DOI: 10. 13569 / j. cnki. far. 2015. 05. 117

国际政治中的网络安全: 理论视角与观点争鸣

刘杨钺

摘 要 科学准确地评估网络安全对国际政治的影响，是新世纪以来国际关系和战略研究面临的重要课题。然而，在这个问题上学术界并没有形成共识，而是出现了日益明显的争论与分歧。本文梳理了国际关系视阈下网络安全的三种理论视角，并分别归纳为网络安全威胁忧虑论、网络安全效用怀疑论和网络安全话语建构论。在分析不同视角的基本逻辑与核心主张的基础上，本文进一步探讨了这场论争对国际关系理论发展的启示和意义。正确理解网络技术发展的国际安全意义将是有效指导政策与战略设计的基本前提，也是网络安全领域知识生产和积累的必要途径。

关键词 网络安全 网络冲突 国际关系理论 国际体系

网络技术发展究竟会对国际安全带来怎样的影响? 这个问题无疑是新世纪以来国际关系和战略研究面临的重要课题。截至 2014 年，迅速发展的互联网已经覆盖了全球 42. 3% 的人口 (约 30. 4 亿网络用户) ,[①]各国社会经济发展日益显著地刻上了信息技术的标记。但与此同时，伴随普及率和依赖度而来的网络安全风险不断上升，网络安全已不仅仅是互联网用户的利益关切，而是逐渐成为国家安全战略的核心内容。对“网络珍珠港”、“网络 9·11”等灾难情境

* 刘杨钺，国防科技大学人文与社会科学学院讲师，国防科技大学国际问题研究中心兼职研究员 (长沙 410074) 。

** 本文是作者主持的全军军事科研计划项目 (项目编号: 14QJ004-114) 和湖南省社会科学成果评审委员会委托课题 (项目编号: XSP20140506W) 的阶段性成果。

① 数据来源 “Internet World Stats”, http: //www. internetworldstats. com/stats. htm。

的警告，在美国等西方国家的战略话语中日趋常见。[①] 而这并不意味着对网络安全的忧虑仅仅停留在想象阶段。联合国裁军研究所 2013 年的一份报告指出，全球已有 27 个国家建立了军事网络作战的职能部门，而逾百个国家将网络安全（军事或者民用）纳入了国家政策体系。[②] 现实政治发展无疑强化了对网络安全威胁的认知。从俄罗斯与爱沙尼亚和格鲁吉亚的网络冲突，到美国针对伊朗核设施发动的网络攻击，以及仍在不断发酵的“棱镜门”系列监控计划，[③] 网络安全已越来越多地与国际政治博弈交织在一起，成为国际体系演化发展的新特征和新变量。从这个意义上看，网络安全研究不仅事关各国政策导向与资源配置，也是正确理解和分析新时期国际政治基本态势的迫切需要。

然而，对于如何评估网络安全的国际战略意义，学术界并没有形成共识，而是出现了日益明显的争论与分歧。一方面，网络技术发展被认为将对国际安全产生革命性的影响，[④] 随着网络攻防不断升级和网络依赖性的增强，“电力、油气管道、铁路航空运输、银行、食品流通和其他关键系统都将在国家间网络攻击面前不堪一击”，仿佛国际政治新的“核时代”已然拉开序幕。[⑤] 而另一方面，面对不断出现的网络安全的灾难性话语和情景想象，不少学者开始反思和质疑网络安全究竟能在多大程度上带来国际政治的革命性转变。对网络威胁的描述被认为易于陷入过分夸大和不切实际的假设，而这种过度的安全化举措可能误导国家网络安全的政策。[⑥] 托马斯·里德之所言“网络战争将不会到来”，[⑦] 或许是对这些理论与实践反思所做的最好注释。

在此背景下，本文试图对这场围绕网络安全展开的争鸣进行梳理和总结，

---

① 例如：Leon Panetta，“Remarks by Secretary Panetta on Cybersecurity to the Business Executives for National Security”，2012，http://www.defense.gov/transcripts/transcript.aspx?transcriptid=5136；“U.S. Homeland Chief: Cyber 9/11 Could Happen ‘Imminently’”，*Reuters*，January 24，2013，http://www.reuters.com/article/2013/01/24/us-usa-cyber-threat-idUSBRE90N1A320130124。

② James Lewis，“Cybersecurity and Cyberwarfare: Assessment of National Doctrine and Organization”，in UNIDIR，*The Cyber Index: International Security Trends and Realities*，New York and Geneva，2013.

③ 关于“棱镜门”事件的基本概述，可参见李恒阳 《“斯诺登事件”与美国网络安全政策的调整》，《外交评论》，2014 年第 6 期。

④ Lucas Kello，“The Meaning of the Cyber Revolution: Perils to Theory and Statecraft”，*International Security*，Vol. 38，No. 2，2013，pp. 7-40.

⑤ Richard Clarke，“War from Cyberspace”，*The National Interest*，November/December 2009，pp. 31-36.

⑥ Sean Lawson，“Beyond Cyber-Doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber-Threats”，*Journal of Information Technology & Politics*，Vol. 10，No. 1，2014，pp. 86-103；Lene Hansen and Helen Nissenbaum，“Digital Disaster，Cyber Security，and the Copenhagen School”，*International Studies Quarterly*，Vol. 53，No. 4，2009，pp. 1155-1175；Myriam Dunn Cavelty，“From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse”，*International Studies Review*，Vol. 15，No. 1，2013，pp. 105-122.

⑦ Thomas Rid，*Cyber War Will Not Take Place*，Oxford: Oxford University Press，2013. 该著作由其于 2012 年发表在 *Journal of Strategic Studies* 和 *Foreign Affairs* 等期刊上的相关文章拓展而来。

正确理解网络技术发展的国际安全意义是有效指导政策与战略设计的基本前提，也是网络安全领域知识生产和积累的必要途径。只有掌握了国关学界在网络安全问题上的研究进展，才能在进一步的理论探索和政策实践上避免空洞之言和盲目之举。本文首先对国际关系视角下的网络安全概念加以分析，其次梳理并分析三种不同理论视角的基本逻辑与核心主张，最后着眼于不同网络安全观与国际关系理论发展的关系略加总结和讨论。以此为基础，本文将对如何推动网络安全与战略研究提供思考与建议。

一、国际关系视角下的网络安全

由于“安全”这一“模糊的象征”在国家政策框架中的核心地位，[①] 国际安全研究逐渐成为国际关系领域的重要分支。[②] 其研究议题自冷战结束以来出现了明显的横向拓展，即从传统的军事—政治安全转向其他非传统安全问题。网络空间安全正是在这一背景下进入国际安全研究的话语体系，并由于其日益显现的军事政治意义而开始兼具传统与非传统安全的特征。事实上，网络信息技术的诞生，同冷战时期的大国战略博弈密切相关，[③] 这使得网络空间与国际安全形成了与生俱来的内在联系。然而，即使将目光限定在国际安全视野之下（从而回避了纯粹技术视角下的网络安全研究），网络安全及其相关概念（如网络冲突和网络战争等）也并未产生清晰明确的定义。正如汉森和尼森鲍姆所言，“虽然网络安全问题在政策、媒体和计算机科学等语境下频被提及，但令人惊讶的是，‘安全’一词加上‘网络’的前缀究竟表达着何种意涵，在安全研究领域内却鲜有探讨。”[④]

（一）网络安全的概念内涵

大体而言，网络安全指代了至少两方面的不同意象：一是网络空间面临何种安全威胁，即安全化理论所言之“威胁代理”；二是何者受到网络安全威胁

---

① Arnold Wolfers, “National Security as an Ambiguous Symbol”, *Political Science Quarterly*, Vol. 67, No. 4, 1952, pp. 481-502.

② Barry Buzan and Lene Hansen, *The Evolution of International Security Studies*, Cambridge: Cambridge University Press, 2009.

③ Madeline Carr, “The Political History of the Internet: A Theoretical Approach to the Implications for US Power”, in Sean Costigan and Jake Perry, eds., *Information Technology and International Affairs*, Farnham: Ashgate, 2012.

④ Lene Hansen and Helen Nissenbaum, “Digital Disaster, Cyber Security, and the Copenhagen School”, p. 1156.

并亟须保护，即网络安全的“指涉对象”。[①] 然而，在国际安全话语中，这两种意象相互交织且各自呈现多样化特点，使统一的网络安全概念难以形成。

安全首先意味着远离某种威胁的状态或价值。[②] 当 1989 年计算机病毒被初次发现感染了美国与其他西方国家数千台电脑后，美国总审计局随即发布了一份报告，要求政府部门警惕由网络病毒和其他入侵行为带来的安全风险。[③] 美国国家标准与技术研究所于 1995 年制定了《计算机安全入门》，进一步界定了九种不同的安全威胁，如数据欺诈与盗窃、恶意黑客行为、工业间谍和外国情报窃取等。[④] 随着网络技术日益深入社会生活，对网络安全威胁的感知也随之扩展，相对狭窄的计算机安全概念逐渐为更具包含性的网络安全所替代。安全威胁来源涵盖了一系列相关问题，如服务拒止攻击、网页篡改、网络监视、系统性漏洞等等，[⑤] 而信息物理系统（CPS）和数据采集与监控系统（SCADA）等工业系统中涉及的网络安全问题也日益引起战略关注。[⑥]

严重程度常常被作为区分这些安全威胁性质的主要依据，网络安全也由此被建构为一条包含不同程度威胁的连续体——由程度最低的非蓄意事故（如软件或系统错误）向程度最高的网络战争延伸。位于两个极端之间的则是网络犯罪、网络间谍和网络恐怖主义等不同形式的恶意行为。[⑦] 然而，这种网络安全威胁的光谱式描述实则有着重要缺陷。网络空间冲突涉及的行为主体众多，难以通过参与行为体的特征进行定义和区分。例如，网络间谍行为既可以是国家层面的战略互动，也可以是商业活动所致，而归因问题更使得不同类型的网络

---

① 有关安全化理论的集中论述，参见〔英〕巴瑞·布赞、奥利·维夫、迪·怀尔德《新安全论》，朱宁译，杭州：浙江人民出版社，2003 年；Michael Williams, “Words, Images, Enemies: Securitization and International Politics”, *International Studies Quarterly*, Vol. 47, No. 4, 2003。

② Arnold Wolfers, “National Security as an Ambiguous Symbol”, pp. 481-502; R. Ullman, “Redefining Security”, *International Security*, Vol. 8, No. 1, 1983, pp. 129-153.

③ 该报告转引自 Jason Healey and K. Grindal, eds., *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*, Vienna: Cyber Conflict Studies Association, 2013。

④ National Academy of Sciences, *Computersat Risk: Safe Computing in the Information Age*, Washington, D. C.: National Academy Press, 1991.

⑤ 关于网络安全威胁的列举式说明，参见 Ronald Deibert, “The Growing Dark Side of Cyberspace (… and What to Do About It)”, *Penn State Journal of Law & International Affairs*, Vol. 1, No. 2, 2012, pp. 260-274; Derek Reveron, “An Introduction to National Security and Cyberspace”, in Derek Reveron, ed., *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, Washington, D. C.: Georgetown University Press, 2012。

⑥ Eric D. Knapp, *Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems*, Waltham, MA: Syngress, 2011.

⑦ 以此连续体的方式理解网络安全的著述较为常见，可参见 Myriam Dunn Cavelty, *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*, London: Routledge, 2008; Paul Cornish, Rex Hughes and David Livingstone, *Cyberspace and the National Security of the United Kingdom: Threats and Responses*, London: Chatham House Report, 2009。

安全威胁之间的界线十分模糊。不仅如此，网络安全威胁等级的划分也存有疑问，尽管网络战争被认为是最具破坏性的暴力活动形式，但从造成的损失和总体规模上看，网络犯罪和间谍活动等行为似乎更接近国际安全的直接威胁。如何准确把握和评判网络威胁，恰恰是网络安全研究争论的一个焦点。

另一方面，网络安全的指涉对象建构着安全概念的边界。大体而言，网络安全所指涉的是一个通过数字网络将人、信息与机器连接在一起的人为想象的聚合体。最早发明“网络空间”一词的吉布森将这一空间定义为“共识的想象”，① 但这种“共有主观性”意味着作为安全客体的网络空间很难具备绝对明晰的边界。例如，马丁·利比基将网络空间解构为一个三层次的模型，“物理层”主要指代构成网络空间的物理基础设施和设备，“语法层”主要指使得信息传递成为可能的软件和协议等，而“语义层”则是网络空间流动的信息本身。② 这些不同的结构层次蕴含着不同的安全风险，但它们是否涵盖了网络安全的全部所指则难下定论。舒克丽和克拉克便认为“用户层”也应纳入网络空间和网络安全的框架之中。③ 而在信息层面（即上文所说的语义层）上，则需要进一步区分作为代码的信息和代表价值的信息，亦即信息的数字形式与其内容的区分。如果将后者视为信息的自然外延，那么网络空间的边界将延展至价值、信念、思维等人类主观活动的维度。国际社会围绕网络安全还是信息安全所产生的分歧，在很大程度上正是来自于对网络安全概念边界的认知差异。④

网络空间具有的虚拟性、变化性和复杂性，导致对网络安全的探讨从概念基础上便处于模糊不定的状态。这一基础性问题不仅进一步困扰着网络安全战略的相关概念，而且也为网络安全战略意义的评判分歧埋下了伏笔。

（二）网络冲突与网络战争

当“由政治动机驱动的敌对行为在网络空间出现”⑤ 的时候，网络安全问题便开始升级为网络空间的冲突与对抗。确切地说，网络冲突可被定义为“在网络空间恶意或破坏性地使用计算机技术，其目的是影响、改变或调整实体间

---

① William Gibson, *Neuromancer*, New York: Ace Books, 1984.

② Martin Libicki, *Conquest in Cyberspace: National Security and Information Warfare*, Cambridge: Cambridge University Press, 2007.

③ Nazli Choucri and David Clark, “Cyberspace and International Relations: Toward an Integrated System”, Paper Presented at Massachusetts Institute of Technology, Cambridge, Massachusetts, August, 2011.

④ 参见 Keir Giles, “Russia's Public Stance on Cyberspace Issues”, 4th International Conference on Cyber Conflict, 2012；刘杨钺、杨一心：《集体安全化与东亚地区网络安全合作》，《太平洋学报》，2015 年第 2 期。

⑤ Scott Applegate and Angelos Stavrou, “Towards a Cyber Conflict Taxonomy”, 5th International Conference on Cyber Conflict, 2013.

的外交和军事互动态势，但并未上升至战争等级”。[①] 网络冲突的参与主体既包括民族国家和政府，也包括各类非政府组织和个人。[②] 例如，黑客组织“匿名者”宣称对“伊斯兰国”极端势力发动的网络攻击，即属于非国家行为体的互动。然而，网络冲突并不限于同类行为主体之间的互动，有学者据此区分了“社会政治型”与“民族宗教型”网络冲突，前者主要反映不同社会层级（权威）之间的冲突，典型的便是由网络技术赋权的社会政治运动，后者则体现为平等主体间的网络冲突。[③] 从更宽泛的角度来看，除了直接的敌意行为，围绕网络空间规则制定、资源分配和规范生成而发生的争端和矛盾也可归为网络冲突范畴。[④] 不管是宽泛的还是具体的定义，政治性和对立性构成了网络冲突的核心要件，但使用范畴的差异却可能使对网络冲突的探讨难以契合。

如果说对网络安全和网络冲突的概念分歧主要存在于构成要素和外延上，那么在网络战争上存在的争议则直指这一概念的本质属性。按照查尔斯·蒂利对集体暴力所做的经典分析，战争是破坏性最强、组织程度最高，因而也是最为极端的暴力形式。[⑤] 在这一逻辑之下，网络战争即是网络冲突以及网络安全威胁的终极表现形式。2011 年起，美国与俄罗斯的研究机构在网络安全领域展开了一项二轨外交合作，目的便是澄清纷繁复杂的网络安全概念，为进一步的实质性合作奠定基础。在其共同出版的《网络安全核心术语基础》中，网络战争被界定为“网络冲突的升级状态”，具体指“国家行为体之间针对网络基础设施进行的网络攻击，这种攻击构成了军事行动的组成部分”。[⑥] 与之类似，约瑟夫·奈将网络战争定义为“能够放大物理攻击效能或产生同等效应的网络空间敌意行为”，这种敌意的网络攻击能够“对军事和民用目标带来极大破坏和物理摧毁”。[⑦] 也就是说，上升到战争状态的网络冲突不仅与传统（物理空间）军事行动密切相关，而且在打击目标和效果上必须具有显著性和重要性。这种定义模式赋予了网络战争与传统军事行动相似的战略意义，在理论上将网络空

① Brandon Valeriano and Ryan Maness, “The Dynamics of Cyber Conflict Between Rival Antagonists, 2001-11”, *Journal of Peace Research*, Vol. 51, No. 3, 2014, pp. 347-360.

② 王军：《多维视野下的网络战：缘起、演进与应对》，《世界经济与政治》，2012 年第 7 期。

③ Athina Karatzogianni, *The Politics of Cyberconflict*, New York: Routledge, 2008.

④ Nazli Choucri, *Cyberpolitics in International Relations*, Cambridge: The MIT Press, 2012, p. 126; 沈逸：《全球网络空间治理原则之争与中国的战略选择》，《外交评论》，2015 年第 2 期。

⑤ Charles Tilly, *The Politics of Collective Violence*, Cambridge: Cambridge University Press, 2003.

⑥ East West Institute, *The Russia-U. S. Bilateral on Cybersecurity: Critical Terminology Foundations*, Issue 2, 2014.

⑦ Joseph Nye, “Nuclear Lessons for Cyber Security?” *Strategic Studies Quarterly*, Vol. 5, No. 4, 2011, pp. 18-38.

间想象为陆海空天之外的新的作战与战略空间。①

然而，与传统军事行动相比，所谓的网络战争又有着本质的差别。以克劳塞维茨的战争观来看，战争必须具备政治性（即战争是政治的延伸）、暴力性（必须对人员或物质带来毁伤）和工具性（必须满足特定的战略目的）等基本特性。但已知的网络冲突案例似乎离克氏的战争标准相距甚远。作为程序代码形式的网络武器并不能对人员带来直接杀伤（尽管其对物理设施的破坏作用已在一些实际和实验案例中得以证明）；现有的网络攻击事件大多很难与明确的战略意图相联系，使得战争的“手段—目的”链条并不突出；网络冲突的发起主体往往试图掩盖其攻击行为，而不是利用这种攻击来增加其政治博弈筹码，这也使得网络冲突作为政治工具的功能大打折扣。基于这些理由，里德认为将现实的网络冲突冠之以“网络战争”实则是种曲解，其实际所展现出的不过是破坏、间谍和颠覆等活动在网络时代的新形式。②“网络战争”概念的创造者阿奎拉也指出，这一概念最初只是被用来描述国家在信息主导权上的对抗，在使用过程中却出现了人为的重心偏离。③ 换句话说，网络战争很有可能陷入了萨托利早已指出的“概念拉伸”的陷阱，即某一领域的概念运用到新的领域时发生的意义偏转或失准。④

另一些学者则认为，随着人类政治纷争向网络空间扩展，传统概念本身也应不断丰富以适应新态势的发展。战争并不总是以人员杀伤为主要目标，这一点在人道主义原则日益普及的当代变得更加突出了。因此，将过去建立在暴力、致命性等基础上的战争概念移植到网络空间的冲突与对抗上，并不必然发生概念的不匹配，反而是战争形态演化发展的内在体现。⑤ 特别是考虑到网络攻击已经能够对物理空间产生直接后果，那么对网络战争的讨论就不仅不是离题甚远，而是迫在眉睫了。⑥

从以上分析可以看出，不管是网络安全还是网络战争，统一的概念性共识

---

① Robert Miller, Daniel Kuehl and Irving Lachow, “Cyber War: Issues in Attack and Defense”, *Joint Force Quarterly*, Vol. 61, No. 2, 2011, pp. 18-23.

② Thomas Rid, *Cyber War Will Not Take Place*.

③ John Arquilla and David Ronfeldt, “Cyberwar Is Coming!” *Comparative Strategy*, Vol. 12, No. 2, 1993, pp. 141-165; John Arquilla, “The Computer Mouse that Roared: Cyberwar in the Twenty-First Century”, *Brown Journal of World Affairs*, Vol. 18, No. 1, 2011, pp. 39-48.

④ Giovanni Sartori, “Concept Misformation in Comparative Politics”, *American Political Science Review*, Vol. 64, No. 4, 1970, pp. 1033-1053.

⑤ John Stone, “Cyber War Will Take Place!” *Journal of Strategic Studies*, Vol. 36, No. 1, 2013, pp. 101-108.

⑥ 参见 Gary McGraw, “Cyber War Is Inevitable (Unless We Build Security In)”, *Journal of Strategic Studies*, Vol. 36, No. 1, 2013, pp. 109-119; Michael Schmitt, “Classification of Cyber Conflict”, *Journal of Conflict & Security Law*, Vol. 17, No. 2, 2012, pp. 245-260。

仍然难以形成。这为准确判断网络安全的战略意义带来了困难，因为争论中的不同视角往往从概念起点上便存在差异。而传统战略分析框架和理论（如战略稳定性、攻防平衡等）被用于新的网络空间互动时，分歧和争论更进一步加剧。大致来说，关于网络空间的安全互动对国际政治和国家战略的影响，出现了以下三类主要视角。

二、网络安全威胁忧虑论

自网络技术刚刚进入普及应用时起，许多人便意识到这一技术所蕴藏的巨大的政治能量。激进的自由主义者开始憧憬去中心化的网络技术能够促成国家组织形式的消解，但换而言之，匿名性、即时性、分散化等新技术特征也意味着新的安全挑战。美国国家科学院早在 1991 年便已提出警告，“未来的恐怖主义分子使用键盘造成的破坏将远甚于炸弹。”① 然而，随着网络空间军事化和武器化的不断发展，对网络恐怖主义的警惕很快让位于对国家间网络对抗的忧虑，而后者则被视为国际政治变革的颠覆性元素。

（一）网络冲突成为国际冲突新模式

经验证据表明，网络攻防对抗将成为国际冲突的重要模式。近年来，国家间网络冲突越来越频繁地与传统政治冲突交织在一起，手段和目标日趋复杂，这些冲突事件为忧虑论者提供了重要的现实支撑。2007 年和 2008 年，俄罗斯黑客分别针对爱沙尼亚和格鲁吉亚发动了大规模网络攻击，造成政府、金融、媒体等行业一度陷入瘫痪，而这两起攻击恰逢俄罗斯与这些国家处于激烈争端或武装冲突之际，在战略目的上与物理空间的冲突密切呼应，甚至有人据此将这些冲突视作国家间网络战争的发端。与之类似的网络冲突随后也在乌克兰、叙利亚等政治危机中反复出现，显示网络空间正成为国家间政治博弈的重要战场。2012 年被曝光的“震网”病毒攻击，被认为是美国和以色列针对伊朗核能力实施的破坏计划的组成部分。该攻击通过改变核设施中离心机的运转速率，成功造成伊朗部分设施的功能障碍，也使得网络冲突的目标对象不再局限于虚拟标的或者联网系统，即使物理上断网的核心基础设施也能成为网络攻击的潜在对象。与此同时，“震网”以及后来被发现的“火焰”等病毒攻击能够有效选择打击目标，在一定程度上提升了攻击的准确性并避免了连带损伤，意

① National Academy of Sciences, *Computersat Risk*: *Safe Computing in the Information Age*.

味着网络工具的武器特性得到了进一步强化。①

以下几方面原因或将促成网络冲突在国际体系中的扩散。一是发动网络攻击的门槛不断降低。网络武器本质上是恶意程序代码，因而易于获取、生产、复制或转移。围绕网络攻击所需的漏洞和工具展开的黑市交易逐渐泛滥，使那些即使不具备网络战能力的个人和组织也能获得一定的攻击手段。一些网站和公司专门从事漏洞等攻击资源的收集和转让，其客户对象涵盖了政府、企业、组织和个人等各类行为主体。② 二是运用网络攻击实现特定战略目的已开危险的先例，上文所述的网络冲突案例仍有可能被继续仿效。三是网络攻击的归因问题始终难以解决。由于网络攻击发动者可以隐藏自身地址和身份，或通过入侵和控制其他终端发动攻击，往往难以及时准确判断攻击来源，归因问题因而被认为是网络安全中最为棘手的难题。③ 这一难题可能成为各类行为主体诉诸网络攻击手段的重要诱因。四是现有的国际规范对网络空间冲突约束不足。与网络冲突日益常态化相比，国际社会尚未针对如何限制网络空间的敌对和军事行为达成明确共识。北约邀请国际法专家编制的《塔林手册》虽然探讨了国际法如何适用于网络空间冲突的问题，但这一文件并不具有普遍规范效力，其形成的诸多主张也存在较大争议。因此，无论从内在诱因还是外在约束来看，网络冲突在国际政治中的数量增长似乎难以避免。

（二）网络冲突破坏战略稳定性

网络冲突被认为将严重削弱国际体系的战略稳定性。攻防平衡理论认为，某些类型的军事技术发展有利于进攻一方，导致国家间攻防平衡向进攻占优倾斜，从而使国际体系易于出现冲突和战争。④ 具体来说，当主导性的军事技术使进攻付出的成本超过防御所需的成本时，战争将更具决定性且有利可图，而安全困境则愈发明显。⑤ 网络技术被认为是推动进攻占优态势的重要力量。数据代码的传输超越了时间和地理的局限性，使攻击能够在瞬间发动并完成，传

---

① James Farwell and RafalRohozinski, "The New Reality of Cyber War", *Survival: Global Politics and Strategy*, Vol. 54, No. 4, 2012, pp. 107-120.

② "The Digital Arms Trade: The Market for Software that Helps Hackers Penetrate Computer Systems", *The Economist*, March 30, 2013, http://www.economist.com/news/business/21574478-market-software-helps-hackers-penetrate-computer-systems-digital-arms-trade/.

③ 辛格和弗里德曼在其著作中指出，"或许最难解决的便是归因问题"。Peter Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know*, Oxford: Oxford University Press, 2014, p. 73.

④ Jack Levy, "The Offensive/Defensive Balance of Military Technology: A Theoretical and Historical Analysis", *International Studies Quarterly*, Vol. 28, No. 2, 1984, pp. 219-238; Stephen Van Evera, "Offense, Defense, and the Causes of War", *International Security*, Vol. 22, No. 4, 1998, pp. 5-43; George Quester, *Offense and Defense in the International System*, New Brunswick, N. J.: Transaction Books, 2002.

⑤ Charles Glaser and Chaim Kaufmann, "What Is the Offense-Defense Balance and Can We Measure It?" *International Security*, Vol. 22, No. 4, 1998, pp. 44-82.

统攻防对抗中的力量集结和投送等问题被网络空间的即时性所替代。发展网络技术的最初目的是为了在核威慑背景下保持战略通讯的稳定性和可靠性,① 因此连通性成为最为核心的技术特性,这就意味着其本质上是一种数据连接的网络攻击,在实现途径和技术支持度上总是高于本质上是数据拒止的网络防御。“零日”漏洞(即未被安全供应方发现的系统或软件漏洞)是网络攻击所使用的重要手段,其本质属性便决定了掌握这类漏洞的攻击者在攻防对抗中占据先机,漏洞的检测和相应补丁的供应往往滞后于漏洞被恶意利用,使防御者提前防范的难度增大。总体而言,网络攻击技术的发展总是先于防御技术,这种进攻占优的局面可能打破国际体系平衡,特别是为大国关系的稳定投下了阴影。② 如果考虑到网络攻击可能对核心基础设施带来的“大规模杀伤”效应,那么战略稳定性的基础将变得更为脆弱。

相比之下,防御一方在网络空间付出的成本更高。由于网络攻击来源和方式具有较大的未知性和不可预见性,防御者需要不断更新完善其网络系统(甚至诸多非联网的核心系统)来抵御风险。正如科洛所说,“(网络)攻击者只需要弄清楚其所欲采取的入侵和进攻的具体办法,而防御者则必须持续地保护整个系统,以防范能够想象得到的所有攻击。”③ 不仅如此,网络系统具有普遍性和复杂性,有效的网络防御需要协调多部门多行为主体共同应对,但利益分歧可能阻碍这种合作,④ 例如一些私营部门行为体出于企业声誉和收益的考量,往往不愿意分享和公开遭受的网络攻击信息。因此,许多人认为网络技术会导致攻防严重失衡,传统的战略观念已跟不上网络时代的步伐。时任美国国防部副部长的威廉·林恩在 2010 年指出,“在进攻占优的环境下,堡垒式的思路将不起作用。如果退到(网络)防火墙的马其诺防线之后,结果很可能遭受蹂躏。”⑤

此外,网络攻击还有可能通过诱发不相称的报复行动而使冲突升级。网络攻击的潜在目标包含多个层级,当针对某一层级的攻击出现后,受攻击者很难确定当前的攻击将仅仅停留在这一层级上,还是作为更大范围、更高层级网络

---

① Madeline Carr, “The Political History of the Internet: A Theoretical Approach to the Implications for US Power”, pp. 173-188.

② Kenneth Lieberthal and Peter Singer, “Cybersecurity and U. S. -China Relations”, Brookings Research Paper, February, 2012.

③ Lucas Kello, “The Meaning of the Cyber Revolution: Perils to Theory and Statecraft”, p. 28.

④ 关于利益分配如何影响网络安全实践,可参考 Ross Anderson and Tyler Moore, “The Economics of Information Security”, *Science*, Vol. 314, 2006, pp. 610-613。

⑤ William Lynn III, “Defending a New Domain: The Pentagon's Cyberstrategy”, *Foreign Affairs*, Vol. 89, No. 5, 2010.

攻击的前奏。这可能致使防守者做出错误判断，以更具破坏性的回击来抵消其所估计的潜在进攻，从而造成冲突烈度螺旋式上升。[①] 即使是单纯的防御性行为（例如建立网络防御部队），在另一方以最坏情形的战略研判之下，也可能被解读为进攻的准备活动，并诱发先发制人式的打击。[②] 无论哪种情形，网络空间的互动似乎都将对国际体系的稳定性带来严重损害。

（三）网络冲突颠覆国际秩序

网络冲突还被认为会从根本上动摇现有的国际秩序。一方面，网络空间安全互动带来了参与主体数量的爆炸式增长。个人、黑客组织、犯罪团伙、政治组织、内容和服务供应商、设备制造商、安全研发企业乃至普通的跨国或国内企业，都能在网络安全事务中扮演重要角色。这使得网络攻防对抗中的不确定性大为增加。例如，1998 年美国即将展开针对伊拉克的“沙漠之狐”行动之际，其军事和政府网络系统突遭入侵，而侵入者部分 IP 地址显示为阿联酋，美方曾一度怀疑是伊拉克进行的先发制人打击，但后续调查最终发现其实是两名美国青少年所为。[③] 这种由行为主体多元化带来的战略误判风险，在 2014 年索尼影业遭不明黑客攻击的事件中同样得以体现。当国家间关系存在物理对抗或政治危机时，不明来历（或是伪装来历）的网络攻击很可能造成对峙双方的错误判断，本可避免的武装冲突甚至战争行为有可能就此点燃。不仅如此，行为体的扩散还使传统国际安全机制和模式难以延续。例如，军备控制和威慑能够在一定程度上减轻国家间直接对抗的风险，但当涉及主体不再固定且身份难以验证时，这些传统概念和实践的适用性便受到严重挑战。[④]

另一方面，随着信息网络技术的应用日益广泛和多样化，网络攻击或许会威胁到民用基础设施安全，带来灾难性后果。在这一点上，现有的实验研究已经证明，网络入侵可以干扰和破坏发电站、交通工具和医疗设施等物理设备。[⑤] 虽然目前这类攻击仍停留在理论和研究阶段，但这一危险的发展趋势为大规模的突发事件和社会失序埋下了隐患。特别是当整个人类社会的正常运转逐渐依赖于看不见的信息传输和流动时，未知风险和技术的负面效应或许会如指数般上升。对于国际社会而言，这可能意味着难以预料的安全威胁，而这种威胁可能超越国家的界线，成为重塑国际关系的新变量。

---

① Richard Clarke, “War from Cyberspace”, pp. 31-36.

② Martin Libicki, *Crisis and Escalation in Cyberspace*, Santa Monica, CA: RAND Corporation, 2012.

③ Jason Healey, ed., *A Fierce Domain: Conflict in Cyberspace, 1986 to 2012*.

④ 董青岭：《网络空间威慑：如何推进第三方责任》，《世界经济与政治》，2013 年第 9 期。

⑤ Scott Applegate, “The Dawn of Kinetic Cyber”, 5th International Conference on Cyber Conflict, 2013.

三、网络安全效用怀疑论

前一类观点将网络安全视为国际政治变革的重要因素，认为网络技术或将严重影响二战后国际体系逐渐建立的秩序与稳定。与之相反，另一部分学者则认为目前针对网络安全威胁的讨论被过分放大，网络技术不会对国际政治互动产生深刻影响。

（一）网络安全与对外战略

网络攻击难以成为国家对外战略的有效手段。无论是网络冲突在国际体系中的扩散，还是其对攻防平衡和战略稳定性的负面影响，其中一个重要的内在假设在于，国家行为体能够有效利用网络攻击来实现特定战略目的。但这一假定却受到诸多方面的挑战。古往今来，武力（暴力）的使用总是为了达到两个基本目标，即征服和威慑。对战争和冲突的分析离不开对意图和目的的研判。[①] 就征服而言，网络攻击显然有别于传统的领土冲突模式，但这种区别并非仅仅出于虚拟和实体领域的性质不同，而是武力产生的影响存在重要差异。传统冲突模式通过对设施和人员的大规模毁伤，以及对战略资源和要地的实际控制，能够实现对敌方战略空间的长期占领和力量上的有效压制。但网络攻击带来的后果在很大程度上是暂时的和可逆的。即便考虑最严重的情况，使用网络攻击“切断电网、关闭机场或者破坏通讯会造成重大的损失，但这类破坏能被迅速修复，而且相对而言并不需要付出沉重的代价”。[②] 由于网络攻击难以形成持续性的影响，其作为征服性的战略工具的效能便大打折扣，更有可能作为常规力量的辅助性手段。同样，在改变军事力量平衡上，网络手段有可能为攻击方带来先发优势，但这种优势是转瞬即逝的，因为对手能很快从网络攻击中恢复，要取得持续性的战略压制必须依赖常规武力的使用。这样一来，网络技术便很难扭转传统的力量结构，拥有常规力量优势的行为主体在网络条件下仍然占据上风。[③] 当然，网络攻击或许可以通过使民用基础设施瘫痪来造成敌对国的社

① 克劳塞维茨认为，战争总是工具性的，服务于特定的目标。见克劳塞维茨：《战争论》，中国人民解放军军事科学院译，北京：解放军出版社，2005 年。

② Erik Gartzke, “The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth”, *International Security*, Vol. 38, No. 2, 2013, pp. 41-73.

③ 对“震网”攻击事件的分析也得出了相似的结论，即传统国际政治中的力量天平并未被网络技术的发展所打破，这一点反驳了关于网络攻击降低战略稳定性的理论主张。参见 Jon Lindsay, “Stuxnet and the Limits of Cyber Warfare”, *Security Studies*, Vol. 22, No. 3, 2013, pp. 365-404。

会混乱和人心涣散，从而实现心理上的征服和压制。[①] 但劳森对比了二战时期的战略空袭、大规模恐怖袭击和突发自然灾害等历史经验后发现，即使是对基础设施和社会系统的最猛烈破坏，也并未带来严重的社会恐慌和秩序瓦解，因此假设网络攻击会极大地损伤国家意志力，同样是一种“错误的恐惧感”。[②]

就威慑而言，网络攻击的效用同样受到质疑。“作为一种策略，威慑涉及故意、有目的地使用威胁”，[③] 这就要求威慑的发起者必须有效展示其战略力量，并使被威胁者确信做出某项行为会招致特定的打击。然而，一旦网络威慑的发起者明确传递出拥有特定攻击能力的信号，便有可能暴露这种攻击能力所瞄准的目标系统的薄弱点，而对象国进行有针对性的网络防御将会容易许多，从而导致网络威慑的可信度大大降低。[④] 在常规力量威慑中，战略力量与目标选择之间并无确定的联系（例如一方拥有洲际弹道导弹，但打击范围可以覆盖对象国所有本土和海外战略目标），而网络武器与目标选择之间的联系更为密切，“震网”病毒能够扰乱核设施运转，但用其攻击军事指挥系统却不可行，而且这类武器使用过一次便在很大程度上不再有效。简而言之，网络攻击的重要特性在于其不被人察觉的快速性和潜伏性，这些特性与威慑战略很难兼容。此外，网络攻击无法摧毁甚至伤及对手的报复能力（不管是使用网络攻击还是常规力量进行报复），这意味着其作为威慑手段并不足以改变或者慑止对手的行动。[⑤] 需要注意的是，上文所指的网络威慑是将网络技术作为威慑的工具，从反面来看，林赛认为战略性的网络攻击本身是能够被慑止的。理由在于，网络攻击的归因问题并非无法解决，越复杂的网络行动所涉及的环节和人员就越多，反向追踪时可能透露的信息也越多，因此战略性的网络攻击很可能无法始终保持匿名性。这样一来，网络攻击的潜在效用同样被削弱，因为战略攻击发起者必须考虑到身份很可能被曝光并招致报复。[⑥] 不管上述哪种情形，网络攻击都难以成为重要的对外战略手段，[⑦] 网络安全互动对国际政治

---

① John Kelly and Lauri Almann, “eWMDs: The Botnet Peril”, *Policy Review*, No. 152, 2008.

② Sean Lawson, “Beyond Cyber-Doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber-Threats”, *Journal of Information Technology & Politics*, Vol. 10, No. 1, 2013, pp. 86-103.

③ Lawrence Freedman, *Strategy: A History*, Oxford: Oxford University Press, 2013, p. 157.

④ Erik Gartzke, “The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth”, pp. 41-73.

⑤ 利比基对如何慑止网络攻击者进行了分析，并指出网络攻击行为很难被威慑所制止，这一观点与上文的论述侧重点并不相同，但反映出相似的内在逻辑。参见 Martin Libicki, *Cyberdeterrence and Cyberwar*, Santa Monica, CA: RAND Corporation, 2009。

⑥ Jon Lindsay, “Stuxnet and the Limits of Cyber Warfare”, pp. 365-404.

⑦ 在这一点上，有学者分析了 2007 年以来几次主要的国家间网络冲突案例，并认为这些案例显示出，网络攻击远不能达到攻击者所期待的对外战略目的，因此网络攻击只是外交战略中的一件“钝器”。参见 Emilio Iasiello, “Cyber Attack: A Dull Tool to Shape Foreign Policy”, 5th International Conference on Cyber Conflict, 2013。

的影响仍然有限。

（二）网络技术的双刃剑效应

事实上，许多被认为困扰着网络防御者的因素同样困扰着进攻者。例如，网络系统的复杂性虽然增加了有效防御的成本，但对于进攻者而言，对攻击效果的精确控制和预判也变得更加困难。① 正是由于信息流动具有高度的连通性和无边界性，网络武器在释放之后如何准确“抵达”目标系统、如何限定攻击范围并避免其扩散，以及如何获知攻击效果是否实现等问题都随之出现。即使是攻击目标较为精确的“震网”和“火焰”等病毒攻击，也影响到了对象国以外的其他国家，而将这些攻击复制到朝鲜核设施的努力则完全未能成功。② 简言之，如果不可预知性是网络防御的噩梦，那么它对网络攻击的限制作用同样不可忽视。与之类似，网络技术的军民两用性、身份匿名性（即上文所述的网络攻击的隐蔽性与威胁可信度之间的矛盾）等特点都会对攻防两方造成影响，而另一些特点甚至使防御比进攻更加容易。围绕网络安全形成的多方共同体（包括网络安全企业、研究者、政府部门等），使得网络防御在许多时候得到了国际行为体的多样化支持，网络安全逐渐成为国际社会的公共产品。③ 例如，网络安全公司卡巴斯基就经常追踪和曝光一些潜伏的网络攻击事件并提出应对方案。而在一些重要的网络安全事件（如“飞客”蠕虫和“心脏滴血”漏洞等）中，非国家行为体自下而上的安全治理协作也发挥了重要作用。总的来看，网络空间攻防对抗并不必然导致进攻占优的局面，有利于防御和进攻的因素常常是并存的。

上述内容为质疑网络安全战略意义的观点提供了第二层理由，即思考技术对政治的影响时必须避免技术决定论的误区。技术发展固然会带来某些类型的政治后果，如改变互动方式、增强互动密度等，④ 但这些影响并非是单向的，人类社会在适应技术变革的同时，也不断改造和重塑着技术发展的轨迹，以消

---

① Lawrence Cavaiola, David Gompert and Martin Libicki, “Cyber House Rules: On War, Retaliation and Escalation”, *Survival: Global Politics and Strategy*, Vol. 57, No. 1, 2015, pp. 81-104.

② 路透社最先报道了美国曾企图对朝鲜复刻“震网”攻击，却由于朝鲜核设施保密程度更高等原因而失败。参见 Kim Zetter, “The US Tried to Stuxnet North Korea's Nuclear Program”, *Wired*, May 29, 2015。

③ 一种较为激进的观点认为，网络安全的供应主体多元化并且相互协调，因此分布式的网状治理应当是网络空间安全治理的最优模式。参见 Milton Mueller, Andreas Schmidt and Brenden Kuerbis, “Internet Security and Networked Governance in International Relations”, *International Studies Review*, Vol. 15, No. 1, 2013, pp. 86-104。

④ 技术变革等因素带来的“互动能力”的改变，正是国际体系转型的重要内容。参见 Barry Buzan and Richard Little, *International Systems in World History: Remaking the Study of International Relations*, Oxford: Oxford University Press, 2000; Geoffrey Herrera, *Technology and International Transformation: The Railroad, the Atom Bomb, and the Politics of Technological Change*, Albany: State University of New York Press, 2006。

解在变革过程中出现的外部性。从上述情况来看，网络技术也受到这一规律的制约，其在某方面产生的影响可能被技术本身的两面性所抵消。在这一点上，生物技术及其武器化应用具有一定的借鉴意义。生物武器由于其隐蔽性和大规模杀伤性，也被认为是造成重攻轻防的军事技术，而且其鲜明的军民两用特性使得有效的军备控制变得十分困难。① 但另一方面，病原体的有效威力也受制于疫苗等防御技术的进展，当目标群体对某类生物武器具备免疫力后，该生物武器的效能便微乎其微了，而生物技术发展所需要的专业知识和规模研发效应等因素则制约着生物武器的扩散和使用。② 如果说生物武器的这些特性在过去数十年里并没有深刻改变国际秩序稳定的话，那么并没有充分理由认为网络技术发展将会在国际政治领域产生颠覆性变革。

（三）网络安全与地缘政治

从现有的网络冲突案例来看，国家间网络安全互动在很大程度上仅仅是地缘政治互动的延续。在这一点上，瓦利亚诺等人梳理并建立了 2001—2011 年间敌对国家间的网络冲突数据库，共收集了 110 起网络冲突事件。③ 这些数据至少反映出两方面令人欣慰的趋势：一是网络冲突并未成为国家安全互动的主要形式。在这十年间的 126 对敌对双边关系中，仅仅有 20 对（约 16%）卷入了网络冲突。而绝大部分（80%）网络冲突都表现为单向性的网络攻击，即仅有一方对另一方发动的打击而没有反向的报复行为。这也从侧面反映了网络空间博弈并不一定能成为国家对外战略的重要工具。二是网络冲突具有明显的地缘政治烙印。这些网络冲突事件要么发端于地区国家间长期形成的对峙或竞争关系，要么直接伴随着物理空间的现实冲突，成为国家间武装对抗的一部分。正如数据库的建立者所言，“绝大部分的网络冲突出现在区域敌对关系中”，因此很难与现实地缘政治互动分离开来。网络安全公司火眼（FireEye）在近年的一份研究报告中也得出了相似的结论，认为“（网络攻击的）战略归因归根结底在于地缘政治分析”。④ 从这个意义上看，国家间网络安全互动并没有脱离地理因素的羁绊，因此网络安全的战略影响也会束缚在既往的国际政治框架之

---

① Gregory Koblentz, “Pathogens as Weapons: The International Security Implications of Biological Warfare”, *International Security*, Vol. 28, No. 3, 2003, pp. 84-122.

② Sonia Ben and Ouagrham-Gormley, “Barriers to Bioweapons: Intangible Obstacles to Proliferation”, *International Security*, Vol. 36, No. 4, 2012, pp. 80-114.

③ Brandon Valeriano and Ryan Maness, “The Dynamics of Cyber Conflict Between Rival Antagonists, 2001-11”, pp. 347-360.

④ FireEye Labs, “World War C: Understanding Nation-State Motives Behind Today's Advanced Cyber Attacks”, September 30, 2013, http://www.fireeye.com/blog/technical/threat-intelligence/2013/09/new-fireeye-report-world-war-c.html.

中。“网络战争将主要以常规战争的附属品出现，或者作为一种权宜的、象征性的方式对敌对者表达不满。网络战争……不是一种独立的甚至替代性的冲突模式，而只是现有的武装冲突逻辑的延伸。”①

四、网络安全话语建构论

上述两种视角形成了截然对立的态势，一派认为网络安全将给国际政治带来颠覆性变革，另一派则指出网络安全互动不足以深刻影响国际政治态势。这种观点争鸣不仅仅停留在学术探讨层面，在全球政治博弈中也有所体现，因为对网络空间及其安全问题的定性对于全球治理架构的原则和机制有着重要影响。这一点在近年来围绕网络空间治理的国际博弈中可见一斑，② 但这同时也显示出互动中的社会观念和话语对安全议题的建构作用。因此，安全不仅指代一种客观状态，也应被理解为具有主体间性的社会建构产物。③ 将这一逻辑移植到网络安全领域，便产生了不同于上述两派观点的第三种视角，即网络安全的影响并非客观给定的状态，而是在话语结构和行为塑造下形成的主观认知。这种视角认为，对网络安全的夸大描述或低估反映出不同的“共有主观性”，因而将着眼点置于考察特定的安全化行为主体如何有效地构建并表达网络安全威胁的过程。

通过情景假定、类比、逻辑演绎等多种途径，安全化主体建构出不同的网络威胁意象。汉森与其合作者将这些意象的建构过程分为三类:④ 一是“超安全化”，即网络安全话语依赖于假想的灾难情境，使安全意象的严重性和紧迫性远高于现实安全威胁。超安全化的话语主体往往强调突发网络安全事件可能造成的毁灭性后果，特别是社会、金融、军事等领域核心信息系统的瘫痪，可能带来整个社会政治秩序的崩塌。在这种语境下，其他大规模杀伤性武器（如核武器和生物武器）的历史经验常常被用来推测网络空间安全的潜在影响，⑤

---

① Erik Gartzke, “The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth”, p. 73.

② D. Drissel, “Internet Governance in a Multipolar World: Challenging American Hegemony”, *Cambridge Review of International Affairs*, Vol. 19, No. 1, 2006, pp. 105-120; Alexandra Klimburg, “The Internet Yalta”, *CNAS Commentary*, February 5, 2013; 沈逸：《全球网络空间治理原则之争与中国的战略选择》；郎平：《全球网络空间规则制定的合作与博弈》，《国际展望》，2014 年第 6 期。

③ Michael Williams, “Words, Images, Enemies: Securitization and International Politics”, p. 513.

④ Lene Hansen and Helen Nissenbaum, “Digital Disaster, Cyber Security, and the Copenhagen School”, pp. 1155-1175.

⑤ Gregory Koblentz and Brian Mazanec, “Viral Warfare: The Security Implications of Cyber and Biological Weapons”, *Comparative Strategy*, Vol. 32, No. 5, 2013, pp. 418-434; Joseph Nye, “Nuclear Lessons for Cyber Security?” pp. 18-38.

尽管这些经验在网络空间并无真实的先例可循。第二种过程是“日常安全实践”，这类话语将网络安全意象与受众的普遍经历和日常知识联系在一起，从而使危险图景“近在眼前”。通过使用“病毒”、“感染”、“漏洞”等贴近日常生活的比喻，话语主体建构出网络安全与受众对象之间的直接联系，也为相应的安全策略主张（如提高预防能力）提供了合法性。三是“技术化”，即网络安全的专业化知识占据了独特的话语空间。这类话语往往将网络安全描述为根本上由技术发展导致的次生问题，因而技术的不断完善亦有助于最终形成安全可靠的、复原力强的网络系统。但技术化的建构过程也伴随着安全问题的“去政治化”，即应对网络安全的重心由政策和战略话语下降为技术和专业话语。这三种建构过程背后体现出不同的安全化主体的认知倾向，每种语境都映射出特定的指涉对象，为网络安全营造了不同的威胁意象。与此相似，卡维迪也区分了“技术群落”、“社会政治群落”和“人类机械（互动）群落”等三种不同的网络安全话语体系，并对每种体系关联的话语主体和威胁表征等要素进行了分析。更为重要的是，不同的话语体系也与特定的网络安全实践相联系，使得“语义建构不仅设置了（围绕网络安全展开的）博弈的话语规则，而且也成为服务于这种博弈的重要工具”。①

也就是说，网络安全在本质上是一种主观状态，不管是认为网络安全将带来国际政治互动的深刻变革，还是主张网络攻防难以成为国家战略的重要工具，反映的只是不同的安全化主体对网络安全的认知差异，以及由此塑造的安全实践。这就意味着网络安全在很大程度上是可塑的，对网络安全风险的过度解读进一步强化了威胁认知，导致以冲突和控制为主导的安全实践，实际上营造着互信更低、规则弱化的网络安全环境（例如网络军备竞赛），从而陷入趋向冲突的“自我实现的预言”。② 同样，安全问题也可以通过认知建构过程实现“去安全化”，也就是议题从安全和战略的高政治话语结构中下移，返回到日常的公共话语和普通的政治协调范畴。③ 因此，话语建构论者往往对网络安全问题持反思主义立场，认为应对现有的网络安全政策和实践加以批判性重思，因为正是这些政策和实践加固了冲突原则和消极认知的社会化。如卡维迪所言，“认识到威胁表述方式蕴含的政治权力及其背后的偏好，有助于人们搞清楚这

① Myriam Dunn Cavelty, “From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse”, p. 118.

② 〔美〕温特：《国际政治的社会理论》，秦亚青译，上海：上海人民出版社，2001 年；David Houghton, “The Role of Self-Fulfilling and Self-Negating Prophecies in International Relations”, *International Studies Review*, Vol. 11, No. 3, 2009, pp. 552-584。

③ Michael Williams, “Words, Images, Enemies: Securitization and International Politics”, p. 523.

样一个事实，即网络安全并不必然要与权力争夺、战争和军事行动联系在一起，人们总有其他更好的（政策）选择。”① 就这一点而言，话语建构论与质疑网络安全战略意义的观点存在相似主张，认为网络空间安全互动未必会造成现有国际体系和规则的颠覆性改变。将网络空间界定和描述为一种新的战争空间，无助于理解如何有效防护网络系统，也无助于战略家和安全从业者形成准确、实际的判断。② 但不同的是，网络安全的建构本质意味着趋向冲突或趋向合作具有极大的不确定性，这使得反思主义范式很难为维护网络安全提出明确和可操作的政策主张。

需要指出的是，尽管话语建构论对网络安全的发展前景持模糊态度，但却对理解话语结构差异，并进而探索不同安全化主体间的合作提供了有益思考。网络安全忧虑论认为，网络技术将推动国际体系攻防平衡向进攻占优转变，网络时代的国际政治互动将具有更高的不稳定性，这迫使无政府状态下的行为主体竭力争夺新的战略空间以获取先发优势。在这种情况下，网络这一新疆域仍然是由大国政治博弈所定义的。围绕网络安全展开的国际合作即便可能，也仅仅是大国之间达成的有限协调，其核心是为不可避免的网络战争确立基本规范。③ 审慎论者质疑网络攻防在国家对外战略中的效用，认为网络空间将成为国家间对抗新战场的说法其实是夸大了现实的安全威胁。网络安全行为主体的多元化不仅使安全这一公共产品的供给得到保障，而且为合作治理网络安全问题提供了新的模式。这种新模式以多元主体自下而上的协作为基础，以自发式、参与式的平等合作替代等级制的大国协调，实质是为当前国际互联网治理的“多利益攸关方”模式寻找合法性依据。④ 这两种视角延伸得出的安全合作前景难以兼容，突出表现在国际社会关于互联网治理机制的争议和分歧上。而话语建构论则认为，行为主体之间要形成有效合作，首先必须调和安全化实践

---

① Myriam Dunn Cavelty, “From Cyber-Bombs to Political Fallout: Threat Representations with an Impact in the Cyber-Security Discourse”, p. 119.

② Martin Libicki, “Cyberspace Is Not a Warfighting Domain”, *I/S: A Journal of Law and Policy for the Information Society*, Vol. 8, No. 2, 2012, pp. 321-336.

③ 许多学者认为，国家行为体仍将是网络空间安全的主要参与者，因此安全合作也将主要体现为国家间的竞争与妥协。可参见 James Forsyth and Billy Pope, “Structural Causes and Cyber Effects: Why International Order Is Inevitable in Cyberspace”, *Strategic Studies Quarterly*, Vol. 8, No. 4, 2014, pp. 112-128; Rex Hughes, “A Treaty for Cyberspace”, *International Affairs*, Vol. 86, No. 2, 2010, pp. 523-541; Daniel Drezner, “The Global Governance of the Internet: Bringing the State Back In”, *Political Science Quarterly*, Vol. 119, No. 3, 2004, pp. 477-498。

④ J. P. Singh, “Information Technologies, Meta-Power, and Transformations in Global Politics”, *International Studies Review*, Vol. 15, No. 1, 2013, pp. 5-29; Milton Mueller, *Networks and States: The Global Politics of Internet Governance*, Cambridge: The MIT Press, 2010; Milton Mueller, John Mathiason and Hans Klein, “The Internet and Global Governance: Principles and Norms for a New Regime”, *Global Governance*, Vol. 13, No. 2, 2007, pp. 237-254.

的内在差异。只有当行为主体对威胁来源和性质等内容的认知较为接近时，其所产生的应对措施以及特殊政治规则才能够相互协调而非彼此矛盾，有效的国际合作才具备重要的观念基础。① 这一观点有效解释了网络安全国际合作难以推进的重要原因，也为发展程度、文化差异等因素纳入合作议程提供了理论支撑。前述两类网络安全合作观的内在矛盾，在话语建构论和安全化理论视角下得到了调解之道。

五、结语与启示

网络安全已成为新世纪国际安全和政治博弈的焦点内容。网络安全的政治和战略影响究竟如何定性，也随之成为争论日益激烈的难解之题。本文大致梳理了国际政治框架下探讨网络安全的三种视角，这些视角在理解网络安全这一新的政治现象上各执一词，甚至在某种程度上彼此对立，难以兼容。从更深层次意义上看，这种争论为国际关系理论研究提出了新的命题。

首先，这些争论的内在核心在于对国际体系的根本认识差异。如同生物学的宏观认识是建立在对生物和生态系统的总体考察上那样，国际关系的理论建构往往将国家等行为主体构成的有机整体（国际体系/系统）视为基本的研究本体和出发点。② 然而，对国际体系的不同理解，直接导致了不同理论视角下对国际行为模式判断迥异。新现实主义认为，国际体系的无政府结构迫使体系内的行为主体以自我保全为根本目标，在“自助原则”的指引下通过最大限度谋取权力优势来实现安全。国际政治的本质便表现为无休止的权力竞争以及由此产生的安全困境。先进技术及其军事化应用是主要行为体（民族国家）在这场权力博弈游戏中最重要的砝码，而这种发展规律几乎是不可阻挡的。③ 二战后，国际体系在核武器及其巨大的相互威慑效应下经历了较长时间的“冷和平”，但无政府状态的结构性压力意味着行为体并不会停止其追求绝对优势的

---

① Nicholas Thomas, “Cyber Security in East Asia: Governing Anarchy”, *Asian Security*, Vol. 5, No. 1, 2009, pp. 3-23; A. Kasper, “The Fragmented Securitization of Cyber Threats”, in T. Kerikmäe, ed., *Regulating eTechnologies in the European Union: Normative Realities and Trends*, Berlin: Springer, 2014; 沈逸《数字空间的认知、竞争与合作——中美战略关系框架下的网络安全关系》。

② 〔美〕华尔兹《国际政治理论》，信强译，上海：上海人民出版社，2003 年；Immanuel Wallerstein, *The Essential Wallerstein*, New York: The New Press, 2000。

③ 恩格斯的著名论断指出，“一旦技术上的进步可以用于军事目的并且已经用于军事目的，它们便立刻几乎强制地，而且往往是违反指挥官的意志而引起作战方式上的改变甚至变革”，这一点对于新技术如何进入国际政治角力场做出了重要说明。参见《马克思恩格斯全集》（第 20 卷），北京：人民出版社，1956 年，第 187 页。

脚步。因此，当人类开始在太空和网络空间等新领域展开技术探索时，将这些新领域转化为获取政治权力新来源的动机似乎是顺理成章的。① 权力竞争向新战略空间的扩展将不可避免地引发国际体系新的不稳定，特别是考虑到新技术的潜在效能，其必然在竞争原则的引导下走向军事应用的最大化。因此，在这种冲突主导的国际体系理念下，网络安全被视为触发新一轮国际体系攻防失衡和政治失序的重要因素。自由主义虽然内部研究纲领各异，但都认可国际体系中存在合作与进步的条件。无政府状态下的排列原则并不必然以一种自助自保的“机械系统”为主导，而是可以逐渐形成相互依赖、互助互利的“有机系统”。② 在全球化进程推动下，国际体系中的单元日益多样化，议题逐渐丰富，行为体之间的联系更为复杂多变，这些因素塑造了多元化的利益诉求和互动模式，使得国际政治权力的性质也发生了深刻改变。③ 网络技术发展恰恰推动了国际体系互动密度的急剧增长，催生了新的行为主体和行为方式，也带来了新的利益和权力实现途径。在这种意义上，网络安全并不会使国际系统退回到霍布斯式的自然状态中去，而是孕育着安全治理模式和互动方式的转变。建构主义则强调国际体系的社会建构，认为社会化过程产生的国际体系文化和观念结构塑造着行为体的身份和偏好。④ 与客观物质结构具有的确定性相比，基于共有观念的文化结构是不确定的和可形塑的，这种形塑既受客观物质条件的影响，又在很大程度上来自于主体间的话语和实践互动。⑤ 对于网络安全而言，国际体系的这种模糊可塑性意味着话语和实践是建构安全意象的主要动因。在探讨网络安全问题之前，必须认识到这些探讨本身就构成了这一领域安全化的“言语行为”。

因此，对网络安全的不同解读，根植于对国际体系本质特征的不同理解。事实上，国际体系无政府结构带来的生存压力，与行为主体在互动过程中不断形成的制度性安排、共有知识和共同规范常常是并存的。⑥ 唐世平则进一步指

---

① 金虎：《技术对国际政治的影响》，沈阳：东北大学出版社，2004 年。

② Quddus Snyder, “Taking the System Seriously: Another Liberal Theory of International Politics”, *International Studies Review*, Vol. 15, No. 4, 2013, pp. 539-561.

③ Anne-Marie Slaughter, “America's Edge: Power in the Networked Century”, *Foreign Affairs*, Vol. 88, No. 1, 2009, pp. 94-113; 〔美〕罗伯特·基欧汉、约瑟夫·奈：《权力与相互依赖》，门洪华译，北京：北京大学出版社，2002 年。

④ 〔美〕温特：《国际政治的社会理论》；Richard Ned Lebow, *A Cultural Theory of International Relations*, Cambridge: Cambridge University Press, 2009。

⑤ 关于实践如何受到背景知识的影响，并进而外化和具体化这些知识，可参见 Emanuel Adler and Vincent Pouliot, eds., *International Practices*, Cambridge: Cambridge University Press, 2011。

⑥ Tim Dunne and Richard Little, “The International System - International Society Distinction”, in Cornelia Navari and Daniel Green, eds., *Guide to the English School in International Studies*, New York: Wiley-Blackwell, 2013.

出，国际体系不仅仅包括物质和观念分配结构，还包含系统本身的诸多属性，如地理环境、单元特性、单元互动规模、宏观社会趋势等。[①] 这些复杂的系统特征意味着相对于片面强调单一范式和某一结构性动力，国际体系更应被理解为诸多相互交织却又保持独立的社会进程。[②] 网络空间的不断发展为国际体系注入了新的进程，而这一进程势必与其他进程相互影响，从而产生更为复杂多样的网络空间国际政治后果。亦有学者认为，网络空间是继自然环境空间和社会政治空间之后，人类社会面临的第三种重要的互动领域，[③] 而网络安全对国际体系的影响便来自这些互动领域彼此交叠的地带。因此，围绕网络安全展开的理论争鸣，既是国际关系理论对国际体系本质缺乏共识的结果，反过来也为构建更为全面有效的国际体系理论框架提供了契机。厘清网络空间与国际政治空间的互动关系，是在新的社会历史条件下推动理论创新的重要途径。

其次，科学技术在国际政治中扮演着怎样的角色，对这一问题同样缺乏有效的理论化解答。有学者曾一针见血地指出，“国际关系的诸多理论……在将技术理论化和概念化为全球事务变革的有力动因上，几乎无所作为。虽然技术常常隐晦地出现在国际关系和国际政治经济学的理论中，但却总被解读为一种外部的、被动的、非政治且残余的变量。”[④] 然而，从上述网络安全的不同视角可以看出，网络技术及其政治影响并非完全外生于国际政治动态，而是受到政治和安全实践、规则、话语、文化等多种因素的塑造和影响。技术与技术变革不应被视为理所应当的既定事实，其在很大程度上内嵌于人类社会政治的复杂变化之中。科学技术对国际关系的影响显然不容忽视，这一点从航海技术到核技术都早已得到反复证明，但无论是技术决定论，还是将技术简单视为人类能动性的工具，似乎都难以做到技术发展的自身动力与社会政治实践的有机结合。而在当前技术变革速度越来越快、新安全问题层出不穷的背景下，缺乏对于科学技术的理论解释将愈发难以有效理解国际政治的发展现实。

第三，对于网络安全本身而言，弥合不同理论视角的重点任务是构建更为协调和完备的概念性基础。前文已经指出，网络安全的相关概念缺乏统一明晰的共识。这种概念分歧不仅受到理论范式差别的影响，也与研究者的身份角色及其所属政治社会环境密切相关，其结果便是指涉对象与威胁意象等要素迥异

---

① Tang Shiping, “International System, Not International Structure: Against the Agent-Structure Problematique in IR”, *Chinese Journal of International Politics*, Vol. 7, No. 4, 2014, pp. 483-506.

② 例如，秦亚青将过程定义为运动中的关系，认为过程本身具有自在性。参见秦亚青：《关系与过程：中国国际关系理论的文化建构》，上海：上海人民出版社，2012 年。

③ Nazli Choucri, *Cyberpolitics in International Relations*.

④ Stefan Fritsch, “Technology and Global Affairs”, *International Studies Perspectives*, Vol. 12, No. 1, 2011, pp. 27-45.

的网络安全“多重话语”体系。破解多重话语的认知差异并非要求为网络安全等概念建立普遍接受的单一解释，这在网络安全主体多元、利益复杂的现状下显然难以实现。或许可行的方法是为网络安全寻找更具包容性的概念框架。从安全本体来看，网络安全至少指代了四种相互关联的维度：网域安全，这一维度映射着网络空间作为全球公域的属性，其承载着信息技术推动的各类社会关系的运行，因而安全成为人类社会在新兴空间的共有权利；系统安全，这一维度主要涉及网络在物理空间的实际存在，由于组成网络系统的物理设施仍受到地理因素的约束，因而这一维度往往与国家战略与安全紧密相连；发展安全，这一维度凸显了网络及其相关技术在推动人类社会发展上的重要价值，而发展和资源配置等方面的不均衡（如“数字鸿沟”）是网络安全不容忽视的要素；信息安全，网络空间的核心内容便是不断增长、跨越时空局限的信息流动，信息本身（如信息内容、归属等问题）也成为网络安全的重要维度。厘清这些不同维度的内在关系，深入探索不同维度下网络安全的国际政治意义，或许才能有效弥合现有理论视角的分歧，并且通过理论创新带动知识生成，推动科学理性的网络安全政策产出。

（责任编辑：李　丹）