡并不必然导致结构性压力。据此，斯蒂芬·沃尔特（Stephen M. Walt）修订了华尔兹的均势理论，提出国家追求的是安全而非权力，即国家制衡的目标对象是威胁源，而非一定是权力体量庞大的实体国家。威胁一国安全的并非总是权力体量上占优的国家，增量权力只代表产生威胁能力的上升，并非权力必然导致威胁。正如在传统意义上，实力也不等同于影响力。沃尔特认为，制衡行为的产生并非单纯出于权力的考虑，而是基于对威胁的权衡，即某个国家或联盟出于战略考虑，显示出进攻性现实主义意图，那么它就具备了较高的威胁程

---

[10] 王义桅：《全球公域与美国巧霸权》，载《同济大学学报（社会科学版）》，2012 年第 2 期，第 49-54 页。

[11] 孔小惠：《美国在亚太地区的离岸制衡战略：理论涵义及其实践》，载《中共浙江省委党校学报》，2009 年第 6 期，第 71-77 页。

[12] 埃姆雷·拉卡托斯（Imre Lakatos）的精致的伪证主义认为，接受检验的理论是一个整体结构，是由一系列理论组成的科学研究纲领，单个异例的存在并不能证伪理论（证明理论是错误的），反而通过正面启发法对辅助保护带的修正是理论进步的表现。参见[匈牙利] 伊姆雷·拉卡托斯：《科学研究纲领方法论》，兰征译，上海：上海译文出版社 2005 年版，第 49-58 页。

度，就越有可能被其他国家当做制衡对象，因此容易招致针对它的制衡联盟出现。有时，虽然一国的权力可能不是很强大，但由于它的对外行为容易给别国带来直接威胁，则受到威胁的国家也会与其他相对强国结盟，以应对最具威胁的敌人，这种行为就是战略上的制衡而非战略追随。[13] 沃尔特指出，决定威胁程度的因素有：权力总量（aggregate power）、地理位置邻近（geographic proximity）、攻击能力（offensive power）和侵略意图（aggressive intentions）。具体来说，国家的权力大小，地理位置上是否与他国毗邻，攻击能力强弱，或侵略意图显露的程度增加，都可能成为威胁源，从而使该国成为制衡的对象国。[14]

沃尔特运用威胁制衡论研究了冷战后制衡美国的联盟缺位现象，他认为，尽管美国在权力总量上大大超过其他大国，但从“地理邻近度、进攻能力、侵略意图等方面来看，并不对其他大国构成威胁，这些要素大大削弱了大国制衡美国的倾向”，[15] 从而解释了冷战后对美国的制衡缺位现象。

2. 利益制衡缺位论及追随偏好。

除了考虑国际体系的压力，以兰德尔·施韦勒（Randall L. Schweller）为代表的新古典现实主义者，从其独特的视角出发，进一步认为追随是一种更普遍的行为偏好。在施韦勒看来，仅仅假定无政府状态的外部因素和国家因此追求自保的内部反应是不够的，这会导致强烈的现状偏见（the status quo bias）。[16] 于是，他从行为体的偏好出发，提出了利益制衡论。行为体并不总是从保证生存的角度，预设体系中存在掠夺性的国家，去制衡那些威胁其安全和体系稳定的国家和联盟。对于现状国家来说，安全和维护体系稳定是最基本的需要，因为现状是其获得好处的外部环境保障。但对于现状不满的修正主义国家而言，安全并非其首要目标，如何确保利益更大化才是它们所需。因此，不满于现状的国家常常会选择追随策略，而不是制衡战略，追随另一个正在崛起的、试图挑战和改变现存秩序的国家，能够确保获得更多的利益。[17]

施韦勒认为，制衡和追随拥有不同的动机，制衡是为了谋求安全，而追随是

---

[13] 韦宗友：《制衡、追随与冷战后国际政治》，载《现代国际关系》，2003 年第 3 期，第 58 页。

[14] Stephen M. Walt, *The Origins of Alliances*, Ithaca and London: Cornell University Press, 1987, pp. 21-28. See also, Stephen M. Walt, “Alliance Formation and the Balance of World Power,” *International Security*, Vol. 9, No. 4 (Spring 1985), pp. 9-13.

[15] 刘丰：《大国制衡行为：争论与进展》，载《外交评论》，2010 年第 2 期，第 112 页。

[16] [美] 兰德尔·施韦勒：《没有应答的威胁——均势的政治制约》，刘丰、陈永等译，北京：北京大学出版社 2015 年版，第 35-38、61-63 页。

[17] 韦宗友：《制衡、追随与冷战后国际政治》，载《现代国际关系》，2003 年第 3 期，第 58 页。

为了获取收益。根据利益偏好，利益制衡论者将国家划分成两类：一种是维持现状的国家，以谋求最大化的安全为战略目标；另一种是修正主义的国家，以谋求最大化的权力为目标。[18] 为了追逐更大的利益，对现状不满意的国家会追随更强大的、上升中的、具有修正主义意识的国家，只有对现状满意而不乐意谋求改变的国家才会采取制衡行为。[19] “利益平衡理论”在解析冷战后的联盟实践时无疑具有更大的解释力，施韦勒认为，国家的行为由其所认定的利益所决定，而不仅仅由权力分布或所谓的威胁所决定，[20] “国家更关注谁拥有权力，而非权力的不平衡。利益而非权力，决定了国家如何选择敌友”。[21]

在这个意义上，从利益制衡论出发，最优选择并非制衡战略，而是追随或其他应对战略。为什么那么多国家不愿意制衡，而是偏好于追随或不作为、不介入？利益论给出了很好的解释，但是施韦勒的论述仅仅解释了修正主义国家的行为倾向，没有涵盖更广泛的国家类型。在现实情境中，并非仅存一种具有修正主义国家性质的国家类型，也并非是仅仅限于修正主义国家会偏好于非制衡的追随、不作为或不介入。究其原因而言，系统环境压力等也是非常重要的解释变量。

3. 实力门槛论

在国际体系中权力的集中程度与制衡的实力门槛成正比，即当权力集中程度提高时，制衡的实力门槛将会随之提高，尽管制衡的动机很强烈，但制衡成本过高，从而造成了制衡的缺位。威廉·华尔福思（William C. Wohlforth）认为，“在任何体系中，如果权力过分集中在最强大国家的手中，要对其进行制衡，就要付出极其高昂的代价，这样就会形成一个门槛（threshold），令其他国家望而却步”。[22]

制衡的门槛表现为国家之间实力的差距，制衡的实施需要以强大的实力为后盾，只有实力差距不大时才有实施制衡战略的可能，只有具备相当的实力才能够担当起系统内制衡者的重任。[23] 中国学者刘丰认为，“在多极体系下，权力集中

---

[18] 刘丰：《制衡霸权：结构压力、霸权正当性与大国行为》，载《国际政治科学》，2009年第3期，第35页。

[19] 刘丰：《制衡霸权：结构压力、霸权正当性与大国行为》，载《国际政治科学》，2009年第3期，第29页。

[20] 汪伟民、张爱华：《单极体系下的联盟理论与实践》，载《世界经济与政治论坛》，2006年第2期，第89页。

[21] Randall Schweller, *Deadly Imbalances: Tripolarity and Iiitter's Strategy of World Conquest*, New York: Columbia University Press, 1998, Conclusion.

[22] William C. WoMforth, “U.S. Strategy in a Unipolar World,” in John Ikenberry, ed., *America Unrivaled: the Future of the Balance of Power*, Ithaca, N.Y.: Cornell University Press, 2002, p. 103.

[23] 刘丰：《均势生成机制的类型与变迁》，载《欧洲研究》，2009年第4期，第5页。

程度最低，国家制衡的方式多样且灵活，国家制衡的实力门槛最低。在两极体系下，只存在两个主导性的大国，制衡的手段主要是通过增强自身的军事实力，这对制衡的实力提出了更高的要求。而单极是一种国家实力差距太大以至于很难制衡的结构，对于国家采取制衡行为的门槛最高。”[24] 华尔兹也认为：“强国与其他国家之间的实力差距越大，拉近距离所需的时间就越长。”[25] 在这种情况下，制衡战略不可避免地会出现一定程度的缺位。

讨论完传统安全领域内制衡的逻辑、方式与修正情况，我们看到制衡战略在具有重要影响力、为大国所青睐的同时，也常常存在缺位与迟到的现状，也有被国家行为体摒弃的时候。那么在一些非传统安全的领域内，地缘战略里分而治之、领土补偿、加强军备、联盟以及平衡手的存在等制衡方式和作用意义同时发生了变化，是否会出现可以替代制衡的其他战略选择呢？例如，大国会选择追随、不介入或者再进一步选择抛弃过度的彼此战略警戒和不信任，转而选择持合作姿态？下面，我们将以网络安全问题为例，对于这个问题展开进一步的讨论。

二　网络安全领域中的制衡问题

网络环境具有无地理概念、多元行为体、国家能力再分级等诸多特性，重构了安全问题的结构，进而造成网络安全领域下博弈机制的变化，具体表现为归因困难、意图沟通困难、冲突易发等。

（一）网络环境对安全问题的重构

网络环境的特性改变了传统的安全思维。权力在网络环境中传递，更容易失真。相比传统安全领域，行为体在网络安全领域内，更加脆弱、更加敏感。按照这种逻辑，行为体应该有更强烈的意愿对安全威胁做出反应，例如通过采取制衡战略寻求安全。那么现实情况又是如何？如果国家在网络空间里修正制衡战略，也无法改进战略效果，它们的战略选择偏好又会发生什么变化呢？回答这些问题需要首先剖析网络安全环境的特性及其对安全问题的重构。

1. 网络世界无地理概念不受投放能力的限制

在现实世界的战略博弈中，制衡的重要实现手段是能够通过权力的投射，而

---

[24] 刘丰：《制衡霸权：结构压力、霸权正当性与大国行为》，载《国际政治科学》，2009年第3期，第32页。

[25] [美] 肯尼思·华尔兹：《冷战后的国际关系与美国对外政策》，2004年10月15日在北京大学的演讲，第3页。

权力的远程投放会导致成本的上升，随着投射距离的增加，投送成本也会随之递增，与此同时权力效能却呈递减趋势，帕特里克·奥沙利文（Patrick O' Sullivan）指出，力量投射离本国越远，“摩擦损耗”越大，投送的费用就越高，抵达目的地的有效实力也就越少。[26] 肯尼斯·博尔丁（Kenneth N. Boulding）也提出了“力量损失梯度”（loss of strength gradient）的概念，指出一国的力量向外扩张时随着辐射范围的扩大，力量损耗也越大，投射成本不断增加。[27] 正如约翰·米尔斯海默（John Mearsheimer）所说，地理上的限制导致全球霸权极具稀缺性。因为地区上水体等地理因素遏制了大国权力的有效投射。在这个意义上讲，区域性的霸权成为替代全球霸权的重要选择。大国受制于地理限制只能在可以到达的区域内投射能力，具有进攻性的军队能够到达的范围即是大国能力投放的范围边界。[28]

网络世界并没有地理的概念。以空间信息技术为例，“卫星网络具有覆盖面广、组网灵活、建网快、不受地理环境限制等突出特点”。网络能力的投放可以是随时随地的，也可以跨越大洋、大洲，同时又没有射程等能力限制的影响。但是，没有边界的能力投递并没有想当然地带来战略制衡。

2. 网络环境中各行为体都有能力发动袭击

在网络环境中，政府和非政府组织等各行为体都有能力发动袭击，行为主体更为丰富。

传统意义上，我们谈战略制衡，常常是假定战略互动是在实力、身份大致对等的国家之间发生。当战略互动的国家并非实力对等时，国家将会青睐结盟的方式来实现战略制衡的目的。现实的威胁来自对等行为体即国家，但网络空间里的攻击则可能是民间行为体，例如黑客高手或者恐怖组织。袭击来自非政府行为体并不意味着杀伤力和破坏性就降低了，相反，通过低廉的工具和攻击手段，例如运用信息炸弹、病毒程序和木马发动网络攻击，却足以有能力瘫痪一国的金融、水利和供电系统。此外，网络数据的泄漏可以带来极高的经济损失。通过植入或损害程序，使机器服从于攻击者的操作口令，此类的网络攻击具有成本低、技术含量低但损害性高的特点。谁都可以发起袭击，攻击行为又可以极度隐蔽，但这

---

[26] [英] 帕特里克•奥沙利文：《地理政治论——国际间的竞争与合作》，李亦鸣译，北京：国际文化出版社 1991 年版，第 11-12、70-73 页。

[27] 韦宗友：《霸权阴影下的对外战略》，上海：上海人民出版社 2010 年版，第 43 页。

[28] [美] 约翰·米尔斯海默：《大国政治的悲剧》，王义桅、唐小松译，上海：上海人民出版社 2008 年版，第 149-151，169-170 页。

些破坏行动对正常社会秩序的破坏巨大。

网络安全事件频频发生，计算机硬件企业莱斯（LaCie）的数据泄漏事件、亿贝网络信息服务有限公司（eBay）数据泄漏事件、比特币交易破产事件等等。2014年4月，莱斯公司发出警告，由于网络黑客利用Adobe Cold Fusion的安全漏洞而发起的攻击，致使僵尸网络的形成，导致部分用户的名字、住址、邮箱地址、银行卡号、卡片有效期与密码都存在潜在的安全隐患。2014年5月22日，亿贝公司正要求近1.28亿用户重置密码,原因是黑客可以从亿贝公司网站获取用户密码、电话号码、用户地址等个人数据。比特币交易作为一件新事物刚刚出现在世人的视野中，然而全球最大比特币交易平台Mt.Gox却于2014年就申请破产，原因是比特币软件存在漏洞，黑客透过该漏洞可以修改交易信息。

各国虽然可以推动网络技术的进步，提高防护网络安全的级别，但网络攻击仍然可能是来源于各处各方和各种行为体。虚拟世界缺乏可知性、可控性和规律性，网络攻击无孔不入，打击起来无从下手，如果要采取制衡战略，制衡对象同样不明。

3. 网络技术的发展打破了传统安全领域中对国家的级别分类方法

互联网大国即使掌握了较之其他国家更雄厚的资金、技术和策略，在发起网络攻击方面的优势更为明显，但在优势的生命周期和覆盖广度上都大大减少。随着网络技术的快速更迭，在网络空间里，很难给出区分大国的制衡与小国或其他行为体制衡差异的标尺，可能每一个国家都是某一个互联网领域的大国。国家级别和制衡难度之间的联系并非直线的，而是错综复杂的。网络具有开放性、跨境性、隐蔽性和自由性的特点，网络技术和应用的普及一方面增加了自由度，另一方面也对网络安全的维护提出了更高要求。发起网络攻击的方式可以是多种多样、低门槛、极其隐蔽的，并非单纯的网络攻防战形式所能描述的。隐蔽了互联网协议地址（IP地址）的网络攻击成本极低、难以溯源，甚至社交网站都可能成为发起网络战的平台。正如英国《卫报》所披露的美国“真诚声音行动”（OEV），它属于舆论战的方式。OEV通过借助“在线个人管理服务”使美国士兵拥有多个显示不同国家IP地址的“身份”。[29]美国士兵借助这些“马甲”在中东国家的社交网站上发布舆论，对抗反美舆论，试图控制当地的舆论阵地。发起攻击的行为体也远不止国家行为体，一些非国家行为体甚至是个人，这些行为体在实力上是“非

[29] 张笑容：《第五空间战略：大国间的网络博弈》，北京：机械工业出版社，2014年版，第68页。

对称的”，却具有发起破坏性极强的网络攻击能力。网络黑客可以使政府网络瘫痪，攻击用水、用电、金融等基础设施。2013 年 3 月，黑客对韩国发起了历史上空前规模的攻击，韩国主要银行系统计算机网络瘫痪，大量企业、电视台及其他通讯媒体资料泄露，不得不中止提供服务。

（二）网络安全领域下博弈机制的变化

做出面对安全威胁博弈的策略，依靠的是信息机制、传递机制，威慑机制等战略工具。但是，当这些战略工具在网络空间内变得缺失或者无效的情况下，制衡战略就不可避免地存在着缺陷。

1. 不能快速有效归因

只有做出有效的归因，才能迅速决策。归因理论（attribution theory）起初源自社会心理学，归因是观察者掌握被观察者行为的重要途径，对外部环境加以控制，对被观察者的行为进行因果解释。很多情况下，无法对行为体的行为进行归因，还可能会产生误判，特别是受制于时间限制，必须迅速做出归因，进行战略反应。所谓“误判”即观察者观察到的情境偏离了被观察者原有的预期、意图和打算。

卢卡斯•凯拉（Lucas Kella）认为，由于网络空间里存在高度虚拟性，导致无法溯源、归因更加困难、误判高发、信任缺失，也由此使之具有“战略不稳定性”（strategic instability）。网络空间里难以进行有效归因具有客观技术性原因。网络技术非常新颖，各类网络漏洞客观存在着，针对各类网络漏洞的攻击行为常常千变万化、难以捉摸，加之诸多行为体和鱼龙混杂的信息都充斥在网络空间中，这就加剧了网络空间战略不稳定性的程度。[30]

而网络空间在严重的模糊性和不确定性之下，对迅速反应（instant response）战略的偏好和诉求却非常强烈。[31] 行为体如果不及时对网络攻击做出战略反应，则会被认为是战略无能，反而可能会招致更多的网络攻击。因此，麻省理工学院计算机科学与人工智能实验室资深科学家戴维•克拉克（David D. Clark）明确表示“归因是威慑的核心”。系统规划与分析公司（System Planning and Analysis）的系统与技术分析员乔纳森•所罗门（Jonathan Solomon）明确

[30] Lucas Kella, “The Meaning of The Cyber Revolution: Perils to Theory and Statecraft,” *International Security*, Vol. 38, No. 2 (Fall 2013), pp. 7-40.

[31] Keith B. Alexander to the U. S. Senate Committee on Armed Services, Washington, D.C.: U.S. Government Printing Office, April 15, 2010, p. 218-219.

谈到，要想让惩罚威慑起作用，威慑方必须能够高度自信地确认攻击方。[32]

除了隐藏问题，还存在另外一个战略难题，即在网络环境下“嫁祸”（false flag）变得更加容易。拥有先进网络技术的行为体（可以是个人、组织、机构、国家等各种行为体）可以借助技术手段通过隐匿身份的方式，从第三方（实时或离线）的角度，攻击其他行为体的网络，甚至完全可以隐藏或借助他者的 IP 地址发起网络攻击。因此，面对这种极度隐匿的攻击，迅速确定哪个行为体在何处、何时发起网络攻击，是有一定难度的。即使能够确切知道来自某国的一台计算机发起了对一个国家机构的网络攻击，也不能随便断定这个国家一定是发起攻击的“幕后黑手”。[33] 更有甚者，一些国家可能把网络攻击外包给黑客，借用第三方的方式成功地挑拨离间，让双方发生冲突。网络行动的固有匿名性使得“嫁祸”行动在网络空间更容易进行。[34] 即使是有国家、组织或个人声称对某次网络能力的投射活动负责，我们都有理由怀疑它们在说谎。因为网络空间的虚拟性在隐蔽进攻者身份的同时，也使战略承诺缺乏可观测性而变得不再可信。

这就容易产生一个怪圈，迅速反应需要迅速归因，但归因却受制于网络空间的客观条件限制，无法保证准确性和时效性。所以，正如基斯·亚历山大（Keith Alexander）所建议的，进行“即时反应”受到国家青睐，是为了确保战略威慑或者其他战略行为的有效实施。但是，无法进行有效归因，但依然需要做出迅速战略反应，就需要基于客观印象或者是非条件反射做出战略决策，这急剧地增加了网络空间的战略不稳定性。[35] 总之，战略不稳定性产生的部分原因正是由于在无法有效归因的情况下，制衡战略的系统稳定功能无法按照预期正常实现。

2. 不能准确进行意图沟通

通过意图沟通，可以提供可靠的行为轨迹，建立相互信任机制，促成双方合作。现实世界中的战略沟通基本遵循着上述的逻辑。网络世界具有虚拟性和实体性。前者增加了不确定性，对正常信息传递和意图沟通的影响作用更为明显。制衡战略在内的各种战略手段能够发挥作用，其基础都是意图（包括欺骗性意图）

---

[32] Jonathan Solomon, “Cyber deterrence between Nation-States: Plausible Strategy or a Pipe Dream?” *Strategic Studies Quarterly*, Vo1. 5, No. 1 (Spring 2011), p. 5.

[33] 何奇松：《美国网络威慑理论之争》，载《国际政治研究》，2013 年第 2 期，第 57 页；任琳：《网络空间战略互动与决策逻辑》，载《世界经济与政治》，2014 年第 11 期，第 73-90 页；董青岭：《网络空间威慑：如何推进第三方责任》，载《世界经济与政治》，2013 年第 9 期，第 113-124 页。

[34] 何奇松：《美国网络威慑理论之争》，载《国际政治研究》，2013 年第 2 期，第 57 页。

[35] Herbert S. Lin, “Offensive Cyber Operations and the Use of Force,” *Journal of National Security Law & Policy*, Vol. 4, No. 1 (September 2010), pp. 63-86.

的成功传递。如果不能及时传递意图，就无法对行为轨迹做出判断，导致信任缺失。

网络具有实体性，主要是指网络的组成和依赖各种基础设备搭建了可被检验的现实体验。网络以各种程式、图像、声音、电子邮件和文本等作为存在形式，并且网络传输过程中信息的发出方可以隐匿或是不断变动自己的身份。此外，网络使用者身份虚拟、信息通道不畅、信息鱼龙混杂等[36] 都是网络虚拟性的表现。虚拟性意味着行为者可以逃避传递虚假或有害信息的实际后果。网络空间的虚拟性带来了更多的不确定性，背叛的道德成本变得很低。即使行为体真心诚意地传递友好意图，最终达成合作的可能性也很低。因为虚拟性的存在，技术上的意图传递的不畅、以往声誉不好或是第三方的嫁祸[37] 都可能毁掉合作的可能。在技术上缺乏溯源的可能性，活动在网络空间的各行为体不需要为自身的言论和行为负责。究其根本则是网络空间内虚拟性的存在破坏了意图沟通的渠道，从而导致了信任缺失，行为难以具有连贯性。

3. 不能进行有效威慑威慑 战略主要是指国家为避免实力被低估后会遭受灾难性攻击，而不得不积极展现自己进行战争的能力和意愿。[38] 因为无关紧要事件上的退让，会让进攻对手认为是过于软弱而动了发起进攻的意图。[39] 而核威慑则是通过持有核武器进行威慑，以恐吓而非动武的方式，[40] 使敌对国家认识到发起进攻可能遭受到的不良后果，从而不得不放弃进攻性的行为倾向和战略偏好。威慑战略成功的关键在于威慑意图的成功传递，以使对手国家充分地认识到发起进攻的严重后果。

从威慑理论机制的角度来看，威慑战略是通过威胁使对手屈从于自己的意愿。[41] 从国际安全的角度看，就是针对对手的认知系统和心理防线，通过恫吓或者欺骗达到不动一兵一卒、没有硝烟战火就可以实现国家间关系的相对稳定。为了达

---

[36] Will Goodman, “Cyber Deterrence Tougher in Theory than in Practice?” *Strategic Studies Quarterly*, Vol. 4, No. 3 (Fall 2010), pp. 102-135.

[37] [美] 马丁·C. 利比基：《兰德报告：美国如何打赢网络战争》，北京：东方出版社 2013 年版，第 40 页；董青岭：《网络空间威慑：如何推进第三方责任》，载《世界经济与政治》，2013 年第 9 期，第 113-124 页。

[38] [美] 罗伯特·杰维斯，《国际政治中的知觉与错误知觉》，秦亚青译，北京：世界知识出版社，2003 年，第 51 页。

[39] Joseph S. Nye Jr. and Sean M. Lynn-Jones, “International Security Studies: A Report of a Conference on the State of the Field,” *International Security*, Vol. 12, No. 4 (Spring 1988), pp. 5-27.

[40] 樊吉社：《影响冷战后美国军控政策的若干因素》，载《世界经济与政治》，2001 年第 9 期，第 28-33 页。

[41] George Downs, “The Rational Deterrence Debate,” *World Politics*, Vol. 41, No. 2 (January 1989), p. 226.

到抑战的目的，必须让恐吓信号足够明显，使对方认识到威慑是可信的。网络空间的威慑呈现为明示型威慑和默示型威慑两种，[42] 前者强调战略意图的传递要更为重要。[43] 当然，究竟是哪种威慑的效果更好，存在着很多争议。过度明显的战略信号传递容易引起敌手的过分恐惧、甚至是过度反应。为了抑战而采取的威慑战略反而最终将会把国家引入战争的泥潭。

在威慑的方式上，格伦·斯奈德（Glenn Snyder）把威慑的手段分为“惩罚威慑”（deterrence by punishment）与“拒止威慑”（deterrence by denial）两种方式。[44] 前者是指采取惩罚的方式报复进攻者，迅速和压倒一切地迫使进攻者认识到发起攻击是得不偿失的，这种威慑方式立足于行为体自身的（反击）打击能力；后者则强调防御能力，通过建立和储备强大的、有效的、及时反应的防御能力，使敌方感到无法通过进攻实现预期目的，从而放弃发起攻击的意图。[45] 由于不能确保“二次打击能力”，惩罚威慑用于网络安全领域存在很大问题，以牙还牙的报复方式是建立在“确保相互摧毁战略”之上。与传统军事打击不同，网络反击不能让对手明确意识到遭受报复的后果，更不能像核威慑那样，有明确的巨大的附带伤亡预期，决策层不能够预测成本与收益。同时，纯粹的拒止威慑手段也是有局限性的。即使对手认为其攻击不一定会成功，但是如果觉得网络攻击成本较低，他们是不会被慑止的，仍会尝试发起网络攻击。[46] 实际上，需要将网络防御措施隐藏起来，这种“藏锋”的行为却不可避免地削减了威慑的效果。

此外，在网络空间里，小国以及非国家行为体（例如黑客组织）损失小，大国损失大，小国更容易威慑大国。与常规的军事实力不同，网络实力（网络武器）带有一定虚拟性，如果不展示所拥有的网络武器，将虚拟的“底牌”亮出来，行为体的网络威胁、防御能力对于对手来说就是不可视和不可感知的，因此也就不能针对对手产生威慑效果。这都与传统的制衡理念相矛盾，大国更有制衡偏好还是小国更有制衡偏好变得相当不明确。由于计算机网络的特性，网络武器一旦展示出来，对方会很快生成防备策略与研制反制的网络武器，这样反而会削减威慑

---

[42] 董青岭、戴长征：《网络空间威慑：报复是否可行?》，载《世界经济与政治》，2012年第7期，第99-116页。

[43] [美] 马丁·C·利比基：《兰德报告：美国如何打赢网络战争》，薄建禄译，北京：东方出版社2013年版，第178-180页。

[44] Glenn Snyder, *Deterrence and Defense: Toward a Theory of National Security*, Princeton: Princeton University Press, 1961, pp. 3-l6.

[45] 程群、何奇松：《美国网络威慑战略浅析》，载《国际论坛》，2012年第9期，第68页。

[46] 何奇松：《近年美国网络威慑理论研究述评》，载《现代国际关系》，2012年第10期，第8-9页。

和防御的效果，[47] 不能慑止对手的进攻行为。良好的防御可能会抵御攻击，但同时削弱了威慑效果。因此，大国有必要提供系统稳定的公共产品，从而防止战略冲突升级的情况发生。

三　网络大国的战略选择

在网络空间中，制衡等战略偏好似乎被遗忘在角落里，究其原因是网络安全领域的诸多博弈机制失效，国家谋求安全的手段发生改变，影响了大国的战略意愿和选择偏好。尤其是对于大国来说，制衡他国未必可以获得安全，合作远比制衡、威慑等其他战略手段的战略收益更高。当然，面对各种战略机制的失效，国家可以谋求破解归因能力的技术局限，从而修复制衡和威慑战略的效果。[48] 但考虑到短时间内实现技术突破并降低战略成本的可能性不高，本文论及网络安全领域内的战略选择，主要讨论放弃传统战略不信任、突破囚徒困境、谋求合作治理的选择路径。因此，并非谋求在网络空间内修复制衡和威慑等战略工具，而是探索采取另外一种战略选择的可能性。

（一）网络资源大国选择合作更具获益可能

在传统安全领域，军事威胁主要涉及领土及主权的完整性，因此法国、德国和俄罗斯等大陆国家更容易受到周边国家的制衡。而在金融、贸易等非传统安全领域，由于霸权国能够在一定时期内更有效地提供部分“公共物品”以至于在一定程度上延缓了制衡的出现。其中冷战后，新自由制度主义阵营的学者在分析大国制衡行为缺位现象的成因时认为，冷战后，美国主导的国际秩序被纳入高度制度化框架下，主导国能够提供关键公共产品，[49] 保障其他国家的生存和发展需求，使这些国家形成了对大国构建制度的路径依赖。当然，在部分领域内（例如金融），

---

[47] Stephen J. Lukasik, “A Framework for Thinking about Cyber Conflict and Cyber Deterrence with Possible Declaratory Policies for These Domains,” in National Research Council of the National Academies, ed., *Proceedings of a Workshop on Deterring CyberAttacks: Informing Strategies and Developing Options for U.S. Policy*, Washington, D.C.: the National Academies Press, 2010, p. 108.

[48] 作者在 2014 年发表的《网络空间战略互动与决策逻辑》一文中已经集中讨论了这一选择偏好，所以本文希望换一个角度研究合作的可能。参见任琳：《网络空间战略互动与决策逻辑》，载《世界经济与政治》，2014 年第 11 期，第 73-90 页。

[49] 有关国际公共产品及其意义的论述参见：Charles P. Kindleberger, “Dominance and Leadership in the International Economy: Exploitation, Public Goods, and Free Rides,” *International Studies Quarterly*, Vo1. 25, No. 2 (June l981), pp. 242-254; Charles P. Kindleberger, “International Public Goods without International Government,” *American Economic Review*, Vo1. 76, No. 1 (March 1986), pp. 1-13；Robert Gilpin, *The Political Economy of International Relations*, Princeton: Princeton University Press, 1987, pp. 74, 86-87。

随着原有主导国实力的相对下降，主要公共产品也存在供应不足的现象。网络安全是一个典型的非传统安全领域，目前的网络安全治理缺少制度支持。主导网络安全制度和规范的大国利用提供公共产品的机会，可能会占更多的先发优势；同样，如果重复其他领域内欧美主导的非中性制度框架，则意味着权责不对称现象的再次出现。所以各国要在互联网治理制度的塑造层面上，尽量避免单个互联网技术大国试图塑造的“制度非中性”，在源头上避免利益受损。网络安全治理需要负责任的互联网大国提供中性制度作为“公共产品”，维持该领域内的秩序与稳定。

不可否认，互联网大国在提供公共产品、维系网络空间安全方面，有更大获益的可能。在主观和客观上，网络资源大国都应表现出更强烈的意愿。但如何在理论和实践层面上都能够将合作的潜在获益转化为大国的合作意愿，仍然是一个非常严峻的现实命题：

1. 谋求安全的手段的改变影响大国的战略意愿和选择偏好

从传统安全角度考量，各国（特别是大国）有必要担忧自身在实力分布中的位置变化，防止其他国家获得超越自己的权力优势，从而危害自身的生存和安全。一般来说，对手是具有对称身份的国家行为体，身份辨识性强，战略对策针对性强，效果明显。越是大国越具有充足的资源、可以通过制衡或其他战略手段谋求安全。但在网络空间领域，谋求霸权地位、进行地缘布局、动用制衡战略，并不能确保国家获得安全。即使是霸权国家，也无法实现“网络空间零威胁”。由于在网络空间内“实力门槛”的降低，威胁常常来自具有“非对称身份”的非国家行为体，攻击源更加难以辨识。但是，在网络安全领域内，制衡战略的直接受益很小。由于大国对网络的依赖程度更高，受到攻击的目标更大，遭受的损失也更大。一旦举国的网络基础设施受到攻击，利益损失将十分惨重。在这个意义上，网络安全领域大国提供公共物品的动机更强烈。

国家在网络空间里战略互动需要面对的“非对称性问题”，不仅仅是攻击源身份上的非对称性，更为严重的是网络作为虚拟空间营造出来的信息非对称性问题。当国家面对某一次网络攻击时，甚至可能不知道报复对象是谁，下一轮防御的重点是什么；即使要报复连报复的意图该传递给谁、怎么传递都是不可实现的。从博弈的过程来看，先发制人的战略拥有无可比拟的优越性。[50] 因为互动双方在

[50] 任琳：《网络空间战略互动与决策逻辑》，载《世界经济与政治》，2014 年第 11 期，

信息保有上是非对称的，谁先发起攻击则可能取得战略上的优势。网络攻击的施力者处于暗处，他可以在对方毫无知晓的状况下调查和分析攻击对象的系统弱点、缺陷和运行规律，并在做好充分准备之后发起突然袭击。这种性质的网络攻击是防不胜防的。但是，国家与国家、国家与其他行为体的博弈是多次的重复博弈，同时每次博弈的信息非对称性都是一般现实世界博弈无可匹敌的。不断争夺先发制人优势，意味着网络战的恶性重复，没有任何一个国家或非国家行为体可以处于网络的安全状况下。即使受攻击方是网络资源大国，在技术、制度、软资源上都拥有其他国家望尘莫及的能力，可以通过以往受攻击的经验分析自身的系统性漏洞等增强防御能力，但这种方式也只能避免某些形式的攻击。同时，由于网络技术更新快，攻击方式不断变化，仍然难以避免通过隐匿 IP 地址等方式的攻击，在受攻击的时机和方式上，网络大国依然是防不胜防。如果核算成本，网络大国也是在做赔本买卖。合作远比开展无休止的网络战划得来。网络资源大国增强防御能力、填补系统漏洞、进行系统维护的成本将是非常高昂的。与传统安全领域不同，为了谋求安全采取制衡却收效很低；相反，在传统意义上合作或追随是为了获取收益，但在网络空间里却意味着获取安全。

2. 网络安全领域大国提供公共物品的能力更充足

正如前文提及，施韦勒认为，制衡和追随（合作）背后的动机不同，制衡谋求的是安全，而追随谋求的是收益。如果制衡等战略在网络空间失效，也就难以谋求安全。为了追逐更大的利益，合作将是最优选择。对于小国来说，搭便车远比自行出力划算得多。不可否认，网络安全领域大国提供公共物品的能力更充足。大国能提供更多的公益产品（开发服务器，IP 地址等），技术扶持成本更低。

目前，发达国家与发展中国家在网络资源控制上存在着显而易见的差距。在关键的基础设施方面，以支撑全球网络空间关键基础设施的海底光缆系统为例，资料显示，“自 1988 年 12 月开始，第一条跨洋海底光缆（TAT-8）进入商业服务。从那时开始一直到 2008 年，欧美公司垄断了全球光缆市场，其铺设的海底光缆普遍发端于欧美发达国家，或者以欧美发达国家为中枢桥接点。虽然从 2008 年开始，相关公司将投资方向转向了基础设施薄弱的非洲等地区，但欧美公司垄断海底光缆的事实没有改变。”[51] 同时，网络资源集中的趋势也非常明显。以美国为例，

第 73-90 页。

[51] 沈逸：《后斯诺登时代的全球网络空间治理》，载《世界经济与政治》，2014 年第 5 期，第 115-116 页。

其控制了根服务器和地址资源等最重要的网络空间资源。如 IP v4 架构下可分配约 43 亿个 IP 地址，美国有 15.67 亿个，中国仅有 3.3 亿个。美国还通过“互联网名称与数字地址分配机构”（ICANN）等非政府组织掌握关键资源的分配权。关键性权力如域名控制和否决权由美国商务部通过与“互联网名称与数字地址分配机构”的协议控制。[52] 由于发达国家在网络渠道和技术上的优势，在涉及信息流动的网络控制权上，发达国家具有明显优势。如威尔伯·施拉姆（Wilbur Schramm）得出结论，经济上富庶的国家享有更多媒介资源，在世界信息流动中占据优势地位，拥有相对多的可控权。[53]需要补充的是，如果得到恰当引导，这些资源也可以转化为一些亟须提供的全球性公共产品，维护网络空间的安全与稳定。

3. 大国合作所聚集的互联网资源带来巨大的安全和经济利益

中美两国合作的互联网体量是非常庞大的，巨大的合作潜力可以为两国带来巨大的合作动力。除了共建安全互联网环境的利益驱动，中美合作还可以优势互补。一方面，中国在 2014 年的互联网经济规模高达 7 753 亿元人民币，客观上具有天然的大市场，美国的微软等互联网公司都在中国有着大量的业务；另一方面，美国先进的互联网技术和丰富的互联网经济经验，都是中国可以学习和借鉴的。此外，中美合作对于治理网络空间安全具有非常深远的意义。中国和欧盟之间的互联网合作项目也有很多，例如伽利略项目、中欧先进网络高速互联以及相关应用合作协议。这些大型的科技合作项目，都可以为各国带来巨大的经济、安全或其他社会效益。

（二）网络安全治理合作大势所趋

网络安全是各国面临的共同问题，隶属国家安全的范畴。例如中美两国在网络安全合作方面具有认知和利益上的差异，但这并不妨碍两国进行合作，共同治理网络安全事宜。美国认为网络安全是“全球公域”的重要领域之一，这些领域中存在的安全问题是全球性的，是各国共同面临的。[54] 然而，在让渡网络控制权方面，美国又显得情非得已。美国把持着网络资源的控制权（“互联网名称与数

---

[52] 汪晓风：《中美关系中的网络安全问题》，载《美国研究》，2013 年第 3 期，第 11-12 页。

[53] [美]韦尔伯·施拉姆著，金燕宁等译，《大众传播媒介与社会发展》，北京：华夏出版社，1990 年第 1 版，第 60-63 页。

[54] 参见：Abraham M. Denmark, “Managing the Global Commons,” *The Washington Quarterly*, Vol. 33, No. 3 (June 2010), pp. 165-182; Susan J. Buck, *The Global Commons: An Introduction*, Washington, D. C.: Island Press, 1998, p. 1；任琳：《全球公域：不均衡环球化世界中的治理与权力》，载《国际安全研究》，2011 年第 6 期，第 114-128 页；马建英：《美国全球公域战略评析》，载《现代国际关系》， 2013 年第 2 期，第 7-12 页。

字地址分配机构”仍然把持着互联网地址的分配、根服务器等核心资源的控制权、与世界最大的路由器服务商思科公司密切合作）和网络空间规范的主导权。[55] 即使美国近期放出了下放网络资源的控制权和网络空间规范的主导权的口风，但目前的行动力度依然不明。而中国一贯主张，互联网有关的各类公共政策问题隶属国家主权，作为国家重要基础设施的互联网属于中华人民共和国主权的管辖范围。[56] 但当我们罗列中美两国所关心的网络相关问题时，我们发现了诸多共同点：美国关心关键基础设施的安全、网络空间行动自由、商业技术机密安全；而中国关心社会政治稳定、信息基础设施和网络系统安全、网络信息和数据安全。[57] 在与网络相关的基础设施安全、打击网络恐怖主义和维护信息安全等方面，中美享有诸多共识，可以开展密切合作。

各行为体更乐于参与网络安全的治理，有借助双边对话推动的网络安全合作，也有借助区域性组织平台开展的网络安全合作；此外，传统国际组织平台也被常常应用于全球网络安全的治理活动之中，近年以来大国牵头的双边合作尤其活跃。

1. 大国牵头的双边网络安全合作越来越活跃

网络安全领域内的合作逐渐成为中美合作的新焦点。在 2013 年的第五轮中美战略与经济对话中，网络安全议题被作为焦点议题提出，同年还成立了中美网络安全工作小组。[58] 美英的网络合作具有较长历史，2015 年 1 月，英国首相卡梅伦和奥巴马于在联合新闻发布会上宣布，英美两国今后将通过分享情报、模拟试验、包括测试两国银行系统抗进攻能力等方式加大网络安全合作。[59] 美俄也将网络安全合作纳入双边安全合作的重要领域清单之中。[60]

2. 主要国家核心的区域性网络安全合作方兴未艾

以欧洲国家为例，欧盟相继通过了诸多网络安全治理的决议，例如，2002 年的《关于在网络和信息安全领域的共同方法和具体行动》、2006 年的《建立欧洲

---

[55] 王义桅：《全球公域与美国巧霸权》，载《同济大学学报（社会科学版）》，2012 年第 2 期，第 49-54 页。

[56] World Summit on Information Society, “Building the Information Society: A Global Challenge in the New Millennium,” Declaration of Principles of First Phase of the WSIS, December 12, 2003, p. 7.

[57] 周琪等：《网络安全与中美新型大国关系》，载《当代世界》，2013 年第 11 期，第 30-34 页。

[58] 《第五轮中美战略与经济对话框架下经济对话联合成果情况说明（全文）》，新华网，http://news.xinhuanet.com/politics/2013-07/13/c_116523398.htm?anchor=1。

[59] http://news.china.com.cn/world/2015-01/19/content_34597589.htm，登录日期：1 月 17 日。

[60] Press TV (Iran), “United States, Russia Sign First Cyber-security Pact,” June 18, 2013, http://www.presstv.com/detail/2013/06/18/309698/us-russia-sign-1st-cybersecurity-pact。

信息安全社会战略的决议》和 2013 年通过的《欧盟统一安全战略》等，[61] 依此作为区域内网络安全治理的行动纲领。欧洲委员会在2001年通过了《网络犯罪公约》，避免了区域内各国由于量刑不一可能引发的纠纷，在欧洲区域层面上对治理网络安全提供了可行性方案，对具有跨境性的网络犯罪提出了有针对性的治理方案。

3. 传统国际组织继续发挥作用

在联合国框架下，有《联合国反跨国有组织犯罪公约》、联合国毒品控制和犯罪预防办公室、联合国经社理事会、互联网治理工作组、互联网治理论坛等组织平台与规范框架。在国际电信联盟框架下，有全球网络犯罪议程等相关报告和文件，例如《关于网络安全和网络犯罪的全球协议》，就协调各方力量、共同治理网络安全问题提供了诸多规范文本上的支持。这些传统的规范框架与组织平台为打击网络犯罪提供了必要的国际法依据，统筹各方行为。

我们不得不承认，在很多方面，我们依然不能将合作的潜在获益充分转化为大国的合作意愿，但近期的这些合作努力也说明了大国对网络空间内安全获取渠道的重新认识。通过彼此猜忌的制衡战略谋取安全的方式并不可靠，合作治理才是获取安全的重要渠道。

四　结论

本文回顾了传统安全领域中制衡战略的逻辑，讨论了威胁制衡论、利益制衡论、实力门槛论等几种典型的制衡战略在实际应用中不断修正的表现。在讨论了制衡战略的现实影响、可能缺位和迟到的情况之后，引发了我们对制衡战略进行了深度反思。进而，本文将制衡战略过渡到一个非传统安全领域内，即网络环境对安全问题的重构，例如网络世界没有地理的概念、不受投放能力限制、网络环境中各行为体（包括政府和非政府组织）都有能力发动袭击，主体显得更为丰富。那么在网络这一非传统安全的领域内，是否会有制衡战略的其他替代性战略选择，例如，追随、不介入或者再进一步选择抛弃过度的战略警戒而采取合作的姿态？一般来说，体系压力、战略博弈和安全诉求会使国家趋向于选择制衡战略。但地理限制、实力对比和意图传递等因素都可能导致制衡缺位的现象发生。特别是在

[61] Commission of the European Communities, A Strategy for a Secure Information Society-“Dialogue, Partnership and Empowerment,” COM (2006)251, May 31, 2006; 蒋丽等：《国际网络安全合作的困境和出路》，载《现代国际关系》，2013 年第 9 期，第 52-58 页。

网络空间里，各类沟通机制不畅、意图传递受阻、威慑等战略工具失灵，制衡战略无法呈现出显性效果。所以，国家更加倾向于谋求合作或追随的战略。其中，霸权国更能够且乐意提供更多的公共产品；网络大国更加青睐通过合作规避非传统、非对称、难溯源的安全隐患。网络资源大国更具合作倾向的原因包括谋求安全的手段发生改变、大国提供公共物品的能力更充足、网络领域内大国合作可以带来巨大的安全和经济利益。

联系邮箱：deuyut@163.com