网络空间的攻防平衡与网络威慑的构建*

沈　逸　江天骄

【内容提要】　网络空间已经成为大国战略博弈的新领域。网络空间的军事化是一个难以逆转的客观趋势。目前关于网络攻防、网络威慑及其对大国战略稳定影响的讨论存在不足。一部分观点认为，归因、划线、对称报复等技术困境的存在使得网络威慑难以成立。而网络攻防失衡、进攻更占优势的结果将打破战略稳定，并导致频繁的网络战争，甚至引发冲突升级。然而，这种怀疑论和悲观论实际上模糊了不同程度的网络安全事件之间的界限，又未能全面理解网络攻防之间存在的巧妙平衡。通过对特定网络攻防技术进行区分，再结合对于重大网络安全事件的经验分析，不难发现大规模网络攻击的后果存在诸多不确定性因素，而归因问题也并非无法化解。由此一来，“向谁报复”“在何种情况下报复”以及“如何报复”这三大困扰网络威慑的问题也基本上迎刃而解。以现实主义的基本理念，务实对待和理解网络空间的攻防均衡，通过构建积极的网络威慑实现网络空间的战略稳定，在当下已经具备一定的可行性，也应该成为大国在网络空间战略互动的一个主要方向。

【关键词】　网络战；攻防平衡；网络威慑；网络安全

【作者简介】　沈逸，复旦大学网络空间治理研究中心主任，研究员；江天骄，复旦大学国际关系与公共事务学院博士研究生。（上海　邮编：200433）

【中图分类号】　D815.5　【文献标识码】　A　【文章编号】　1006-9550（2018）02-0049-22

* 本文系国家社科基金一般项目“中国参与网络空间国际规则制定研究”（项目批准号：17BZZ092）的阶段性成果。感谢《世界经济与政治》杂志匿名审稿专家的意见和建议。文中错漏由笔者负责。

一 引言

网络空间已经成为人类活动的第五空间，如同约瑟夫·奈(Joseph Nye)指出的，信息革命发生在既有的政治与社会结构之中，[①]因此网络空间同样面临保持安全与稳定的问题。如同冷战时期的安全研究聚焦如何保持大国战略稳定，避免发生全面核战争导致同归于尽一样，如何在网络空间保持大国战略稳定，正日趋成为各方研究者关注的主要问题。在2016年年底结束的美国总统选举中，有关俄罗斯通过黑客攻击干扰、影响乃至最终左右选举结果的争论，进一步深化了有关网络空间行为与大国战略稳定的讨论。美国国防部于2017年2月发布的《国防科学委员会网络威慑专题小组最终报告》指出，为了应对来自俄罗斯和中国的大规模网络攻击的威胁，美国必须通过明确的报复战略来阻止这类进攻。[②] 大国之间是否会因为网络攻击而爆发大规模的网络战并引发冲突升级是新时期网络技术革命给国际社会带来的难题，在此背景下，探讨实现网络空间战略稳定的务实路径，应该成为一项具有重要理论价值与现实意义的任务。

与核武器相比，目前网络武器的研发、实际使用以及由此带来的网络空间国家之间进攻与防御能力的建设，仍然处于发展过程之中。如何认识网络空间进攻与防御之间的关系，是认识和理解网络空间威慑问题的关键。本文运用攻防失衡与平衡的分析框架，展开相关的研究。在结构上，下文将回顾以往关于网络空间中进攻与防御失衡进而导致网络战频发的观点，并指出其中的矛盾和不足之处。事实上，网络攻防之间尽管具有非对称性，但仍可以形成巧妙的平衡。这种平衡为将传统的威慑战略运用到网络空间提供了重要基础。随后将聚焦讨论网络空间威慑的有效性问题，并指出基于务实路径在网络空间构建有效威慑不仅是可行的，也是必要的。这种威慑形成的过程可能会带来某些冲击，但总体可控。而且在形成之后，从整体看，不仅有助于网络空间达成新的战略稳定，而且对现有国际体系中大国之间的战略稳定也将具有积极意义。

① 约瑟夫·奈著，郑志国等译《美国霸权的困惑》，北京：世界知识出版社2002年版，第120页。

② Defense Science Board, "Task Force on Cyber Deterrence," http://www.dtic.mil/dtic/tr/fulltext/u2/1028516.pdf，访问时间：2017年10月20日。

二 网络战威胁及对网络攻防平衡的新认识

在现有研究中,国外学者倾向于认为网络空间的攻防力量是不平衡的,进攻方将占据比较显著的优势。这是相关研究者将一般攻防理论[①]运用到网络空间的主要研究成果。持这类观点的学者进一步指出,网络空间中存在着进攻占据优势(offence dominance)的情况,这连同网络技术革命和网络武器的出现一起,将从根本上改变传统国际关系中的攻防平衡(offense-defense balance)。[②]

进攻占优的观点主要源于对网络空间技术特征的分析。首先,由于存在"零日漏洞攻击(zero-day attack)",即在相关软件的安全补丁还未上线或是上线的同一天就遭受攻击。其次,即使没有发生"零日漏洞攻击",也无法保证整个网络安全系统没有瑕疵。网络防御需要构筑起一道万无一失的长城,而进攻只需要攻其一点即可突破。防范网络攻击与打击贩毒和偷渡有着许多相似之处。除非事先掌握可靠情报,否则无论投入多少,效费比都会很低。[③] 再次,防御本身处在碎片化的风险之中。私人部门(private sector)掌控了国家的相当一部分网络资源。考虑到企业的声誉或是经营策略,私人部门大多不愿意在调高安全风险等级或是共享网络信息等方面与政府展开合作。甚至在遭到攻击之后,许多企业仍然选择隐瞒事实。[④] 而经济全球化也进一步加

① George H. Quester, *Offense and Defense in the International System*, New York: John Wiley and Sons, 1977; Jack L. Snyder, *The Ideology of the Offensive: Military Decision Making and the Disasters of 1914*, Ithaca: Cornell University Press, 1984; Ted Hopf, "Polarity, the Offense-Defense Balance, and War," *American Political Science Review*, Vol.85, No.2, 1991, pp.475-494; Stephen Van Evera, "Offense, Defense, and the Causes of War," *International Security*, Vol.22, No.4, 1998, pp.5-43; Charles L. 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; Karen Ruth Adams, "Attack and Conquer? International Anarchy and the Offense-Defense-Deterrence Balance," *International Security*, Vol.28, No.3, 2003, pp.45-83.

② John B. Sheldon, "Deciphering Cyberpower: Strategic Purpose in Peace and War," *Strategic Studies Quarterly*, Summer 2011, p.98; Lucas Kello, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft," *International Security*, Vol.38, No.2, 2013, pp.7-40.

③ Samuel Liles, Marcus Rogers, J. Eric Dietz and Dean Larson, "Applying Traditional Military Principles to Cyber Warfare," in C. Czosseck, R. Ottis and K. Ziolkowski, eds., *2012 4th International Conference on Cyber Conflict (CYCON)*, Talinn: NATO CCD COE Publications, 2012, pp.169-180; Forrest Hare, "Borders in Cyberspace: Can Sovereignty Adapt to the Challenges of Cyber Security?" NATO Cooperative Cyber Defence Center of Excellence, 2009, https://ccdcoe.org/publications/virtualbattlefield/06_HARE_Borders%20in%20Cyberspace.pdf,**访问时间:** 2017 **年** 9 **月** 20 **日**。

④ Karine Silva, "Europe's Fragmented Approach Towards Cyber Security," *Internet Policy Review*, Vol.2, No.4, 2013, http://policyreview.info/articles/analysis/europes-fragmented-approach-towards-cyber-security,**访问时间:** 2017 **年** 10 **月** 20 **日**。

深了潜伏在供应链中的安全问题。许多设备在海外制造的过程中极有可能被植入病毒。此外,网络武器可以通过直接复制或变异的方法快速扩散。① 跨国犯罪集团和黑客地下产业链导致恶意软件的扩散渠道更加畅通,获得网络武器的门槛变得更低。最后,网络归因困难重重。② 随着各种加密、代理技术的发展,要成功定位攻击发起者并予以及时的还击几乎难以实现。如果单纯从技术角度分析,在网络空间中既不能通过构筑坚不可摧的防御来拒止敌人的进攻,又无法借助强有力的报复手段来慑止隐匿攻击。进攻的一方享有天然的优势,而防御的一方则显得有些先天不足。

进攻占优的观点将刺激各国发起网络军备竞赛,加深安全困境。在网络技术革命之前,国家间通过明确一系列基本共识、原则和法律制度在一定程度上缓解了国际社会无政府状态的影响。而在进攻占优的观念主导下,网络技术似乎给试图颠覆现行秩序的行为体带来了机会。有学者提出,网络技术革命带来了动荡不安的前景。各国都尚未充分理解网络武器的意义和用相应的法律去规制这一武器的使用,在缺乏有效威慑的情况下,网络战将会成为诱人的战略选择。③ 国家行为体将倾向于选择通过大规模网络攻击而非传统的外交以及军事活动,"兵不血刃"地破坏对方的安全、经济和社会发展。④ 尤其对发达国家来说,由于其过分依赖网络系统,网络攻击能够以非常低的成本造成巨大的损失,从而使原本实力弱小的国家或非国家行为体更容易借助这种不对称优势向大国发起挑战。⑤

此外,网络武器又易于扩散,大幅增加意外战争的可能性。在传统领域,信心建立措施(CBM)、外交热线和其他一系列规范有助于缓解紧张局势、避免冲突升级,而关

① Stephen W. Korns, "Cyber Operations: The New Balance," *Joint Force Quarterly*, Vol.54, 2009, pp.97-98; William A. Owens, Kenneth W. Dam and Herbert S. Lin, eds., *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*, Washington, D.C.: National Academies Press, 2009, pp.2-32.

② Martin C. Libicki, *Cyberdeterrence and Cyberwar*, Santa Monica: RAND, 2009; David D. Clark and Susan Landau, "Untangling Attribution," *Harvard National Security Journal*, Vol.2, No.2, 2011, pp.25-40; W. Earl Boebert, "A Survey of Challenges in Attribution," in Committee on Deterring Cyberattacks, ed., *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*, pp.51-52; Peter W. Singer and Allan Friedman, *Cybersecurity and Cyberwar*, New York/Oxford: Oxford University Press, 2014, p.73.

③ Lucas Kello, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft," pp.36-37.

④ Lucas Kello, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft," p.26.

⑤ Joseph S. Nye, Jr., "Cyber Power," Belfer Center for Science and International Affairs, Harvard Kennedy School, May 2010, p.4, https://www.belfercenter.org/sites/default/files/legacy/files/cyber-power.pdf,访问时间:2017年9月20日。

于网络空间的沟通和协调可能非常模糊。由于国家间彼此难以摸清对方的真实意图，误判的可能性增加。在竞争对手之间，认为自身占据进攻优势的一方很有可能采取先发制人的行动。总体上，如果难以建立有效的威慑，国家间网络战争的发生将变得频繁，国家遭受大规模网络攻击的可能性将急剧上升。① 网络空间的攻防失衡很有可能破坏战略稳定并危及整个国际秩序。

如果上述判断成立，那么其推导出的结论应该是当前世界范围内主权国家之间在网络空间中将持续发生显著的对抗，甚至是某种形式的网络战争。但经验观察的数据并不支撑这样的判断，最为常见的现象，仍然是网络犯罪、网络间谍、网络黑客等很难归因于攻防失衡的低烈度的网络安全事件（cyber incident）屡屡发生。

为何国家间并没有像攻防失衡论者所预计的那样爆发频繁的网络战争？实际上，许多观点未能明确区分网络间谍活动、一般性的网络攻击和大规模的网络战。② 而更为关键的是，相当多的研究主要依据纯粹信息技术领域的分析，并没有能够真正从国家安全的分析框架出发去认识和理解攻击和防御之间的平衡关系，即用信息系统的攻防平衡取代了国家间的攻防平衡分析。

从实践看，在大量的案例中，网络战的威胁被有意或无意地夸大（threat inflation），对网络攻击概念的泛化使用导致了对于实施网络攻击难度的低估，最典型的表现就是混淆了网络攻击和网络利用这两类相似但存在重大区别的活动。③ 根据美国国防部、参谋长联席会议等发布的文件来看，国家安全战略框架下的网络攻击（CNA）和网络利用（CNE）这两种类型的行动是这样被定义的：网络攻击是指由计算机网络发起或针对计算机网络而进行的各种扰乱、禁止访问、破坏和摧毁计算机

① Andrew F. Krepinevich, "Cyber Warfare: A Nuclear Option?" Center for Strategic and Budgetary Assessment, 2012, p.8, http://csbaonline.org/uploads/documents/CSBA_e-reader_CyberWarfare.pdf, 访问时间: 2017 年 10 月 20 日。

② Stephen M. Wal, "Is the Cyber Threat Overblown?" *Foreign Policy*, March 30, 2010, http://walt.foreignpolicy.com/posts/2010/03/30/is_the_cyber_threat_overblown, 访问时间: 2017 年 10 月 20 日; Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies*, Vol.35, No.1, 2012, pp.5-32。

③ Myriam Dunn Cavelty, "Cyber-Terror—Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate," *Journal of Information Technology & Politics*, Vol.4, No.1, 2008, pp.19-36; Jane K. Cramer and A. Trevor Thrall, "Understanding Threat Inflation," in A. Trevor Thrall and Jane K. Cramer, eds., *American Policy and the Politics of Fear: Threat Inflation Since 9/11*, London: Routledge, 2009, pp.1-15; Jerry Brito and Tate Watkins, *Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy*, Arlington: Mercatus Center, George Mason University, 2011.

信息的行动(攻击分类如表1所示)。[①] 在攻击过程中,不仅包含对于数据的破坏和操控,而且强调由此产生的后果,特别是通过攻击行动造成的物理毁伤,包括关键基础设施的破坏以及人员的伤亡。[②] 网络利用更多是指利用网络进行侦查、干扰、窃取信息等活动,日常生活中被广泛报道的案例绝大多数属于此类行动。虽然与网络攻击在技术、手段甚至是某些外部表现形式上存在相似性,但仍然应当区别对待。[③]

表1 网络攻击的类型[④]

攻击类型	描述	主要特征	潜在目标	案例
僵尸程序或DDoS攻击	通过控制大量系统发起集中访问,使目标网络连接中断	成本较低;技术门槛不高;效果仅局限于中断访问而不能造成物理损伤	大部分网络	2008年,俄格冲突中俄罗斯中断了格鲁吉亚政府网站的连接
普通恶意软件	利用漏洞入侵、传输数据或扰乱系统正常运行	成本较低;对防护较弱的系统适用	大部分计算机或网络	计算机病毒、钓鱼软件、蠕虫病毒
高级恶意软件	利用漏洞入侵、传输数据或扰乱系统正常运行	成本较高;技术门槛高;能够入侵防护级别较高甚至与外部网络隔绝的系统;同时可能造成连锁反应	重点基础设施	震网病毒对伊朗的浓缩铀离心机造成了破坏

资料来源:笔者自制。

① Department of Defense, Washington, D.C., "Dictionary of Military and Associated Terms," Joint Publication 1-02, November 8, 2010, http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf,访问时间:2017年10月20日。

② 如果网络攻击只是导致信息层面的影响而没有造成严重的物理毁伤或人员伤亡,那么这种攻击不构成国际法意义上的武力攻击(armed attack)。参见Michael N. Schmitt, "Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework," *Columbia Journal of Transnational Law*, Vol. 37, 1998-1999, pp.885-937; Yoram Dinstein, "Computer Network Attacks and Self-Defense," *International Law Studies-Naval War College*, Vol.76, 2002, pp.99-119。

③ 就像使用无人机既可以实施侦察,又可以发动攻击,或两者兼而有之,但侦察和打击显然是需要区别对待的行为。

④ Adam P. Liff, "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War," *Journal of Strategic Studies*, Vol.35, Issue 3, 2012, pp.406-407.

从国家安全的角度来看，利用网络进行侦查、干扰、窃取信息或者发动分布式拒绝服务攻击(DDoS)与利用网络对关键基础设施造成严重破坏的网络攻击是性质完全不同的事件(见图 1)。这就好比仅因为与火药产生的化学反应有关，就将用烟花进行恶作剧与持枪抢劫银行、安装路边炸弹和使用巡航导弹视为同样性质的行为，而这至少是不严谨的归类。①

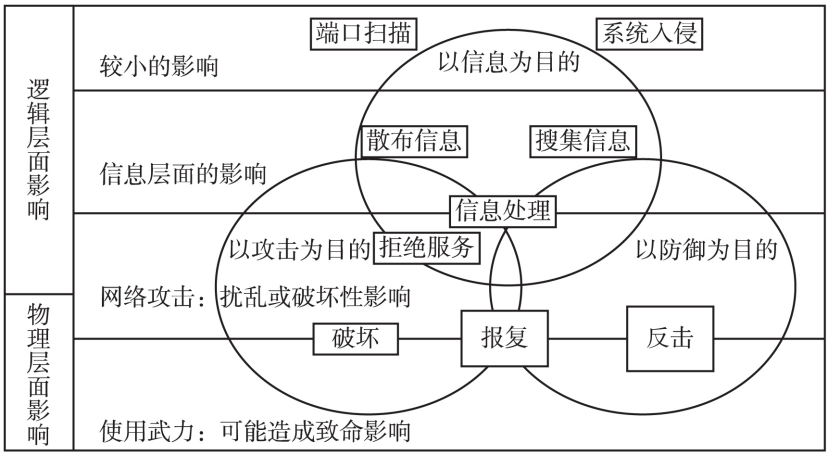

图 1　网络技术活动分类

资料来源： Robert Belk and Matthew Noyes, "On the Use of Offensive Cyber Capabilities: A Policy Analysis on Offensive US Cyber Policy," Paper, Science, Technology, and Public Policy Program, Belfer Center, March 2012, p. 22, https://www.belfercenter.org/sites/default/files/files/publication/cybersecurity-pae-belk-noyes.pdf，**访问时间：** 2017 年 10 月 20 日。

就已经发生的案例进行分析可以发现，实施能够威胁国家安全的网络攻击的难度远比预想的要高，仅认定网络攻击技术的高速发展就会自动导致滥用网络攻击能力实施网络战的论点并没有得到实际案例的支撑。从 2001 年至 2011 年，地缘竞争对手在网络冲突事件中不仅没有发生擦枪走火，反而表现出了自我克制。② 这种克制很大程度上是源于网络攻击的门槛。关于震网病毒的案例研究表明，实施有效的威胁国家安

① 彼得·辛格、艾伦·弗里德曼著，中国信息通信研究院译《网络安全：输不起的互联网战争》，北京：电子工业出版社 2015 年版，第 60—61 页。

② Brandon Valeriano and Ryan C Maness, "The Dynamics of Cyber Conflict Between Rival Antagonists, 2001-2011," *Journal of Peace Research*, Vol.51, No.3, 2014, pp.347-360.

全的战略级网络攻击的成本巨大且门槛极高。[①] 该网络武器的研制与实施过程远非轻而易举。

首先，需要通过搜集情报理解复杂的工业控制系统并发现可以利用的漏洞；然后设法将网络武器放置到与外界隔绝的系统当中并确保能够按时引爆，还要对此进行反复的实验。这样庞大的工程需要大量的人力、物力、财力和先进技术的保障。战略网络战与普通的网络攻击或是黑客活动相去甚远，需要对于不同的攻击目标定制不同的网络武器，投入高、研发周期长且需要具有相当的试验条件（例如离心机），非网络强国几乎难以实现。此外，战略网络攻击被曝光的风险也很高。大规模行动往往因为大量的准备工作而暴露蛛丝马迹。参与秘密行动的人越多、准备周期越长，泄密的可能性也就越大。[②] 而所谓的奇袭（例如珍珠港事件、九一一事件等）总是伴随着许多偶然因素，在很大程度上，事件中的有利条件（例如遗漏重要情报）往往源于对手的各种失误。所以，战略级网络攻击的成功还有赖于网络空间以外的大量因素。即便个别国家不惜一切代价成功研制了高级恶意软件并能够顺利实施计划，网络武器的战略作用究竟有多大仍值得怀疑。[③] 在这种情况下，频繁发动大规模网络攻击既不明智也不现实。

因此，即使是在网络技术经历着突飞猛进发展的今天，大规模网络攻击并非许多技术决定论者所想象的那样能够轻易实现。国家在面临网络技术革命所可能引发的安全困境时也并非没有消除误判、重塑战略稳定的可能。当务之急是要形成新的认知框架，客观评估网络攻防的平衡状态，从而对于网络空间中的特定活动——如网络进攻、网络防御、网络利用等——形成共同的理解和预期。

三　对网络攻防平衡的新认识

与传统的关于进攻占据优势的认知不同的是，网络攻击的后果存在着局限性和不确定性。事实上，频繁的网络攻击会增加自我暴露的风险，反而有利于防御方进行能力建设，甚至有可能帮助防御方解决对网络攻击的归因问题。对于网络攻击归

① Jon R. Lindsay, "Stuxnet and the Limits of Cyber Warfare," *Security Studies*, Vol.22, No.3, 2013, pp.365-404.

② Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks," *Journal of Strategic Studies*, Vol.38, No.1-2, 2015, p.31.

③ David Betz, "Cyberpower in Strategic Affairs: Neither Unthinkable Nor Blessed," *Journal of Strategic Studies*, Vol.35, No.5, 2012, pp.689-711; Thomas Rid, "Cyber War Will Not Take Place," pp.5-32.

因问题的探讨已持续了较长的一段时间。有一些学者提出归因问题完全无法解决,①也有观点认为归因更多反映的是政治问题而非技术问题。② 所谓归因就是国家认为它是什么(attribution is what states make of it)。③ 许多方法可以有助于化解归因困境。

首先,可以对遭受攻击的情况进行分析,小规模的攻击不太可能是为了政治施压,大规模的攻击不太可能是意外,隐蔽性强的攻击可能是意在窃取数据。如果运用过多的资源进行攻击,则意味着攻击者可能是单独行动,而不具备组织化程度,因为组织强调效率。为了提升攻击效率,攻击者可能重复使用相关恶意软件或采取熟悉的攻击手法,这种特征暴露了攻击行为。④ 而通过长期观察攻击的时间以及间隔,攻击者所在的时区和位置很有可能被探查到,攻击越多越容易暴露马脚。⑤ 攻击过程中可能留下的自然语言信息也有可能暴露攻击者的身份。上文已经谈到,由于针对特定复杂系统进行攻击的任务难度较高,许多个人和组织自然被排除在外。同时又需要针对复杂系统搜集大量前期的情报工作,这一环节也很有可能暴露行动。网络攻击很有可能是大规模行动的一个环节,因此通过考察整个地缘政治态势也能发现端倪(例如爱沙尼亚和格鲁吉亚事件)。即便归因不是完全正确,公布一些调查报告或者发布所谓的证据仍然可以对攻击者造成外交和心理上的压力。通过污名化策略(naming and shaming)可以打击对手的国际声誉和软实力,从而在一定程度上起到反制作用。⑥ 尽管归因能力越强越好,但在没有绝对把握的情况下仍然可以结合具体情况采取相应措施。⑦

---

① David D. Clark and Susan Landau, "Untangling Attribution," in Committee on Deterring Cyberattacks, ed., *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*, pp.25-40; Jason Healey, *A Fierce Domain*, Washington, D.C.: The Atlantic Council, 2013, p.265.

② W. Earl Boebert, "A Survey of Challenges in Attribution," pp.41-54; Amir Lupovici, "The 'Attribution Problem' and the Social Construction of 'Violence'," *International Studies Perspectives*, Vol.3, 2014, pp.1-21.

③ Thomas Rid and Ben Buchanan, "Attributing Cyber Attacks," p.7.

④ 一个进行过大量网络牟利活动的国家可能会暴露其独特的行事手法(modus operandi,简称 MO),可以利用它来追踪攻击源头。如果攻击方只是简单的方法重复,那么归因就相对容易。尽管攻击方仍然有太多方法来隐藏自己,但仍然可以通过分析攻击规模、手法大致判断出攻击意图,进而缩小范围找到攻击者。参见马丁·利比基著,薄建禄译《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 86 页。

⑤ "Crowd Strikes's Threat Intelligence," in *Global Threat Report*, January 22, 2014, p.18, https://www.crowdstrike.com/resources/reports/global-threat-report-2014/,访问时间:2017 年 11 月 5 日。

⑥ Joseph S. Nye, Jr., "From Bombs to Bytes: Can Our Nuclear History Inform Our Cyber Future?" *Bulletin of the Atomic Scientists*, Vol.69, No.5, 2013, p.12; Dmitri Alperovitch, "Towards Establishment of Cyberspace Deterrence Strategy," Paper from 3rd International Conference on Cyber Conflict, 2011, pp.1-8.

⑦ Forrest Hare, "The Significance of Attribution to Cyberspace Coercion: A Political Perspective," Paper from 4th International Conference on Cyber Conflict, 2012, pp.1-15.

其次，若要通过网络攻击施加持续的影响力，则必须要与其他手段相结合，网络武器单独使用的战略有效性本质上是有限的。① 网络作为军事行动的倍增器能够发挥强大的辅助作用，但在没有传统军事行动配合的情况下，仅仅依靠网络无法实施占领，也不可能迫使对方投降。② 事实上，大部分网络攻击可以被快速修复。③ 与核武器所造成的致命效果不同，各方对网络武器究竟能造成多大的破坏力并没有清晰的共识。网络武器具有生命周期短且后果不确定的特点（见图 2）。④ 不同类型的攻击具有不同的功效衰退率。如果某种攻击手法的知名度很高（例如震网病毒），那么相关漏洞也会很快被修复；而网络牟利活动由于长期不容易被发现，因此衰退率比较低。⑤ 还存在着许多其他导致网络攻击可能无效的原因，例如在阿富汗战争中，美国的网络攻击作用不大，因为对手并不依赖于网络系统。网络攻击也并非如宣称的那样是精确打击武器。⑥ 网络攻击后果的不确定性，包括武器扩散、连锁反应等，都很有可能波及第三方并造成附带毁伤。震网病毒被发现后，许多系统又遭受被改编过的病毒的袭击，造成了严重的级联效应（cascade effect）。⑦ 而在网络空间互联互通的背景下，大规模网络攻击所带来的严重后果很有可能反噬攻击者自身。虽然匿名使得攻击看似不对称，但大规模网络攻击的反作用是对称的。尤其如中美两国一般，在经济金融高度相互依存的情况下，任何一方遭受网络攻击同样会给另一方的经济金融发展带来冲击。⑧ 这种不确定性和反噬作用使得大规模网络攻击成为某种程度上自我遏制的武器。

同样地，网络防御也并非毫无效用，尽管网络攻击具备优势，但拥有良好的防御和快速恢复的弹性将提升攻击的难度。相比核武器所造成的近似绝对的毁伤效果，网络

---

① Erik Gartzke, "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth," *International Security*, Vol.38, No.2, 2013, p.58.

② Martin C. Libicki, *Cyberdeterrence and Cyberwar*, p.119.

③ Martin C. Libicki, *Conquest in Cyberspace: National Security and Information Warfare*, New York: Cambridge University Press, 2007, pp.5-6; Tim Maurer, "The Case for Cyberwarfare," *Foreign Policy*, October 19, 2011, http://www.foreignpolicy.com/articles/2011/10/19/the_case_for_cyberwar，访问时间：2017 年 11 月 5 日。

④ Erik Gartzke, "The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth," pp.41-73; David Kushner, "The Real Story of Stuxnet," *IEEE Spectrum*, Vol.50, No.3, 2013, pp.48-53; Samuel Liles, et al., "Applying Traditional Military Principles to Cyber Warfare," pp.1-12.

⑤ 马丁·利比基《兰德报告：美国如何打赢网络战争》，第 53—54 页。

⑥ Martin C. Libicki, *Cyberdeterrence and Cyberwar*, p.177.

⑦ 除了伊朗以外，世界上有 154 个国家的网络系统遭受到震网病毒的攻击，占病毒感染总数的 40%以上。参见 Nicholas Falliere, et al., *W32.Stuxnet Dossier*, CA: Symantec Security Response, 2011, p.6。

⑧ Joseph S. Nye, Jr., "From Bombs to Bytes: Can Our Nuclear History Inform Our Cyber Future?" p.11.

动能武器（例如导弹）

研发→→→生产→→武器存续→→→→→→→→→→→→→→→→→→→→→拆卸销毁

网络武器（例如震网病毒）

研发→武器存续→安全补丁？→防火墙升级？→更换操作软件？→更换硬件？

图 2　网络武器生命周期①

资料来源：笔者自制。

攻击仍然是可以防御的，遭受攻击之后具备足够能力和资源的行为体仍然可以具备有效的恢复能力。防御方可以通过设置多个防御层次和大量的系统冗余，尽可能减缓攻击速度，为检测和应对争取时间。当攻击者需要采取包括搜集信息、研发武器、植入并释放武器等一系列步骤时，防御方可以在任何步骤发现并采取行动。同时，防御方还可以巧妙地利用欺骗战术迷惑对手。由于大多数对于欺骗战术的研究视角都聚焦于进攻一方，网络空间的复杂特征总是被当成防御方所面临的挑战。② **但实际上这种复杂性对于进攻方来说同样意味着许多困难和不确定因素。防御方可以通过设置"蜜罐"等技术手段，**③**使攻击者担忧到处都布满陷阱，从而迷失方向，并最终服务于攻击检测、归因和关键基础设施的防护。**④ **考虑到最有价值的攻击目标往往是最为复杂的，而攻击成本和被发现的风险极大，攻击者就很有可能转向那些低风险、低回报的目标。**⑤ **事实上，任何作战领域都不存在所谓完美（**perfect**）的防御，只有建立妥善（**good

① Michael Robinson, Kevin Jones and Helge Janicke, "Cyber Warfare: Issues and Challenges," *Computers & Security*, Vol.49, 2015, p.81.

② Barton Whaley, "Toward a General Theory of Deception," *Journal of Strategic Studies*, Vol.5, Issue 1, 1982, pp.178-192.

③ Lance Spitzner, "Honeypots: Catching the Insider Threat," *Proceedings of the 19th Annual Computer Security Applications Conference*, Washington, D.C.: IEEE Computer Society, 2003, pp.170-179; Neil C. Rowe, E. John Custy and Binh T. Duong, "Defending Cyberspace with Fake Honeypots," *Journal of Computers*, Vol.2, No. 2, 2007, pp.25-36; Julian L. Rrushi, "An Exploration of Defensive Deception in Industrial Communication Networks," *International Journal of Critical Infrastructure Protection*, Vol.4, No.2, 2011, pp.66-75; Kristin E. Heckman, et al., "Active Cyber Defense with Denial and Deception: A Cyber-Wargame Experiment," *Computers & Security*, Vol.37, No.3, 2013, pp.72-77.

④ Jim Yuill, Dorothy E. Denning and Fred Feer, "Using Deception to Hide Things from Hackers: Processes, Principles, and Techniques," *Journal of Information Warfare*, Vol.5, No.3, 2006, pp.26-40; Kristin E. Heckman and Frank J. Stech, "Cyber-Counterdeception: How to Detect Denial & Deception (D&D)," in Cyber Wargames, ed., *Sushil Jajodia*, New York: Springer, 2015.

⑤ Erik Gartzke and Jon R. Lindsay, "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace," *Security Studies*, Vol.24, No.2, 2015, p.343.

enough)的防御体系,使其足以承受一定程度的损伤并能够快速得到修复,从而继续作战。[①] 所以,冗余、欺骗和快速恢复的弹性使得网络防御并非不堪一击。例如网络并未在2008年的俄罗斯与格鲁吉亚冲突中起到决定性作用。[②] 格鲁吉亚通过改变其在美国服务器上的网站的主机,将其移动到光纤连接带宽更宽、系统管理员更机敏的环境中,成功避开了DDoS攻击。[③] 而即便是震网病毒也没有迫使伊朗放弃核计划,反而使其迅速强化了自身网络部队的建设。[④] 而网络攻防平衡最为核心的一点还在于对手会通过修复被攻击的漏洞而降低自身系统的脆弱性。[⑤] 发动网络攻击的过程其实也是帮助对手揭示其系统漏洞的过程。所以网络攻击越频繁,后续攻击的难度也就越大,网络攻击的效果也就相应被削弱。由于网络防御能力的差别,相同频度的网络攻击也会产生不同的攻击效果(如图3)。

综合网络攻击与网络防御两方面来看,两者之间事实上存在着巧妙的平衡与辩证统一。在一轮接一轮的军事技术革命中,从来都是兵来将挡、水来土掩,网络攻防的水平都会不断提升,网络武器越强大,网络防御的意识也越高。进攻方对网络技术隐蔽、快速的特点进行利用,防御方则通过欺骗、设置冗余和快速修复进行应对。尽管越来越多的国家建立起网络部队并将网络武器投入实战,但这同时引起了更多国家对网络安全的重视,并在此基础上凝聚共识、制定规则。许多非国家行为体对网络攻击的参与也唤起了社会中各行各业广泛的网络安全意识,以期共同应对网络威胁。尽管网络武器有着不同寻常的效用,但单纯依靠网络攻击即可

① Colin S. Gray, "Strategic Thoughts for Defence Planners," *Survival*, Vol.52, No.3, 2010, pp.159-178.

② Stéphane Lefebvre and Roger N. McDermott, "Intelligence Aspects of the 2008 Conflict Between Russia and Georgia," *Journal of Slavic Military Studies*, Vol.22, No.1, 2009, pp.4-19; Timothy L. Thomas, "The Bear Went Through the Mountain: Russia Appraises Its Five-Day War in South Ossetia," *Journal of Slavic Military Studies*, Vol.22, No.1, 2009, pp.31-67.

③ 马丁·利比基《兰德报告:美国如何打赢网络战争》,第103页; Stephen Korns, "Botnets Outmaneuvered: Georgia's Cyberstrategy Disproves Cyberspace Carpet-Bombing Theory," *Armed Forces Journal*, January 1, 2009, http://armedforcesjournal.com/botnets-outmaneuvered/,访问时间:2017年11月20日。

④ Paul K. Kerr, John Rollins and Catherine A. Theohary, *The Stuxnet Computer Worm: Harbinger of an Emerging Warfare Capability*, Washington, D.C., Congressional Research Service, 2010; David Albright, Paul Brannan and Christina Walrond, *Did Stuxnet Take Out 1,000 Centrifuges at the Natanz Enrichment Plant?* Washington, D.C.: Institute for Science and International Security, 2010.

⑤ Gregory Rattray and Jason Healey, "Categorizing and Understanding Offensive Cyber Capabilities and Their Use," in Committee on Deterring Cyberattacks, ed., *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*, p.79.

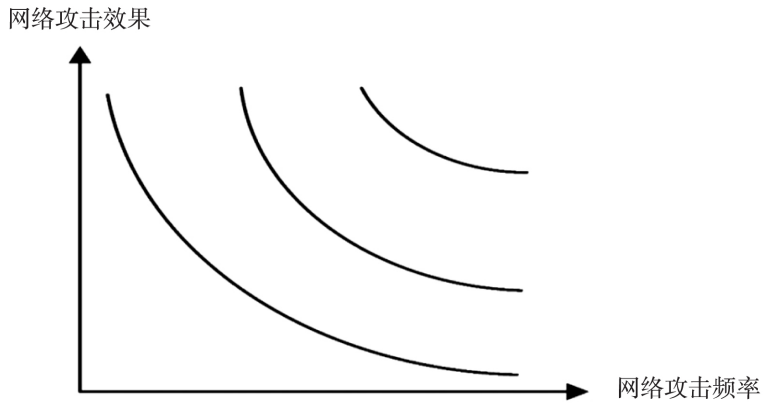

图 3　网络攻击频度与攻击效果示意图

资料来源: 笔者自制。

将对手一击即溃的论调更多属于假想。[①] 网络力量所具有的真正战略意义是创造有利于己方而不利于对手的环境，即通过战术网络战发挥作用。[②] 而当网络与其他手段相结合时，真正具有决定性意义的往往不是某一项新技术、新武器的使用，而是通过灵活的军事战略原则和排兵布阵，最大限度地发挥自身作战优势，打击对手的弱点。

综上所述，虽然目前在网络空间攻击和防御之间仍然是非对称的，攻击相比防御仍然具有一定的优势，但在国家安全框架下来看，攻击和防御仍然是相对平衡的，并没有出现攻击方占据压倒性优势从而单方面改变游戏规则的现象。

四　网络威慑的实现路径

在网络攻防平衡的前提下，传统威慑理论在网络空间中的运用得到确立。威慑作为一种古老的战略思想一直是国家应对战争威胁的主要手段。威慑的核心环节是劝服(convince) 对手，使其相信采取行动的后果是不利的。[③] 清晰地表达意图并展示相

① Martin Libicki, "Cyberspace Is Not a Warfighting Domain," *I/S: A Journal of Law and Policy for the Information Society*, Vol.8, No.2, 2012-2013, pp.321-336; Colin S. Gray, *Making Strategic Sense of Cyber Power: Why The Sky Is Not Falling*, Washington, D.C.: Strategic Studies Institute and U.S. Army War College Press, 2013.

② John B. Sheldon, "Deciphering Cyberpower: Strategic Purpose in Peace and War," p.103.

③ Lawrence Freedman, *Deterrence*, Malden: Polity Press, 2004, p.6.

应的实力是关键所在。而产生这种心理效果的前提是信息对称，即双方对于进攻、防御以及报复的效果都有比较清晰的认识，可以计算出利弊得失。[①] 威慑主要分为拒止和报复两大类。[②] 所谓拒止就是通过足够强大的防御来削弱对手进攻成功的可能性、减少其进攻得手所带来的收益，但拒止需要付出巨大的防御成本；而报复则是通过给对手的攻击行为施加严重的后果，使其不愿付出可怕的代价而放弃行动。20 世纪初期的军事学说仍然强调防御，例如通过修筑马其诺防线来实现拒止威慑。而随着军事技术的发展，防御的漏洞变得越来越明显。到了第二次世界大战时期，闪电战、进攻崇拜成为军事作战领域的新潮流。冷战时期，由于核打击几乎无法防御，更多的战略重心于是放在了报复威慑上，即通过相互确保摧毁来避免战争的发生。尽管如此，冷战中后期，美苏两国仍然通过建立导弹防御获取一定程度的拒止威慑，试图打破所谓的恐怖平衡。冷战结束后，威慑仍然是 21 世纪美国国家安全战略的核心。为了应对更加复杂的安全威胁，美国在 2003 年又提出了定制型威慑（tailored deterrence）的概念，即根据对手不同的身份、利益、认知以及决策过程，在不同的背景下施加相应的威慑手段，最终影响对手的利益计算。[③] 从 2011 年至 2015 年，美国白宫和国防部陆续发布《网络空间国际战略》和《网络空间行动战略》及其修订版本，这些文件将传统威慑战略引入网络空间。

在网络空间中，报复威慑主要涉及“向谁报复”“在何种情况下报复”以及“如何报复”三个方面的问题。诚然，这三个问题有可能影响报复威慑的可靠性和有效性。根据以往的不少分析而言，在网络空间中所有人都可以采用匿名身份，唯一有效的追踪方式是 IP 地址。而由于各种加密、代理技术的发展，成功定位攻击发起者并予以及时还击几乎是难以实现的。[④] 即便能够找到幕后真凶，如果攻击者所在国不给予相应的协助，也根本无法启动司法程序。更不用说这其中还涉及许多没

① Albert Wohlstetter, “The Delicate Balance of Terror,” *Foreign Affairs*, Vol.37, 1959, pp.211-234; Bernard Brodie, *Strategy in the Missile Age*, Princeton: Princeton University Press, 1959; Thomas C. Schelling, *The Strategy of Conflict*, Cambridge: Harvard University Press, 1960; Robert Jervis, “Deterrence Theory Revisited,” *World Politics*, Vol.31, No.2, 1979, pp.289-324; Patrick M. Morgan, *Deterrence: A Conceptual Analysis*, Beverly Hills: SAGE, 1983; Robert Jervis, R. N. Lebow and J. G. Stein, eds., *Psychology and Deterrence*, Baltimore: Johns Hopkins University Press, 1985.

② Glenn H. Snyder, *Deterrence and Defense: Toward a Theory of National Security*, Princeton: Princeton University Press, 1961.

③ Kevin Chilton and Greg Weaver, “Waging Deterrence in the Twenty-First Century,” *Strategic Studies Quarterly*, Spring 2009, pp.31-34.

④ Larry Greenemeier, “Seeking Address: Why Cyber Attacks Are So Difficult to Trace Back to Hackers,” *Scientific American*, June 11, 2011, http://www.scientificamerican.com/article/tracking-cyber-hackers/，访问时间：2017 年 12 月 2 日。

有定论的国际制度合作问题。在这种情况下,报复错误还可能树立新的敌人。报复威慑还面临着划线困境(艾奇逊困境),即清楚地界定什么样的行为会遭到报复意味着对那些没有触及红线的挑战束手无策。① 而广泛的承诺显然难以全部兑现,最终将削弱承诺的可信度。此外,根据国际法上的对称性原则,通过网络来反击对手发动的网络攻击(in kind)似乎是比较妥当的。但如果反击的力度较弱就无法通过让对方付出沉重的代价来迫使其改变行为,网络攻击仍将继续;如果发起强有力的反击,甚至不惜动用网络以外的军事手段,则很有可能引发冲突升级。然而,这三个问题并不必然存在,也并非没有解决方法。在一定的情况下,报复威慑可以通过划定较为清晰的威慑目标、设定可靠的报复门槛、建立和展示可信的报复力量予以确立。

具体而言,首先,关于"向谁报复"的问题,网络威慑的目标是比较清晰的。威慑的对象应该是那些企图利用网络袭击本国的对手。这种网络袭击的严重程度应当与军事行动可能造成的后果基本相当。所以威慑的对象必须符合两点:(1)明确的敌人;(2)严重的大规模网络攻击。② 一些批评网络威慑不可行的观点实际上错误地将威慑对象扩大化了。网络黑客、网络间谍(牟利)、网络犯罪等活动确实难以归因并及时报复,但这些行为既不一定是敌人所为,所采用的隐匿攻击或分布式拒绝服务攻击也一般无法造成严重的后果。由于本来就没有达到直接影响国家安全的程度,也就不在威慑的范围之列。网络恐怖主义是否属于威慑对象同样值得怀疑。绝大多数的恐怖组织利用网络进行活动策划与协调、募集资金、招募支持者、宣传思想以及搜集情报等工作。③ 当然,恐怖组织也会利用网络进行黑客攻击,但研发复杂的高级网络武器并实施大规模网络攻击对于恐怖组织来说性价比不高,④也未必能够造成所期望的恐怖效果。⑤ 如果是国家行为体发动的大规模网络攻击,那么

① 美国国务卿艾奇逊曾在 1949 年发表讲话明确美国的海外核心利益。美国明确谈到将对哪些国家进行保护使其免遭苏联入侵的威胁,但没有提到韩国。当 1950 年朝鲜战争爆发后,人们质疑正是因为没有给予韩国安全保护的承诺从而使苏联阵营发动大规模进攻。

② Patrick M. Morgan, "Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm," in Committee on Deterring Cyberattacks, ed., *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*, p.58.

③ Evan F. Kohlmann, "The Real Online Terrorist Threat," *Foreign Affairs*, Vol.85, No.5, 2006, pp.115-124; Timothy L. Thomas, "Al-Qaeda and the Internet: The Danger of 'Cyperplanning'," *Journal of Range Management*, Vol.43, No.4, 2003, pp.344-346.

④ Irving Lachow, "Cyber Terrorism: Menace or Myth," in Franklin Kramer, Stuart Starr and Larry Wentz, eds., *Cyberpower and National Security*, Dulles: Potomac Books, 2009, pp.442-447.

⑤ 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.

归因问题很有可能不言自明。网络攻击与现实世界有着密切的关联。许多观点过分强调了网络技术作为一种有效的手段，而忽视了更为关键的目的性因素，即为何要发动网络战。[①] 所谓战争，就是己方通过运用实力（进攻或防御）、发出威胁（威慑或威逼）或所谓的影子战争（例如外交手段）迫使对手去做己方想要做的事。[②] 战争是政治的延续，战争作为一种手段必然清楚地表达政治目的。[③] 不同的政治目的伴随着不同的网络攻击形式，单纯的牟利行为可能难以被察觉，但如果是试图通过网络施压或者结合网络采取军事行动，那么依靠隐匿攻击无法实现其政治目的。因此，网络威慑所需要应对的大规模网络攻击基本不会受到归因问题的困扰。

其次，关于“在何种情况下报复”的问题，根据上文对网络攻防平衡的讨论可以发现，划定报复门槛的问题是可以得到解决的。由于对手能够通过修复被攻击的漏洞而降低脆弱性，网络攻击频繁度的增加会导致后续攻击的难度上升。单纯依靠战略网络战难以彻底击败对手或迫使其投降，而攻击所产生的附带毁伤和其他不确定性结果反而给攻击者造成巨大的压力。所以，在对待大规模网络攻击时，潜在攻击者或审慎克制，或孤注一掷。既然威慑的目标是劝阻敌人不要发动大规模的网络攻击，那么时不时在重大利益问题上宣示报复政策，将报复的门槛设置得高一些是明智的。那些小规模的网络攻击、网络黑客或是网络间谍行为本来就不在报复对象之列。实施威慑的一方在一些小规模的网络攻击问题上不做出回应并不会削弱其报复政策的可信度，这恰恰是因为这些行为没有达到需要报复的门槛。而从潜在攻击者的角度来说，也不会频繁发动报复门槛以下的一般性网络攻击，因为这样做反而会帮助对手修复漏洞、提升防御力甚至暴露自己。

最后，关于“如何报复”的问题，为了使报复可信，必须展示（demonstrate）足够的报复力量。由于国家间对于各自是否拥有网络武器以及能够造成多大的伤害并没有客观清醒的认知，再加上为了避免削弱战斗力，许多网络武器和网络行动都秘密进行，结果反而导致报复威慑的可信度降低。在这种情况下，适当炫耀武力——“秀肌肉（brandishing）”——有助于提升报复威慑的可信度。[④] 展示能够反复侵入对

① Erik Gartzke, “The Myth of Cyberwar: Bringing War in Cyberspace Back Down to Earth,” p.42.

② Geoffrey Blainey, *The Causes of War*, New York: Free Press, 1973; James D. Fearon, “Rationalist Explanations for War,” *International Organization*, Vol.49, No.3, 1995, pp.379-414.

③ Carl von Clausewitz, Michael Howard and Peter Paret, eds., and trans., *On War*, Princeton: Princeton University Press, 1976, p.87.

④ Martin C. Libicki, *Brandishing Cyberattack Capabilities*, Santa Monica: RAND Corporation, 2013.

手敏感网络系统的能力，将使对手感知到己方强大的网络实力。在这一过程中，揭示对手的系统漏洞并成功渗透可以削弱对手对自身网络实力的信心。但由于对手会很快修复漏洞，想要持续渗透面临巨大的挑战。此外，大部分敏感系统都加固了防御措施并与外界隔绝，而高强度的侵入方式可能导致冲突升级。所以“炫耀武力”同样存在一定的挑战和风险。除了直接向对手“炫耀武力”之外，报复威慑的可信度还取决于本国在网络安全问题上一贯的行为模式、他国对本国整体的军事科技水平的认知（本国军事力量的国际声望）以及在特定情况下使用网络武器的可能性。美国通过公开宣示威慑政策、发动震网病毒攻击并开展大量网络战演习，已经充分展示了强大的网络实力。美国使用震网病毒一事并没有在美国国内遭受广泛质疑，[①]就连美国国防高级研究计划局（DARPA）被披露正在研发网络武器一事也没有受到谴责。[②] 与此同时，英国和加拿大等国家也表示支持网络先发制人的策略。[③] 2016 年，美国和英国公开宣布对“伊斯兰国”发动网络攻击。而此前俄罗斯被指对爱沙尼亚和格鲁吉亚发动的网络攻击同样展示了其强大的网络实力，从而提升了网络威慑的可信度。

同时，可信的报复力量不应局限于单一的网络攻击武器，而是应当结合不同类型的威胁定制不同的报复工具，将威慑政策、法律手段、外交手段、经济制裁、网络攻击甚至传统军事手段混合使用，才能灵活应对各种挑战。[④] 尽管用网络手段报复网络攻击的做法既符合国际法中的对称原则，又可以避免冲突升级，跨域威慑（cross domain deterrence）反而能起到更好的效果。[⑤] 比如网络反击显然是无法应对网络间谍行为的。除了归因问题之外，网络间谍行为本身就说明了对手并不拥有值得窃取回来的资产。所以，通过提高对手的经济成本，包括使用制裁、关税和外交施压等工具，或许比网络反击更能从根本上影响对手的行为。而在威慑大规模网络攻击的问题上，跨域威慑迫使对手顾忌报复手段的不确定性。为了规避遭受大规模报复的风险，对手往往会

① David Sanger, “Obama Order Sped Up Wave of Cyberattacks Against Iran,” *New York Times*, June 1, 2012, p.1.

② Ellen Nakashima, “With Plan X, Pentagon Seeks to Spread U.S. Military Might to Cyberspace,” *Washington Post*, May 30, 2012, p.A1.

③ Agence France-Presse, “Cyber Strikes a ‘Civilized’ Option: Britain,” *Technology Inquirer*, June 3, 2012, http://technology.inquirer.net/11747/cyber-strikes-a-civilized-option-britain，访问时间：2017 年 10 月 20 日。

④ William A. Owens, Kenneth W. Dam and Herbert S. Lin, eds., “Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities,” National Research Council, 2009, Chapter 1, http://www3.nd.edu/~cpence/eewt/Owens2009.pdf，访问时间：2017 年 12 月 2 日。

⑤ Patrick M. Morgan, “Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm,” p.68.

选择稳妥的攻击方式或者干脆放弃攻击。美国的威慑战略中没有具体明确报复的手段，而是采取一种战略模糊（calculated ambiguity），将多种手段组合到一起，从中选择最合适的报复方式。美国国防部国防科学委员会在其2013年发布的《弹性军事系统与高级网络威胁》报告中指出，为应对高级别的网络威胁，美国将不惜动用网络力量、常规力量甚至核力量来维护安全利益。① 而俄罗斯对大规模网络攻击的立场同样是会选择任何战略武器进行回应。② 英国和法国也将严重的网络攻击等同于传统军事行动，并保留在极端情况下动用战略武器进行反击的权利。③ 跨域威慑似乎有些“疯狂”，但威慑战略的成功恰恰需要那么一点非理性成分。因为如果进攻方认为受害方将始终保持理性，不会愿意冒冲突升级的风险，那么受害方的威慑策略可能就失败了。④

此外，拒止威慑的效用及其必要性也不容忽视，毕竟报复威慑并非万灵药。就像打击犯罪一样，尽管强化了多种手段，但犯罪分子依然层出不穷，很难确保哪些威慑必然是有效的。报复威慑也不能被指望用来应对更加广泛的网络黑客、网络牟利、网络抗争等行为。尽管网络大国之间在网络威慑的框架下能基本维持战略稳定，但仍然可能由于缺乏透明度而导致战略互疑、军备竞赛和误判。而如果对手真的孤注一掷，不顾后果也要发起攻击，那么无论如何强调报复都无济于事。所以万一报复失灵，良好的防御总是可以尽量将损失减少到最小。在网络空间中，拒止和报复作为威慑战略的两种形态是相互补充、辩证统一的关系。攻防双方的拒止和报复存在互动关系。对手的防御越弱，己方报复的可信度也就越高。所以高度可信的威慑战略需要同时兼顾拒止和报复能力的建设。由于大部分网络攻击都是利用系

① Defense Science Board, “Resilient Military Systems and the Advanced Cyber Threat,” January 2013, pp.7-8, pp.85-86, http://www.dtic.mil/dtic/tr/fulltext/u2/a569975.pdf, 访问时间: 2017年12月2日。

② Stephen Blank, “Can Information Warfare Be Deterred?” *Defense Analysis*, Vol.17, No.2, 2001, pp.121-138; Matthew Campbell, “‘Logic Bomb’ Arms Race Panics Russians,” *The Sunday Times*, November 29, 1998; Timothy L. Thomas, “The Russian View of Information War,” in Michael H. Critcher, ed., *The Russian Armed Forces at the Dawn of the Millennium*, Center for Strategic Leadership, U.S. Army War College, 2000, pp.335-360.

③ Cabinet Office, National Security and Intelligence, HM Treasury, and The Rt Hon Philip Hammond MP, “National Cyber Security Strategy 2016 to 2021,” November 1, 2016, https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021, 访问时间: 2017年12月20日; Ministry of Foreign Affairs and International Development, France, “France and cyber security,” December 2014, http://www.diplomatie.gouv.fr/en/french-foreign-policy/defence-security/cyber-security/, 访问时间: 2017年12月20日。

④ Patrick M. Morgan, “Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm,” p.61.

统漏洞发起的，所遭受的网络攻击的严重程度也就取决于自身的能力建设。[①] 网络威慑与核威慑的一大区别就在于网络防御可行而且必要。[②] 报复威慑可以减少网络防御的资金投入，反过来网络防御也可以提升报复威慑的可信度。网络防御能力越强，报复威慑被考验的机会就越少。优秀的归因能力显然是网络防御的重点之一。尽管不应将其绝对化，但归因能力显然是越强越好。而即便遭受了网络攻击，良好的防御使得普通攻击基本无效，同时又确保了实施反击的可能性，进一步强化了报复威慑的可信度。[③] 美国《国防科学委员会网络威慑专题小组最终报告》明确指出，网络威慑需要结合报复能力和网络弹性，包括对网络攻击的归因能力、关键基础设施的恢复能力以及其他重要的网络安全创新技术。[④] 人们可能无法清楚地区分对手没有发动攻击究竟是因为担心被报复还是因为防御抵消了攻击的效果。这就像学界至今无法明确界定威慑究竟何时有效、何时失效一样，但至少战争在总体上被避免了。

在上述网络威慑的框架下，根据国家对网络的依赖程度和常规军事实力大致可以划分出四类国家：依赖网络且拥有强大的常规军事实力（A 类）；依赖网络但常规军事实力较弱（B 类）；不依赖网络但拥有较强的常规军事实力（C 类）；不依赖网络且常规军事实力较弱（D 类）。其中，国家对网络的依赖程度是一个重要的指标，可以参考国际电信联盟（ITU）发布的《衡量全球信息社会发展水平报告》（Measuring the Information Society）。[⑤] 网络攻击的程度越严重，所能够摧毁的社会财富数量越大，但最终趋向于一个定值。这个值的大小是由不同国家对网络不同的依赖程度所决定的（如图 4）。

依赖网络的国家一般对于网络攻击极为敏感，而不依赖网络的国家也很有可能不信任网络的效用。在上述四类国家中，D 类国家一般不具备较强的网络攻防能力，同时由于军事实力有限，也难以想象会向大国发起网络攻击。因此，这里主要探讨 A 类

① 分布式拒绝服务攻击是个例外，但实际上像军队、电厂等基本上都在很少与外界交互的情况下可以运转，所以分布式拒绝攻击只是网络攻击危害中的次要因素。参见马丁·利比基《兰德报告：美国如何打赢网络战争》，第 4 页。

② Patrick M. Morgan, "Applicability of Traditional Deterrence Concepts and Theory to the Cyber Realm," pp.75-76.

③ 马丁·利比基《兰德报告：美国如何打赢网络战争》，第 69—70 页。

④ Defense Science Board, "Task Force on Cyber Deterrence," http://www.dtic.mil/dtic/tr/fulltext/u2/1028516.pdf，访问时间：2017 年 12 月 22 日。

⑤ International Telecommunication Union, "Measuring the Information Society Report 2015," http://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2015/MISR2015-w5.pdf，访问时间：2017 年 12 月 22 日。

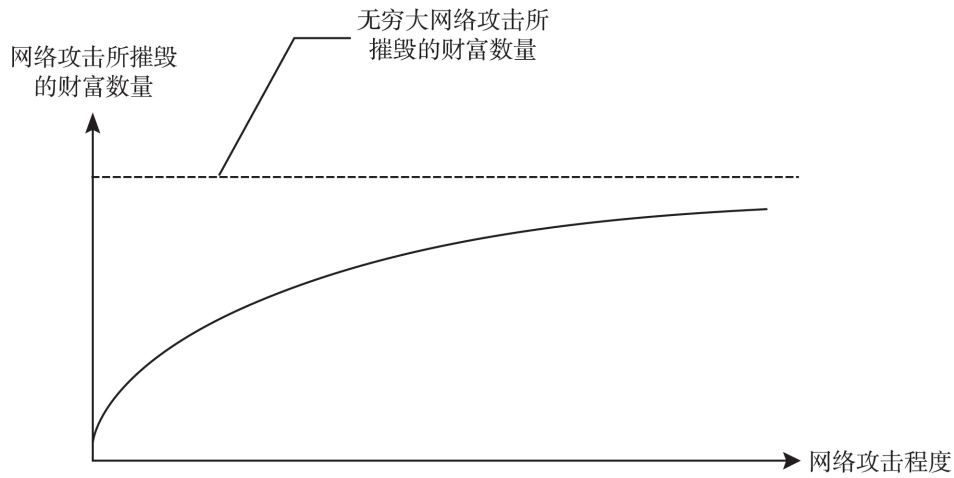

图 4　网络攻击程度与所摧毁财富数量的关系示意图

资料来源: 笔者自制。

国家之间以及 A 类国家与 B 类和 C 类国家可能发生网络冲突的情景。A 类国家与 B 类国家之间的网络冲突最为接近的案例是俄罗斯被指对爱沙尼亚发动网络攻击。由于攻击已经发动,所以在这个案例中威慑其实是失效的。但俄罗斯所展示出的强大实力为其今后威慑其他 B 类国家增强了可信度。由于 B 类国家依赖于网络,所以只要对手具备强大的网络进攻能力,那么后果往往极其严重。再加上在常规军事冲突中处于下风,所以 B 类国家在与 A 类国家的对抗中居于劣势。反过来 A 类国家对于 B 类国家的网络威慑也就有效。A 类国家与 C 类国家间的网络冲突最为相似的案例是朝鲜被指入侵索尼影业而遭到美国实施“断网”打击。C 类国家虽然不依赖于网络,但可能拥有较强的网络进攻能力,且军事实力较强。当 A 类国家遭到 C 类国家的网络攻击后,反制措施的选择余地其实有限。因为对手不依赖网络,所以网络反击的效果不大。由于对手军事实力较强,为了避免冲突升级(尤其在朝鲜的案例中要避免迫使对方运用战略武器) ,A 类国家必须控制反击的力度,将冲突升级的主导权掌握在自己手中,但为了确保威慑的可信度又必须采取明确的报复措施。因此发动网络反击既可以展示报复的决心,又不会因为造成严重后果而导致冲突升级。如果对手不为所动、持续攻击,那么 A 类国家仍然可以选择其他更加严厉的手段进行报复。因为有了上一轮的铺垫,此时宣示进一步报复的可信度也更高。而只要展示出强大的网络实力、制定灵活的应对策略并宣示坚定的威慑意图,A 类国家间爆发大规模网络冲突的可能性就会较低。根据网络攻防平衡的关系,一般性的网络攻击都无法对双方产生较大的

影响，而攻击越频繁则越有可能强化对手且暴露自己，因此双方都会保持审慎和克制。由于双方都依赖网络，发动大规模网络攻击可能获得暂时的优势，但考虑到双方的军事实力对比大致处于平衡状态，为了避免对手大规模报复所引发的灾难性后果，大规模网络攻击仍然会被慑止。

五 结论

整体而言，尽管相关问题正处于高速发展和变化的过程中，但决策的关键还是要落实到人的思考和判断上。只要各国逐步形成准确的关于网络空间的共有知识，并采取恰当的网络威慑战略，网络技术革命就不会危及大国战略稳定或颠覆国际秩序。共有知识的内涵包括对网络攻防、归因和其他网络活动的技术特征及其政治后果的共同理解和预期。这种共同的理解和预期需要以客观分析为前提，而夸大的威胁或是错误运用理论则将对其产生负面影响，能否形成共同的理解和预期将最终导致完全不同的国家行为模式。例如，信奉网络进攻占优思想的国家会倾向于先发制人，试图通过速战速决的方式赢得胜利，并导致网络战的频率增加。然而，网络攻防之间存在着辩证统一的关系。要确保一次成功且高效的网络攻击需要细致周密的前期准备。而由于攻击对象的系统可能十分复杂，所以准备工作往往耗时费力，并非如想象中那样轻而易举。由于对手可能很快修复漏洞并恢复系统，要持续进行有效攻击就变得更加困难。对于因为难以归因而导致网络攻击频繁的担忧实际上忽略了任何战争都带有明确的政治目的，而隐藏身份是无法表达意图或迫使对手改变行为的。低烈度的网络安全事件可能十分普遍，但网络战基本不会是隐蔽的单方面行为，而是在双方甚至多方战略互动和政治博弈的大框架下进行。以突然袭击方式发起网络攻击的构想经常被誉为拥有“四两拨千斤”的神奇效果，而实际上效果有限，门槛较高，后果难以控制。这不仅是指传统军事行动中所面临的信息不对称问题，更主要的原因是网络空间的快速变化。目标系统可能已经修复漏洞或更换硬件、软件，从而导致攻击无效。实施攻击也可能造成未知的技术、政治和法律层面的连锁反应，甚至反噬自己。这种不确定性使得单纯的网络攻击难以产生致命的效果，也就无法从根本上改变国家间的力量对比。因此，如果能够在网络攻防平衡等关键问题上形成准确的共有知识，将可避免各国发动投机性的冒险行为或在受到攻击而归因能力有限时采取过度反应。

本文认为，如果能够进行有效的认知建构，各国将对于不同网络攻击可能造成的

后果形成一致的预期，即较易实施的低技术水平的网络攻击一般情况下难以造成物理毁伤，频繁使用不仅暴露自己而且会强化对手；大规模的网络攻击成本和风险极高，也未必能够改变国家间的力量对比，需要审慎评估。这种共有知识通过不断的磋商和交流长期积累，最终形成一种信息共享和约束机制。其目的是规范国家行为，避免归因能力有限时的过度反应以及投机性的冒险行动，进而确保在网络空间构建最基本的战略稳定。

对于网络攻防平衡的认识很大程度上化解了传统威慑战略，尤其是报复型威慑在网络空间中所面临的障碍。当面临大规模网络攻击时，归因问题往往不言自明，大幅度压缩了基于一厢情愿思维模式或者错误信息实施投机性先发制人攻击的空间，而由于网络攻防平衡的态势，网络攻击的自我遏制消除了划线困境，通过适度的“炫耀武力”并结合“跨域威慑”的报复手段可以提升网络威慑的可信度。在网络威慑的框架下，报复和拒止作为威慑的两种形式存在辩证统一的关系。由于报复型威慑难以排除意外战争或是非理性行为的风险，良好的防御依然可以作为必要的补充来减小损失。而强大的网络防御能力本身又可以提升报复的可信度，从而慑止潜在对手。由于冲突升级的结果仍然受制于国际关系中的传统因素，即便发生网络战，也往往是在大国攻击小国的过程中发挥作用。小国由于实力有限，而网络并不能彻底改变力量对比，所以以弱胜强的可能性很小。网络技术的发展进一步拉大了国家间力量对比的不平衡。目前的网络战案例也都支持这一判断。因此，大国对大国以及大国对小国能够确立网络威慑，尤其当对方也依赖于网络时。此外，可靠的网络威慑也取决于国家自身能力的建设。各国可以通过政策宣示自身的网络核心利益，明确不同程度的网络攻击可能面临的反制措施，并围绕这些问题形成长期的沟通协调机制，进而维护长期战略稳定。

（截稿：2017 年 12 月　责任编辑：王鸣鸣）

nition or illusory recognition, but not really inter-subjective recognition.
【Key Words】terrorist group, terrorism, struggle for recognition, collective identity
【Author】Zeng Xianghong, Professor of the School of Management and Institute for Central Asian Studies, Lanzhou University.

Offense-Defense Balance in Cyberspace and a Proposed Model of Cyber Deterrence

【Abstract】Cyberspace has become a new area of strategic game between great powers. The militarization of cyberspace is an objective trend that is difficult to reverse. At present, there is not enough discussion on cyber offense and defense, cyber deterrence and its impact on the strategic stability between major powers. Some experts argue that attribution, line-drawing, symmetrical retaliation and other technical difficulties make cyber deterrence hard to achieve. Furthermore, the perception of cyber offense dominance will break the strategic stability, cause frequent cyberwars, and even lead to the escalation of conflicts. However, such kind of skepticism and pessimism actually blurs the line between different levels of cybersecurity incidents and fails to understand the subtle balance between offense and defense in cyberspace. By differentiating specific cyber offense and defense techniques and combining with empirical analysis of major cybersecurity incidents, it is not difficult to find out that large-scale cyberattacks face many uncertainties and the attribution problem is not unavoidable. As a result, the three questions-the object, the threshold, and the measure of retaliation on cyber deterrence can basically be solved. With the realism concept and pragmatic understanding of offense-defense balance in cyberspace, it is feasible to achieve strategic stability in cyberspace through building active cyber deterrence. It should also become a major direction for the strategic interaction between great powers in cyberspace.
【Key Words】cyberwar, offense-defense balance, cyber deterrence, strategic stability
【Authors】Shen Yi, Director of Center for Global Cyberspace Governance Studies, Fudan University; Jiang Tianjiao, Ph.D. Candidate, School of International Relations and Public Affairs, Fudan University.