大国网络空间安全博弈：一种复杂系统分析视角

孔亦思　李抒音

【内容提要】　网络空间是人造虚拟的社会空间，随着技术发展和普及运用而持续演进，网络空间安全问题成为国家安全问题。网络空间安全博弈是当前大国博弈背景下的一种典型国际现象，具有辩证性、历史性和策略性，大国是最主要的行为体。以国际互联网为主体的网络空间是复杂系统，大国在网络空间安全领域的博弈互动也构成不断演进的复杂结构，因此复杂性科学理论是分析大国网络空间安全博弈问题可行且合适的视角。本文提出，可以将复杂性科学作为认识论引入，将大国网络空间安全博弈视为一个复杂系统，具有整体不可还原、影响因素纠葛、因果关系复杂、个体随势而动等与其他社会复杂系统类似的属性，同时具有针对性、混合性、长期性等独特属性。本文提出一个对复杂系统的初步分析框架，涵盖三个维度：一是从历史维度把握动态演进和复杂状态，紧紧围绕大国战略博弈、网络领域发展两条核心线索，以整体性特征变化为牵引概括阶段性特点，不必精确框定“突变”时间节点；二是从机理维度把握影响因素的复杂作用和矛盾关系，观念因素和物质因素是具有关键作用的两类核心变量，观念因素即博弈的思想渊源与基础问题决定国家“选择去做什么”，而物质因素即博弈的资源禀赋和综合实力问题决定国家“能够做些什么”；三是从行为维度把握互动模式和策略重点，大国会基于国家安全利益需求和自身实力基础选择合适的博弈策略，并综合运用国家实力要素和各种手段，最大化保证博弈目标实现，不同领域涉及能力手段的差异化、策略性运用。

【关 键 词】　网络空间安全　大国博弈　大国竞争　复杂系统

【作者简介】　孔亦思，军事科学院博士研究生；李抒音，军事科学院研究员、博士生导师。

当前，大国战略博弈日趋激烈。与 20 世纪美苏冷战不同，网络空间这个非自然地理空间首次成为大国博弈的关键“增量”和“变量”，网络空间安全问题成为大国的重要关切，派生出的资源分配、价值冲突、秩序建立等重大现实问题，深刻体现出大国博弈的长期性、复杂性、对抗性。网络空间安全博弈是大国博弈的内在组成部分和必然结果，是当前重要的国际政治现象，研究该问题适逢其时。什么是网络空间安全博弈？如何认识和分析大国在网络空间安全领域的博弈现象？目前的相关研究主要侧重于现实情况跟踪和具体问题分析，因此需要在深入解析基本概念的基础上，形成一条能够系统认知大国复杂互动的分析路径。本文首先梳理“网络空间”“网络空间安全”“网络空间安全博弈”等概念，厘清博弈问题的指向与边界；其次，借鉴复杂性科学思想，将大国网络空间安全博弈视为一个复杂系统，分析其主要特征和战略效应；最后，探索提出一个涵盖历史、机理、行为三个维度的初步分析框架。

一　对网络空间安全博弈问题的基本认识

（一）网络空间：从科幻想象到现实存在

什么是网络空间？从不同视角出发会得出不同答案。普通网民日常感受到的是互联网，技术人员认为是信息技术，社会学者理解为公共空间，政客视作影响广泛的政治场域……虽然信息网络已走进千家万户，但关于网络空间的概念却并未完全形成共识，各国有不同定义。

20 世纪 80 年代，美国科幻作家威廉·吉布森借用“控制论”（cybernetics）前缀（cyber），造出 cyberspace 这个复合词，表示一个全新的计算机技术空间①。这个空间是想象力的天堂，具有理想化、无限性、未来性、虚拟性等特点。虽然吉布森的科幻想象与后来的现实出入很大，但是 cyberspace 这个新词却得以保留，并且被美国政府借用后普及全球。美国政府常将 cyberspace 简称为 cyber，与陆海空天并列为第五域，并衍生出 cyber security、cyber threat 等术语。

① Annalee Newitz，“William Gibson Says Cyberspace Was Inspired by 8 - bit Videogames”. https：//gizmodo. com/william - gibson - says - cyberspace - was - inspired - by - 8 - bit - vi - 5815019，访问时间：2024 年 3 月 20 日。

Cyberspace 进入我国后，常见翻译有“赛博空间”“网电空间”“控制空间”等①，在很长一段时间内没有统一的对应术语。这些音译和意译术语要么不符合国内使用习惯，要么与实际意涵出入较大，均不太贴切，给学术研究平添很多麻烦和困惑。经过多年探索，国内现在统一译为“网络空间”。实际上，中文语境下的“网络”可对应 network②（信息网络或其他功能网络）和 cyber（网络空间的简称）两个词语，日常使用“网络”时常常不加以区分。

“网络”这个概念从“信息网络”（network）发展到“网络空间”（cyberspace），内涵发生重大变化：其一，从技术性发展出社会性。俄罗斯学者彼得罗夫认为，空间是支配社会关系的基本概念和地缘政治的主要概念，地缘政治的主要内容是争夺对空间的控制和支配权力③。因此，增加“空间”一词组成的“网络空间”术语，不仅涵盖具体的信息网络，更突出其中开展的社会活动和存续的社会关系。其二，性质从作用媒介拓展为功能领域。对此，美军用“在网络空间”和“通过网络空间”（in or through cyberspace）加以区分。《网络空间作战联合条令》定义，“网络空间作战指运用网络空间能力，在或通过网络空间实现各种目的”④。这个定义涵盖两个方面：一是将网络空间视为目标指向，二是将网络空间视为达成目的的媒介。美国学者从效果角度进一步阐释，“在网络空间”和“通过网络空间”都指源于网络空间的行动，但目的分别是在网络空间制造效应和在陆海空天等物理域制造效应⑤。

俄学界引入 cyberspace 后，创造出音译新词 киберпространство（简称 кибер）。俄官方坚持使用具有本国特色的“信息空间”概念体系（информационное

① 戴浩：《赛博空间概念的由来及译名探讨》，http：//www. sicris. cn/CN/news/news85. shtml，访问时间：2024 年 3 月 28 日。

② Network 一词由来已久，不论其指代对象如何演变，根本特征就是互联互通。16 世纪以前，network 指代线条交错的编织物，17～18 世纪指代科学家研究的血脉循环系统等自然网络，19 世纪开始比喻人际关系和交通网络，20 世纪后期拓展到能源、计算机、电视电话等领域。参见：〔英〕尼尔·弗格森：《广场与高塔》，周逵等译，中信出版社 2020 年版，第 22～23 页。

③ 〔俄〕瓦列里·列昂尼多维奇·彼得罗夫：《俄罗斯地缘政治：复兴还是灭亡》，于宝林等译，中国社会科学出版社 2008 年版。

④ “JP 3－12 Cyberspace Operations”，Joint Chiefs of Staff，2018.

⑤ Michael P. Fischerkeller，et al. *Cyber Persistence Theory*：*Redefining National Security in Cyberspace*，Oxford University Press，2022，p. 167.

пространство），始终没有正式接纳 кибер 术语。一方面，网络空间与信息空间①这两个概念密切相关，前者从属于后者。俄美学者 2011 年达成一致，认为网络空间是信息空间的一个子集和当前最需要关注的领域②。另一方面，这两个概念有很大区别。其一，内涵不同。信息空间概念体系聚焦信息本身及其利用过程，将网络视为信息的一种媒介或环境，没有充分拓展网络空间作为新兴领域的内涵与价值。实际上，网络空间不仅涵盖其中的信息资源，更突出强调作为载体的网络基础设施和系统，因此更能体现网络时代特征。其二，运用差异。美国率先提出网络空间概念并最早纳入国家安全战略，引领全球网络空间概念规范化和政策构建。但也有学者开始反思，网络空间比信息空间概念更加狭隘，美国政策规范都以网络空间概念体系为基础，无法有效应对其他国家综合运用网络和非网络手段造成的混合威胁③。相较而言，俄罗斯则一直认为信息空间涵盖社会、精神、技术等所有方面，网络空间仅仅是信息空间的技术层面，因此只制定信息空间战略政策。俄学者沙里科夫指出，信息安全、信息空间等术语在俄罗斯有其哲学和精神内涵，技术是众多要素之一，且未必是最重要的要素④。

网络空间概念体系的不同会直接影响并导致国家网络空间行为方式的不同。以俄美为例，俄军事学者波波夫和哈姆扎托夫在 2016 年出版的专著《未来战争：概念基础与实践结论》中指出，网络空间军事行动发生在物理域、信息域、人类圈三个领域内。这背后的认知基础是，网络空间要从物理域、信息域和认知域三

① “信息空间”比“网络空间”概念更早出现. 有些文献也表述为“信息领域”或“信息环境”。知网检索发现，20 世纪八九十年代国内已有这些概念的相关研究，如李必祥 1996 年发表的《试论信息空间与信息空间结构》、叶青 1988 年发表的《信息空间与精神空间》等文章。以目前的视角看，其所探讨的问题侧重网络空间的信息和认知层面。“信息安全”这个概念出现于 50 年代，90 年代已进入国家政策文件。随着计算机和网络的发展，“计算机安全”“信息网络安全”“网络信息安全”等概念渐次出现。90 年代后期，“网络空间安全”概念出现并逐渐成为主要术语，除“信息安全”之外的其他近似术语基本弃用。参见王世伟：《论信息安全、网络安全、网络空间安全》，载《中国图书馆学报》2015 年第 2 期。

② Karl Frederick Rauscher and Valery Yaschenko，eds.，“Russia – U. S. Bilateral on Cybersecurity：Critical Terminology Foundations”，EastWest Institute，Moscow State University Information Security Institute，2011.

③ Bryan James Nakayama，“Information vs the Cyberspace Domain”，*Journal of Cyber Policy*，Vol. 7，No. 2，2022，pp. 213 – 229.

④ Pavel Sharikov. “Cybersecurity in Russian – US Relations”，Center for International Security Studies，2013.

个维度去把握。美国《网络空间作战联合条令》则将网络空间分为物理层、逻辑层和网络角色层等“三层”结构空间，并据此开展行动①。

（二）网络空间安全：在差异下寻求最大共识

在“网络空间”概念尚存分歧时，定义“网络空间安全”更非易事：其一，安全边界难以界定。网络空间安全②到底要纳入和排除哪些要素，不仅是学术问题，更是实践行动问题。安全的内涵过于宽泛会导致过度夸大威胁，反而忽略真正重要的安全问题；而安全的内涵过于狭隘则会导致聚焦技术细节，难以综合考量全局影响。其二，安全认知动态演变。有学者将国家对网络空间安全的战略定位演变划分为三个阶段，一是作为技术概念聚焦恶意软件和系统入侵活动，二是作为执法概念聚焦网络犯罪和间谍行为，三是作为军事政治概念聚焦网络冲突和国内基础设施保护等问题③。安全环境影响安全认知，安全认知反过来塑造安全形势。军事政治概念的认知暗含着国家在网络空间有“假想敌”威胁，要就此发展安全能力、制定安全措施，这种过度安全反应反而加剧国家关系中的紧张氛围。其三，安全共识难以建立。以俄美为例，冷战时期，美苏对核安全具有相近认知，双方都掌握先进核武器技术，都清楚核战争的灾难性后果。当前，俄美两国在网络空间领域的概念体系完全不同，始终难以在官方层面达成共识，因此在实践中更容易导致相互误判。

网络空间安全实质是网络空间行为体之间复杂互动的产物，是一定时空范围内网络空间处于一种理想的相对安全状态，是主观认知不感到恐惧、客观现实相对没有危险和威胁的有机统一，是消除威胁、保障持续安全状态的能力及其运用过程。网络空间难以实现绝对安全和永久安全，安全在时间、空间、程度等方面具有相对性和变化性。

---

① “三层”结构空间分别是：物理层，由物理域信息技术设备和基础设施组成；逻辑层，由计算机代码及其逻辑关系组成，是对物理层关联关系的抽象表达；网络角色层，网络账号构成，是对逻辑层数据的抽象表达。参见“JP 3 - 12 Cyberspace Operations”，Joint Chiefs of Staff 2018.

② 本文研究的是“网络空间安全”问题（security of cyberspace），指代网络空间领域的综合安全，强调全局性；“信息网络安全”（network security）指代具体的信息网络安全状况，是前者的子集和技术层面。如无特别说明，本文所用“网络安全”是“网络空间安全”的简称。

③ Cavelty M D，“The Militarisation of Cyberspace：Why Less May Be Better”，2012 4th International Conference on Cyber Conflict（CYCON 2012），IEEE，2012，pp. 1 - 13.

对网络空间安全涵盖内容的认识可归结为两类：一是技术角度，网络空间安全的定义往往包含数据、技术、系统和服务、信息基础设施、人员及其在网络空间的活动等，这是当前最常见的定义方式；二是非技术角度，网络空间安全涵盖政治、国防、经济、文化等方面安全。俄学者库拉金指出，安全的领域已经扩展到世界相互作用的所有领域，每个领域都有自己的特点和有别于其他领域的规律性①。方滨兴院士的定义兼具这两种角度，不仅从技术层面框定网络空间安全的内容范畴，体现网络空间的技术性特征，还从非技术层面纳入网络空间安全的外部影响，把其他领域安全视为网络空间安全带来的次生安全问题②。

研究网络空间安全既要关注微观的技术问题，如具体的网络安全状态、防护能力举措，也要关照宏观的战略问题，即网络空间的整体安全态势和由此产生的战略层面影响③。国家安全视角是审视网络空间安全问题的最合适切入点。

一是网络空间安全是国家安全的重要组成部分。国家安全如果是一个大“拼图”，网络空间安全就是其中的关键一片，是使之完整的前提条件；网络空间安全与其他领域国家安全问题紧密嵌套，相互影响。在网络时代，网络空间安全虽然只是国家安全的一个领域，但其影响是全域渗透的。

二是网络空间安全的旨归在于国家安全需求。王逸舟指出，国家安全是相对于其他国家而言的概念，所追求的目标体现国家和人民在国际政治背景下寻求保障、排除危险、长久存续的根本需求④。网络空间安全首先反映本国安全追求，其中必然存在与他国的差异化需求，以及共同的安全渴望。

三是网络空间安全要兼顾国内和国际方面。国家安全同时具有外部属性和内部成分，只有结合起来才能构成国家安全的“完整画面”⑤。网络空间安全既是国内问题，也是国际问题，两者虽然处在不同层次，有各自的理论基础和前提假定，但是彼此之间密切联系，无法完全割裂。李少军认为，国际安全是国家安全的表现形式和实现手段⑥。就这个意义而言，网络空间国际安全问题寓于网络空间国家安全

① 〔俄〕B. M. 库拉金：《国际安全》，钮菊生等译，武汉大学出版社 2009 年版，第 2 页。

② 方滨兴主编：《论网络空间主权》，科学出版社 2017 年版，第 57 页。

③ 中国现代国际关系研究院总体国家安全观研究中心编：《网络与国家安全》，时事出版社 2022 年版，第 8 页。

④ 王逸舟：《国家安全研究的理论与现实：几点思考》，载《国际安全研究》2023 年第 2 期。

⑤ 同上。

⑥ 李少军：《论安全理论的基本概念》，载《欧洲》1997 年第 1 期。

的大范畴之中。从国内看，网络空间安全涉及法规制定、打击犯罪、建设安全体系等诸多事务；从国际看，要维护网络空间国际和平稳定，避免发生网络冲突。

四是要形成国家网络空间安全观。网络空间安全观是国家安全观的组成部分，是网络空间行为体对安全利益和目标、安全威胁及应对的综合性、整体性看法，是客观见之于主观的理性认识，在长期积累的过程中逐步形成，具有延续性和相对稳定性。其中包含着网络空间安全内涵认识、网络空间利益界定、网络安全威胁感知等诸多方面，本质上就是回答网络空间安全是什么、要什么以及难在哪的问题。以网络安全威胁为例，各国当前并未对网络威胁的性质和重点完全达成共识。常见的威胁划分方式是按照所用技术、危害程度、危害对象和内外来源等加以界定，要么过于抽象而难以有效落实为应对措施，要么过于具体而无法关联到宏观影响。其根本原因在于没有从国家安全视角出发形成整体性的网络空间安全观，因此缺乏对基本概念和利益的前置判定。李少军指出，行为体之间正是因为安全观不同，才倾向于采取不同的威胁应对途径①。因此，安全观差异也是国家在网络空间安全问题上相互博弈的原因之一。

（三）网络空间安全博弈：从约定俗成到学术建构

网络空间安全博弈，就是两个或两个以上国际行为体为实现各自目的和利益，针对网络空间安全问题，从战略到技术等各层次开展的错综复杂的互动过程。网络空间安全博弈是当前大国博弈背景下的一种典型国际现象，反映了国际行为体（特别是国家）间关系，体现了不断演进的互动状态。作为从现象抽象出来的概念，网络空间安全博弈本质上是行为体在网络空间安全领域的综合较量，其内涵要靠具体实践所赋予。

按照不同的分类方式，网络空间安全博弈至少涵盖以下类型：以问题领域为标准，分为网络空间军事安全博弈、网络空间政治安全博弈、网络空间文化安全博弈等；以功能领域为标准，分为网络空间制度博弈、网络空间资源博弈等；以烈度水平为标准，分为网络空间合作、网络空间竞争、网络空间对抗等；以各方得失为标准，分为网络空间零和博弈、网络空间正和博弈等。零和博弈是恶性互动，博弈方消耗大量资源和代价开展交锋甚至发生冲突，结果是一方利益受损甚至两败俱伤。

网络空间安全博弈作为国际行为体在网络空间领域互动的重要形态和典型现

① 李少军、李开盛：《国际安全新论》，中国社会科学出版社 2018 年版。

象，具有以下特征：一是辩证性。网络空间安全博弈是矛盾的统一体，博弈方作为对立面而相互依存、互为前提，在网络空间互动中相互借鉴，同时博弈方相互排斥甚至对抗，导致各方网络空间实力的变化和网络空间安全态势的失衡。就像牛顿定律中作用力与反作用力一样，博弈方在互动中的作为也会反作用于自身，形成施动与受动的复杂结构。

二是时代性。网络空间安全博弈是与时俱进的，在具体形态和表现形式上必然反映当时的国际政治环境、博弈方外交关系、网络技术发展等背景因素，体现出差异化的阶段特征和时代属性。例如，国际上对网络空间行为的关注点已经升级为国家背景的有组织行动，在制定国际规范时，博弈重点和议程也随之转变。

三是策略性。博弈互动充满不确定性，但同时也具有艺术性，本质上是多个行为体之间的策略性互动。虽然实力是博弈方的根本依托，但是策略在博弈过程中能够发挥举足轻重的作用，是影响博弈结果的关键因素。博弈方总是拥有一定的策略选择空间，策略偏好与选择取决于博弈方的价值观念、威胁认知和实力限度等多方面原因。

网络空间安全博弈主体是国际政治行为体在网络空间领域的延伸。国家是国际政治的基本单元和主要行为体，决定网络空间安全博弈的主要层面和表现形态，因此要把国家特别是大国作为研究重点。学界常按照实力水平界定大国，这就需要明确的衡量标准①。就网络空间而言，英国国际战略研究所按照网络实力将国家分为三类：第一梯队是具有全面领先优势的国家（仅美国），第二梯队是在某些方面具有世界领先优势的国家（中、俄等国），第三梯队是在某些方面具

① 杨原认为，大国是有潜力或实力竞争世界霸权、拥有洲级规模的国家，测度标准是自身安全不依靠他国保护，冷战时期的美苏和 21 世纪的中美符合标准；布赞认为，大国的标准包括物质实力和社会角色两种线索，按层次分为三类，美国是唯一超级大国，英/法/德、日本、中国、俄罗斯是大国，另外还有一些地区大国；林奇认为，大国要拥有非同寻常的能力、在近邻之外追求广泛的外交利益、被其他国家按照有影响力的地位来对待，美国、俄罗斯和中国符合大国标准。参见杨原：《大国无战争时代的大国权力竞争：行为原理与互动机制》，中国社会科学出版社 2017 年版，第 17～21 页；〔英〕巴里·布赞：《美国和诸大国：21 世纪的世界政治》，刘永涛译，上海人民出版社 2007 年版，第 59～75 页；Thomas F. Lynch III ed，*Strategic Assessment 2020：Into a New Era of Great Power Competition*，Washington，DC：National Defense University Press，2020. p. 4.

有优势或潜力、但在某些方面存在重大劣势的国家①。可以看出，国际政治传统意义上的大国与网络空间综合实力领先的国家往往有交叉重叠。本文认为，网络空间领域的大国具有塑造和改变网络空间国际结构的实力、行为和地位。

大国在当前的国际网络空间安全博弈中具有主体性地位，原因在于：一是网络空间是大国新的权力来源。各国对互联网依赖程度越来越高，网络空间成为社会经济发展和国家安全的重要基础，甚至关涉国家前途命运。掌控一个国家的网络数据和平台设施，一定程度上意味着具备塑造该国社会行为和观念的能力。“可以控制和塑造的东西通过有指导的行为就转化为权力”②，由此，网络空间作为新的权力来源和获取权力的工具，必然成为大国重视的“必争之地”。

二是大国在网络空间占有实力优势。虽然在治理格局和秩序规范未定之时，网络空间能以非对称方式在一定程度上弥补传统领域博弈实力之不足，但是从当前的实践来看，网络空间实力与国家总体实力是总体匹配、适度错位的。小国难以掌握信息技术的生产资料，难以培育有影响力的 IT 企业，网络空间全球化趋势会加速生产要素流动，导致“马太效应”加剧。因此，小国难以利用网络空间对大国实现彻底的、长期的、颠覆性的反超，大国在网络空间安全博弈中持续占据优势的实力、资源和地位。大国与小国之间不存在博弈的对等位置，小国在网络空间更加受制于大国。

二　大国网络空间安全博弈复杂系统

（一）复杂性科学与适用性分析

1. 复杂性科学与国际政治的复杂性思维

“复杂性”（complex）概念诞生于 20 世纪，原因是生物学、经济学等不同领域内存在许多还原论所无法解释的现象，需要新的科学理论和方法。学者抓住各

① “Cyber Capabilities and National Power：a Net Assessment”，International Institute for Strategic Studies，2021.

② Juha Kukkola，“Digital Soviet Union：The Russian National Segment of the Internet as a Alosed National Network Shaped by Strategic Cultural Ideas”，Finnish National Defence University，2020，p. 2.

学科中体现的“复杂性”特征，由此提出“复杂性科学”①（也被称为“复杂性学说”“复杂性理论”）。牛顿科学范式对世界的描绘是一种“钟表宇宙”图景，具有线性、可还原、可分解等特征；复杂性科学则是对牛顿科学范式的颠覆与超越，把世界视为具有复杂性的复杂系统而非简单分解还原的机器。

目前学界对“复杂性”和“复杂系统”等核心概念并没有明确的统一定义。借鉴米歇尔对“复杂系统”的三个定义②，本文将复杂系统概括为：在微观层面，大量个体交互信息并相互作用，产生复杂集体行为；在宏观层面，缺乏集中控制和复杂规则约束，随着时间推移以某种方式涌现整体性变化。复杂性分为物理复杂性、生物复杂性、社会复杂性三类，复杂系统由此可分为三类：一是天气系统、混沌系统等物理复杂系统；二是人体系统、生命系统等生物复杂系统；三是经济系统、社会系统、战争系统等以人为核心的社会复杂系统③。国际政治中的“复杂性”属于社会复杂性，国际政治复杂系统是有生命主体的社会复杂系统。这类具有适应性主体的复杂系统称为“复杂适应性系统”（CAS），也是本文研究重点，其研究路径方法与其他两类完全不同。表 1 列举了简单系统、复合系统（complicated）④、复杂（适应性）系统之间的区别。复杂系统有诸多特性，学界对此多有论述⑤。其中，适应性、不确定性、涌现性三个根本属性概括了复杂系统的基本面貌，其他特性都是在此基础上所衍生出来的。

① 〔美〕梅拉妮·米歇尔：《复杂》，唐璐译，湖南科学技术出版社 2018 年版，第 15 页。

② 第一个定义：大量组分组成的网络，不存在中央控制，通过简单运作规则产生复杂集体行为和复杂信息处理，通过学习和进化产生适应性。第二个定义：具有涌现和自组织行为的系统。第三个定义：由大量相互作用、相对简单的组分构成的系统，没有中央控制和全局通信，组分相互作用导致涌现、自适应等复杂行为。参见：〔美〕梅拉妮·米歇尔：《复杂》。

③ 胡晓峰：《战争科学论：认识和理解战争的科学基础与思维方法》（修订版），科学出版社 2023 年版，第 36～37 页。

④ 复合系统尽管包括大量要素，但从其组成个体可以得到系统整体属性，且往往是封闭系统。复杂系统则不可能只通过分析其组成部分而得到对系统的整体理解，且系统是开放的，要素间关系是流动变化的。

⑤ 王帆：《新开局：复杂系统思维与中国外交战略规划》，世界知识出版社 2014 年版，第 12 页；〔美〕凯文·凯利：《失控：全人类的最终命运和结局》，张行舟等译，电子工业出版社 2016 年版，第 35 页；胡晓峰：《战争科学论：认识和理解战争的科学基础与思维方法》（修订版），科学出版社 2023 年版，第 38～93 页。

表 1　系统类型及特性①

系统类型	要素数量	线性特征	适应性特征	涌现性特征	例子
简单系统	少	线性	无适应性	无涌现性	枪支
复合系统	较多	线性	无适应性	无涌现性	战机
复杂（适应性）系统	较多（也有例外）	非线性	有适应性	有涌现性	飞行员驾驶战机

国际政治吸纳系统科学的理论方法后，侧重从静态角度研究国际政治系统的结构和性质，追求简约的国际政治规律和通则，背后的思想根基主要是牛顿科学范式下静态、机械、线性的宇宙观。正如美国学者所言，“旧的政治运行连同政治科学太过附着于牛顿物理学的启示。而如今随着整个科学界正在远离机械论、原子论和决定主义转而追求新的世界认知范式，现在政治学领域也到了不得不如此跟进的时候”②。国际政治研究引入复杂性科学思想是对原先认识论和方法论的一次超越，更重要的是认识论上的超越。复杂性作为一种跨学科的思维方式，运用到国际政治研究中有助于增强思考范围和描述能力③。秦亚青认为，国际政治研究应当借鉴复杂性思想，但是复杂性并非作为一种严格意义上的国际关系理论存在，而是“信念、预期和世界观的综合，塑造了研究者的问题取向，重视的是解决问题的思路、立场和方法”。至于具体的研究对象和分析方式，主要区别在于：一是研究对象从静态的国际政治结构转化为演化的国际政治复杂系统，不仅涵盖传统理论研究重点的系统结构和互动单元，还包括外部环境因素、系统涌现属性、系统要素间的联系及互动过程；二是分析模式从自上而下的宏观分析，转变为自上而下、自下而上相结合的辩证研究方法，特别要关注微观层面变量复杂互动产生的系统效应④。

---

① 借鉴兰德报告绘制，原表参见：Sherrill Lingel，et al，“Leveraging Complexity in Great – Power Competition and Warfare：Volume II，Technical Details for a Complex Adaptive Systems Lens”，RAND Corporation，2021. p. 3.

② 〔美〕罗伯特·杰维斯：《系统效应：政治与社会生活中的复杂性》（第二版），李少军等译，上海人民出版社 2020 年版，第 4 页。

③ 王逸舟：《国际政治概论》（第二版），北京大学出版社 2016 年版，第 256～259 页。

④ 丁榕俊：《国际政治的复杂性理论》，中国社会科学出版社 2018 年版；刘慧：《复杂系统与世界政治研究》，南京大学出版社 2011 年版。

2. 对大国网络空间安全博弈问题的适用性分析

大国网络空间安全博弈是大国之间以利益为目标、以实力为基础的动态交互过程。目前，对大国网络空间安全博弈的研究侧重于现实情况跟踪和具体问题分析，总体上还处于“零敲碎打”的状态。因此，亟需一个整体性的分析视角，能够超越零散、迅变的现实事件，完整、系统地看待大国之间复杂的博弈互动，进而有助于挖掘大国网络空间安全博弈的内在逻辑和基本规律。

复杂系统是分析大国网络空间安全博弈问题可行且合适的视角，原因在于：一是以国际互联网为主体的网络空间是复杂系统。20 世纪 90 年代，以 TCP/IP 等简单网络协议为基础构建的国际互联网开始走进千家万户，规模呈爆炸式增长，目前已经发展成为覆盖全球、联通万物的庞大体系，涌现出基础协议中没有规定的全新特征。万维网就是自组织的复杂社会系统，个体无法管窥全貌，海量用户的网络活动使得万维网体现出复杂的宏观特性①。由此，还产生了专门研究大规模网络特性的复杂网络科学和网络思维②。凯文·凯利指出，21 世纪科学的象征是网络，网络是所有大规模系统的原型、群体的象征，“群体将自我撒在整个网络，无数个体思维聚集在一起形成不可逆转的社会性”，加上时间维度的网络与其说是一个物体和一种资源，不如说是某种过程、流程和行为③。

二是大国在网络空间安全领域的博弈互动构成不断演进的复杂系统。大国互动是网络空间国际体系的基本形态，大国关系在互动过程中不断演变，塑造着网络空间国际体系的整体演进方向。割裂、孤立地考察大国某些网络行为或者某些网络事件，无法还原和廓清网络空间国际体系的整体面貌。大国网络空间安全博弈不仅塑造了自身地位，也在不断塑造国际体系本身，大国网络空间安全博弈复杂系统既是大国网络安全状态，也是大国网络互动的时空结构与进程。

需要强调的是，复杂系统的分析视角有其限度。目前，学界尚未对复杂性科学基本概念和原理形成完整、统一的理论，甚至在建模和形式化研究方法上也有待进一步发展。因此，用复杂系统的视角分析大国网络空间安全博弈问题不是给

① 〔美〕梅拉妮·米歇尔：《复杂》，第 310～318 页。

② 20 世纪末，小世界模型和无尺度网络的论文发表，掀起了复杂网络研究热潮。复杂网络科学研究对象是包括互联网在内的各种类型的关系网络。网络思维指更关注事务间联系而非事务本身的一种思维方式。

③ 〔美〕凯文·凯利：《失控：全人类的最终命运和结局》，第 39～42 页。

出具体和确定的答案，其价值在于突出强调大国互动过程中的复杂特性，提供了一个新的观察窗口和启示性的思考指向。

（二）博弈复杂系统分析

1. 主要特征

大国网络空间安全博弈是复杂系统，具有与其他社会复杂系统一样的复杂性特征，具体表现在：一是整体不可还原。网络空间安全事件不同于物理空间冲突，单一网络事件不能完全反映大国网络空间安全博弈的整体面貌，也未必能够直接影响国家间关系。以“月光迷宫”攻击事件为例。事后调查发现，美国关键政府部门、军队、高校在此次事件中遭大规模入侵窃密，攻击者的行动模式与所用工具可以关联到俄罗斯政府背景。此次攻击肇始于 1996 年，1998 年 3 月曝光，当年 9 月美国总统访俄时两国发表联合声明强调共同应对信息网络威胁，而 1999 年美国调查组已经将攻击方锁定为俄罗斯黑客，此时攻击仍未停止。

二是影响因素纠葛。事物的产生不仅需要具备产生条件，也受到内外因素共同影响。大国网络空间安全博弈作为一种全局性现象，并非凭空产生，而有其深刻的历史背景和利益需求，影响因素包括国家对内和对外政策、网络空间和其他领域的复杂联动、对手甚至第三方的影响，结果就是各种因素相互交织影响。国家的认知偏差也会影响博弈策略和行为，进一步扰动网络空间整体环境。

三是因果关系复杂。美国学者格雷厄姆·艾利森感叹，“人类事务中因果关系的复杂性困扰着哲学家、法学家和社会学家”①。国家间复杂互动的因果关系不像钟表系统那样容易解析，而是更类似于凯文·凯利所说的“交叉逻辑的海洋”，小动因可能产生大结果，而国家开展博弈的初衷和结果很可能背道而驰。网络空间安全博弈存在多重效应，其中很多是非直接和延期效应。网络空间安全博弈复杂系统层次越是丰富，效应传播链条越长，因果关系越难以判定。

四是个体随势而动。大国博弈归根结底是人和人的对抗。自组织现象就是行为体适应性的常见表现行为，系统内要素依靠内部相互作用而将自身组织起来适应环境变化。在整体博弈系统中，具有适应性的社会组织和个体根据外部环境和整体形势，发挥主观能动性，自组织、自同步，快速开展网络空间集体行动，进

① 〔美〕格雷厄姆·艾利森：《注定一战：中美能避免修昔底德陷阱吗?》，陈定定等译，上海人民出版社 2018 年版，第 4 页。

而对大局产生影响。例如，全球规模最大的黑客组织之一“匿名者”没有严格的组织架构，往往是出于国际形势变化，结合团体成员兴趣，在网上自发组织，对一些国家政府、重要设施等开展攻击行动。

五是过程具有不确定性。网络空间的虚拟特征决定了这个领域博弈的过程不确定性更加突出，互动行为是否发生、怎么发生很可能处于“迷雾”之中，国家行为体对相关信息不可能完全掌握，对行动的影响也无法完全预料。在国家间发生矛盾冲突时，往往会有“爱国”黑客或是政府背景网络力量对外国发起网络攻击，但是所用“网络武器”失管失控，反而对本国造成网络安全威胁，这种情况屡见不鲜。2010 年美国和以色列情报机构联合开发了针对伊朗核设施的“震网”病毒，虽然其中嵌入限制传播范围的模块功能，但是很快攻击半径就超出开发人员的意图，扩散到其他国家甚至是攻击来源国①。

六是涌现全新特征。大国在网络空间的深度参与，使得该领域各种因素相互作用，产生全新的整体性特征。涌现并非经常发生，实际上，大国网络空间安全博弈复杂系统总体上处于相对稳定的均衡状态，“进化系统最常见的特征并非变化本身，而是没有变化”。涌现的产生可能由于外部的强烈刺激，也可能由于内部的量变积聚，政治冲击是国家间博弈开始、剧变甚至结束的关键条件②。新特征可能具有非线性，表现为“事与愿违”的现象。互联网发展早期，技术理想主义理念占据网络空间价值取向的主流。互联网先驱约翰·佩里·巴洛 1996 年发表著名的《网络空间独立宣言》，表达网络空间“去政治化”构想。本世纪以来，美国加速推动网络空间政治化和军事化，促使其他大国竞相将网络空间用作战略工具，这与互联网最初的价值取向背道而驰。

大国网络空间安全博弈复杂系统还具有其他重要特征：一是针对性。大国网络空间安全博弈是连续展开的互动过程和以事件为导向的快速突变，博弈重点就是互动最密集、矛盾最激烈的领域。大国网络空间安全博弈是全面较量，囊括政治、经济、军事等各个领域议题。在不同背景环境下，不同国家开展的博弈互动具有不同侧重点，必须具体问题具体分析。例如，可从科技角度分析围绕半导

① Gregg Keizer，“Why Did Stuxnet Worm Spread?”. https：//www. computerworld. com/article/2516109/why - did - stuxnet - worm - spread - . html，访问时间：2024 年 3 月 20 日。

② 政治冲击（political shock）是指程度或价值发生重大而迅速变化的政治因素。参见 Paul F. Diehl and Gary Goert，*War and Peace in International Rivalry*. University of Michigan Press，2000.

体、人工智能等网络信息技术产业的中美竞赛。

二是混合性。根据博弈烈度划分，大国在网络空间领域的互动类型包括合作、竞争甚至对抗。不同类型的互动往往紧密交织甚至同时发生，在某个时空背景下，大国之间不会只是单纯、绝对的合作、竞争或对抗，而是处于某种混合状态。正如凯文·凯利所言，复杂系统中的个体间总是为了获得组织资源和认同而相互竞争又共同合作，竞争本身就会孕育出自发的、松散的合作①。同时也要认识到，在一定时期内，必然有某种类型的互动是大国网络空间博弈的主轴。经典国际关系理论认为，大国是理性主体，其行为背后必然有明确诉求，核心动力是追逐自身利益和实现战略目标。因此，国家对于利益的界定，决定了其在网络空间领域互动的姿态。如果把权力界定为核心利益，则大国争夺权力的行为属于零和博弈，彻底击败对手就是于己有利的最好结果，大国博弈就成为你死我活的生存之争，必然以竞争和对抗为基调；如果把共同安全视为相互交织的共同利益，则大国可以在博弈互动中加强合作、在合作中维持适度竞争，最终达成互利共赢的局面。

三是长期性。大国自身往往极具韧性，面对外界网络威胁时一般都能快速从中恢复并汲取教训，进一步夯实自身安全体系。而且网络空间不同于物理空间，不可能依靠一场决定性战争就彻底颠覆权力格局，变更体系秩序。大国网络空间安全博弈的基础是网络空间综合实力，实力消长是一个漫长的过程，这决定了大国网络空间安全博弈必将作为长期现象和过程而存在。“长远眼光是竞争思维的内在要素，持久竞争中没有输赢的结果，而是处于输赢的过程中，每一次挫折都蕴含着未来成功的可能，每一次胜利都蕴藏着可能失败的种子”②。因此，大国在博弈过程中必须坚定决心、保持耐心，不仅要关注短期目标实现，也要关照长期利益得失。

2. 战略效应

大国网络空间安全博弈是战略性现象，战略性指的是博弈利益目标的重大性、时间的长期性、范围的全面性、影响的全局性③。就影响而言，互动可能发生在低层次，效果震荡到战略层面；也可能发生在战略层，但是效果不彰显。从

① 〔美〕凯文·凯利：《失控：全人类的最终命运和结局》，张行舟等译，电子工业出版社 2016 年版，第 67 页。

② “JDN 1 – 19 Competition Continuum”, Joint Chiefs of Staff, 2019, p. 7.

③ 吴心伯：《论中美战略竞争》，载《世界经济与政治》2020 年第 5 期。

全局考察大国网络空间安全博弈的战略效应时，需要辩证看待：

一是负面效应。21 世纪以来，网络空间进入国家安全的方方面面，网络化的民生基础设施、军事信息系统等成为国家安全的脆弱点，网络空间安全问题从技术层面上升到战略层面，成为大国战略博弈的重要组成部分。同时，在网络空间开展攻击行动的技术门槛更低、成本更低、面临的追责风险更低，网络空间是比传统空间性价比更高的大国博弈选项。由此，网络空间安全博弈成为大国的矛盾焦点，在大国普遍推进网络空间军事化的背景下，甚至可能导致新的升级风险，对大国关系和战略稳定造成负面影响。实际上，大国紧张关系和博弈斗争既是网络空间不安全的结果，也是网络空间不安全的根源之一，甚至可能导致网络安全困境加剧和网络军备竞赛升级，增加战略误判和意外事件风险。

二是正面效应。20 世纪美苏博弈背景下的军用技术竞赛诞生了互联网，促使人类社会走进信息网络时代。大国网络空间安全博弈可能会促使国家不断发展新的网络信息技术、完善网络防御体系，推动全球层面的网络空间安全技术和能力发展。同时，博弈还深刻影响网络空间国际格局，推动网络空间秩序形成。以中美为例，两国博弈更多的是关于网络空间怎样长治久安的博弈，考验的是国家发展和治理能力，而非网络攻防等传统安全对抗行动，中美博弈结果很大程度上将决定网络空间未来的国际秩序和价值取向。

3. 分析框架

本文提出一个初步的分析框架（见图 1），从历史、机理、行为这三个不同的维度，分析和把握大国网络空间安全博弈复杂系统。一方面，虽然不能完全描绘系统的全部面貌，但是把大国网络空间安全博弈所涉及的诸多具体问题涵盖在一个框架中分析，有助于整体把握其相互关系。另一方面，强调大国网络空间安全博弈问题的复杂性特征及其表现，有助于超脱不断变化的现实情况，加深对博弈问题的基本认识。

一是对博弈进程的历史分析，从历史维度把握大国网络空间安全博弈系统动态演进和复杂状态，追踪博弈复杂系统的“生长性”。博弈是一个历史范畴而非瞬间动作，大国网络空间安全博弈作为一种历史现象，遵从事物发生、发展、演变的历史轨迹。很多文献在梳理历史时选择以网络空间重大事件为边界划分阶段，这种方式存在两方面问题：其一，具有战略性、转折性影响的重大网络事件屈指可数，这样的划分方式主观性强，缺乏普遍共识支撑；网络空间安全博弈是

一个不断演变、连续变化的“光谱”，其“断裂处”和“突变点”很难识别，未必就是单一的重大网络事件。其二，缺乏网络空间与现实空间之间的映射关联，大国网络空间安全博弈是国家战略博弈的重要方面，国家在网络空间的行为取向背后有政治原因和政治运作，本质上服从于大国政治逻辑。虽然网络空间与现实空间的发展在时间和程度上未必完全一致，但这是现实和网络空间映射影响的传导过程，属于合理区间内的交错匹配。总之，博弈演进分析要遵循和体现背后现实空间政治发展的纵向逻辑，紧紧围绕大国战略博弈、网络领域发展两条核心线索，以整体性特征变化为牵引概括阶段性特点，不必精确框定“突变”时间节点。大国网络空间安全博弈的战略认知和举措受国内政治和国际环境诸多影响，不能眉毛胡子一把抓，要抽取关键情况加以分析，同时特别关照三方面关系：一是内外关系，整体看待国内建设与对外博弈；二是互动关系，整体看待一方对另一方的博弈行为；三是虚实关系，整体看待网络空间与其他领域的关系。

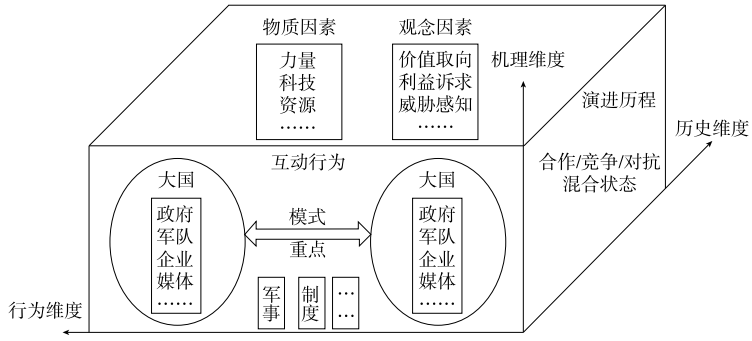

图 1　大国网络空间安全博弈系统分析示意图

同时要注意到，博弈系统始终处于一种混合演进状态。美军认为，传统的平战划分方式已经不足以描述武装冲突门槛下动态竞争的过程，因此创新提出“竞争连续体”概念作为开展长期竞争的全新认知基础，它描述的是一种合作、（低于武装冲突门槛的）竞争、冲突并存的图景，即与同一个国际行为体在不同议题上可以同时以不同的状态开展互动①。林奇指出，“竞争不是冲突的同义词，竞争存在于各国间相互作用的连续光谱上，一端是合作，一端是冲突，各国在不同

① “竞争连续体”不是用“合作、竞争、冲突”三分法替代“和平、战争”二分法。参见“JDN 1－19 Competition Continuum”，Joint Chiefs of Staff，2019，p. 2.

的合作和状态下竞争，目标一致时倾向于合作，目标分歧时走向冲突”①。借鉴这种思想，网络空间安全博弈复杂系统可以视为“博弈连续体”，是合作、竞争、对抗状态的混合体和连续光谱，其中不同的状态因素比重根据具体情况而有所变化。但要注意的是，“博弈 = 合作 + 竞争 + 对抗”这种“三分法”理解并不正确，问题在于：首先，“三分法”聚焦博弈行动和状态，忽略了大国并非单纯要开展这些行动，而是要借此实现预期的整体利益和目标。其次，“三分法”明确地切分行动和状态的类别和边界，忽略了大国网络空间安全博弈的混合状态本质。实际上，大国网络空间安全博弈存在于敌对国家甚至盟友伙伴等友好国家之间。在敌对国家之间，竞争在一定条件下可能升级为对抗；友好国家之间以合作为主，事实上也存在一定程度的竞争，但并不占据主导地位。

二是对影响因素的机理分析，从机理维度把握大国网络空间安全博弈系统影响因素的复杂作用链条和矛盾关系。国际行为体的行为逻辑是国际关系理论研究的一大重点。本文认为，网络空间安全博弈的结构性因素可以分为观念因素和物质因素②两大类，这是对网络空间安全博弈复杂系统具有关键作用的核心变量。国家在网络空间中的行为受观念因素的指导、以物质因素为基础，物质因素变化是观念因素发挥作用的先决条件，观念因素往往在力量对比和国际格局变动之时发挥作用。构成性的观念因素和物质因素交织作用，对网络空间安全博弈复杂系统产生复杂影响，共同产生并塑造网络空间安全博弈现象和结果。观念因素即博弈的思想渊源与基础问题，应当包括价值取向、利益界定和威胁感知等方面，它们相互交织、相辅相成，决定国家“选择去做什么”。价值取向是历史文化的思维惯性，是国家在网络空间领域战略层面表现出的稳定文化特征，对战略思想具有启发意义；利益诉求是国家对自我的战略定位，威胁判断是现实威胁的感知触动。在国际安全研究中，威胁与利益相关，因此分析网络安全威胁，必须先分析网络安全利益；另一方面，面临的安全威胁直接影响国家安全利益内涵，要把握安全威胁的普遍性与特殊性，才能客观界定国家安全利益内涵。任何行为都由选择驱动，不同选择导致不同行为，不同行为导致不同结果。因此，大国在网络安

① Thomas F. Lynch III ed, *Strategic Assessment 2020: Into a New Era of Great Power Competition*, Washington, DC: National Defense University Press, 2020.

② “物质”不仅仅指看得见、摸得着的东西，也是一个抽象概念，指所有不存在于人的“主观性”之中的事物。参见华翔：《国际关系实证主义方法论的思想演变：从“物质”到“观念”》，载《国际论坛》2010 年第 4 期。

全观念因素方面的根本差异和矛盾，是导致网络空间安全博弈的重要原因。

物质因素即博弈的资源禀赋和综合实力问题，应当包括组织力量、科技产业、网络资源等方面，共同决定国家“能够做些什么”。网络实力是国家拥有的网络力量基础和对外博弈能力，是转为网络权力和实现利益目标的前提条件和必要工具，组织力量、科技产业、网络资源等方面因素共同构成国家综合网络实力。国家之间网络实力的不均衡发展会造成国家两极分化甚至引发冲突，因此实力不对等既是开展博弈的物质基础，也是促成博弈的重要原因。在网络空间“牌局博弈”中，国家是“牌手”，物质因素是“牌面”，“牌面”限制了“牌手”的选择限度和行动空间，“牌手”则必须准确掌握自己和对手的“牌面”，也可以通过运筹帷幄增加“牌面”，谋求相对优势和胜势。

三是对博弈互动的行为分析，从行为维度把握大国网络空间安全博弈系统互动模式和策略重点。大国对外开展网络空间安全博弈时，以自身实力和优势为基础，挖掘利用对手薄弱环节，从而最大限度实现己方利益。大国之间的博弈互动会逐渐形成基本模式、主要策略和重点领域。基本博弈模式是对博弈互动现象的规律性概括和基本特征阐述，是大国间经过长期互动后形成、在一定历史背景和时间阶段下具有相对稳定性的产物。策略是根据形势发展而制定的行动方针和斗争方法（原则和方法）。大国基于国家安全利益需求和自身实力基础，做出适合自身的博弈策略选择，然后通过综合运用国家实力要素和各种手段，最有效地保证博弈目标实现。由于网络空间安全博弈是战略层面的国家综合较量，涉及政治、经济、军事、科技、文化等诸多领域，因此不同领域涉及不同能力手段的差异化策略性运用。

结　语

本文主要回答大国网络空间安全博弈是什么、怎么看的问题。网络空间是一个人造空间、虚拟空间，具有持续变化的特性，随着技术的不断发展和人类的深度参与，网络空间将不断演进。网络空间的意义早已超越最初的技术和工具层面，成为重要的社会政治领域。网络空间领域有安全和发展两条主线。网络空间议题“安全化”后，网络空间安全超脱于技术层面的信息网络安全问题，首先被纳入国家安全战略层面加以考量，然后被进一步细分为具体领域安全问题加以处置。网络空间安全问题的实质就是国家安全问题。网络空间安全博弈是当前大

国博弈背景下的一种典型的国际现象，是国际行为体为实现自身目的、针对网络空间安全问题、从战略到技术等各层次开展的错综复杂的互动过程，具有辩证性、历史性和策略性，大国是最主要的行为体。

本文抓住大国网络空间安全博弈现象的复杂性本质，将其视为一个复杂系统。复杂性研究虽然尚未形成完整、统一的理论体系，但是复杂系统具有适应性、不确定性、涌现性等公认的基本特性。复杂性科学思想的引入是对国际政治领域认识论上的超越，对大国网络空间安全博弈问题也同样适用。大国网络空间安全博弈复杂系统具有与其他社会复杂系统类似的复杂属性，包括整体不可还原、因果关系复杂、影响因素纠葛等，同时也具有针对性、混合性、长期性等独特属性，要从全局上辩证看待大国网络空间安全博弈产生的正面和负面效应。最后，本文提出一个大国网络空间安全博弈复杂系统的分析框架，涵盖三个维度：从历史维度把握动态演进和复杂状态、从机理维度把握影响因素的复杂作用链条和矛盾关系、从行为维度把握互动模式和策略重点。

复杂系统研究视角提供了一种整体性、通用性强的分析视角，有助于从纷繁复杂的“线团”中抽取并串联大国复杂互动的主线问题。同时要强调的是，任何一种研究都无法穷尽问题的全部要素，任何一种简化必然与问题本身有所出入，现实世界中大国博弈的复杂性并非单一分析框架所能全面概括。大国无法获得网络空间领域绝对的永久的安全，也无法获得网络空间绝对的永久的主导权，大国网络空间安全博弈问题不存在单一确定解。复杂问题没有简单答案，复杂性科学研究永远在路上。本文只是将复杂性科学作为认识论引入，而非作为方法论运用。网络空间的复杂互动因其永恒变化而永远存在可供研究的问题，如何更好地把复杂性思想与大国博弈问题相结合有待于更加深入的思考。

（责任编辑：王效云）