网络空间冲突的治理困境与路径选择*

丛培影　　黄日涵

【内容提要】 网络空间安全治理问题正日益引起国际社会的普遍关注；其中，网络空间冲突治理问题更是备受关注。与现实的物理空间冲突相比，网络空间冲突具有行为体多元化、进攻手段快速更新、冲突后果不可预知等新特点。这导致网络空间冲突治理面临认知分歧严重、规范难以有效管辖、威慑无效和“结构性难题”等现实挑战。因而，网络空间冲突治理需要转变治理理念，通过国家间务实合作，整合各方优势资源，构建网络空间全球治理机制，并培育合作、共享的治理文化。作为全球网络大国，中国一直以来都积极倡导建立多边、民主、透明的全球治理体系。同时中国将在创新治理理念，弥合数字鸿沟，开展双边、多边国际合作等方面，为构建网络空间国际规则和全球网络治理机制作出积极贡献。

【关键词】 网络空间　冲突　治理　困境　选择

【作者简介】 丛培影，中国青年政治学院青少年研究院助理研究员；黄日涵，华侨大学国际关系学院助理研究员，中国与全球化智库研究员

【中图分类号】 D815

【文献标识码】 A

【文章编号】 1006-1568-(2016)01-0098-19

【DOI 编号】 10.13851/j.cnki.gjzw.201601006

* 本文系国家社科基金青年项目“世界政治 2.0 时代的新型大国关系研究”（13CGJ011）、国家社科基金重大项目“网络空间的国家安全战略研究”（11&ZD061）的阶段性成果。

随着网络信息技术在全球范围内的广泛应用和快速发展，网络与国家安全的关系日趋紧密且受到各国高度重视。在安全议题中，最引人关注的是网络空间冲突。网络空间被军事战略学家和未来学家称为“下一个战争空间”（next battlespace）。各国政府在网络空间中的首要目标是确保本国的核心利益不受损害，保障国民免受网络袭击的侵扰。但现实情况是绝大多数网络袭击并非由政府直接发动和实施，而是由非国家行为体直接策划操作。而且，发动网络袭击的成本低廉、行动隐蔽，且能引发严重后果。这也造成网络空间容易爆发冲突甚至网络战争（cyber warfare）。一旦网络空间发生冲突或战争，其规模和影响范围将难以估量。网络空间冲突也可能导致国家间在现实世界中的直接敌对与冲突。此外，由于缺乏必要的国际法律管辖与规范，网络空间冲突治理也面临着严峻挑战。有效控制网络空间冲突的烈度，制定网络空间国家行为准则，将是国际社会探索网络空间冲突治理的新课题。

一、网络空间冲突的变化与挑战

网络空间冲突源于行为体对网络威胁的感知和由此作出的反应。网络威胁大致可分为两类：一类被称为网络袭击，是指蓄意破坏网络系统的行为；另一类被称为网络牟利（cyber exploitation），即利用网络基础设施来达到非法目的，但不会对网络系统本身造成伤害的行为。[①] 网络袭击针对的目标是国家和非国家行为体，包括主权国家、组织和个人，既可以破坏软硬件和计算机的其他方面，也可以通过非法入侵计算机操作系统，运用不正当的手段获取信息或实施远程控制。网络袭击可能引发网络冲突，而网络冲突又可能升级为网络战争。网络战争一般是指一个民族国家为渗入另一个国家的计算机或网络所进行的破坏和扰乱行为。[②] 网络战争可能严重危害国家的政

[①] Abraham D. Sofaer, David Clark, Whitfield Diffie, “Cyber Security and International Agreements,” in *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*, Washington, D.C.: The National Academies Press, 2010, pp. 179-180.

[②] Richard A. Clarke and Robert Knake, *Cyber War: The Next Threat to National Security and What to Do about It*, New York: Harper Collins, 2010, p. 10.

治、经济和社会安全与稳定，是网络冲突的最高形式。

网络信息技术所具备的即时性、便捷性、廉价性特质，使冲突和战争变得易于操作和实施。网络信息技术使传统的冲突与战争发生了颠覆性变革。只要有一台联网的计算机，少数人就可以实施网络攻击，发动一场没有硝烟的小规模战争。网络空间的武器开发成本极低，只要有一两台计算机，且能够实现网络连接，再配备几名高水平的黑客，就足以制造极具杀伤力的网络武器。[①] 因此，互联网对国家安全的影响都将是全面的、彻底的和前所未有的。网络信息技术源自通讯技术的不断创新与发展。即时通讯技术的出现和不断更新，提升了战场上的政治决策效率。网络信息技术对于武器技术的革新具有重要推动作用，尤其是在核武器时代，计算机技术使核武器更加精准、可靠和高速。冷战时期，美、苏两国十分重视发展信息处理技术。随着计算机技术的全面发展，美国率先提出了“信息战理念”（information warfare doctrine），也就是利用信息技术力量，在策略和手段方面超越对手。西方学者表示，目前国际社会最大的隐患不再是大规模杀伤性武器，而是大规模破坏性武器（weapons of mass disruption）。[②] 在技术突破之外，网络空间冲突与战争更深刻的变革体现在行为主体、攻击手段和冲突后果等方面。

（一）行为主体日益多元化

网络空间为非国家行为体提供了更加广阔的活动平台，使其可以超越领土和主权的限制，在现实和虚拟世界发挥更大的作用。传统的冲突与战争发生在不同群体之间，一般被实力强大的国家所垄断，而单独个体难于发动对群体的攻击。网络信息技术极度放大了相对弱小行为体的力量。借助于网络信息平台，小国可以向霸权国发起挑战，规模小的群体可以向实力强大的主权国家发动袭击，个人也可以发动对群体的攻击。美国一直以来都将朝鲜视为网络空间中的威胁。据美国福克斯新闻网透露，2010 年年初的报告显示，朝鲜已经培训了数千名顶级的计算机专业学生成为出色的“网络战士”（cyber

[①] 樊高月、赵力昌主编：《不流血的战争：网络攻防经典之战》，解放军出版社 2014 年版，第 117 页。

[②] Craig B. Greathouse, “Cyber War and Strategic Thought: Do the Classic Theorists Still Matter?” in Jan-Frederik Kremer and Benedikt Muller, eds, *Cyberspace and International Relations: Theory, Prospects and Challenges*, Verlag Berlin and Heidelberg: Spinger, 2014, p. 23.

warrior），其行动目标锁定为美国和韩国。[①] 近年来，恐怖主义也借助网络载体和信息工具获得了“新生”。基地组织利用互联网技术宣传其极端理念，并利用网络平台实施成员招募、在线培训、资金募集、远程指挥等活动。可以说，网络空间的隐蔽性和开放性特征加大了国际社会防范和打击恐怖主义的难度。[②] 2008 年，波兰一名 14 岁少年通过入侵并控制洛兹市（Lodz）的有轨电车系统，从而引发混乱，导致 4 辆电车脱轨，12 人受伤，所幸事故未造成人员死亡。[③] 对于日益多元化的网络袭击者，美国战略司令部司令凯文·希尔顿（Gen. Kevin P. Chilton）曾形象地认为，“我们的敌人范围，不仅包括令人厌烦的年轻黑客，也包括犯罪组织，还涉及国家行为体”。[④]

（二）攻击手段不断更新

互联网发展的初衷是便于信息的有效流动，实现资源共享、互联互通。开放的环境往往会给安全防御带来更多风险和挑战，网络空间中因而出现了“攻守不平衡”问题。这种结构上的不平衡会激发网络恶意攻击，从而降低对威慑和有效防御的信心。[⑤] 网络空间中的简单静态防御（static defenses），即被动防御，是指最多被强大的黑客视为一个新挑战或待解决的问题。[⑥] 技术娴熟的网络袭击者能够轻松找到网络漏洞并成功绕开安全防御软件。与传统的冲突相比，网络空间中的袭击者处于隐蔽处，并专门攻击目标的薄弱环节。在“攻方压倒守方”的背景下，网络进攻性武器变得十分普遍。一般的网络进攻武器，包括计算机病毒、恶意软件、逻辑炸弹（logic bomb）、拒

[①] Kelley Beaucar Vlahos, “Special Report: The Cyberwar Threat from North Korea,” Fox News, February 14, 2014, http://www.foxnews.com/tech/2014/02/14/cyberwar-experts-question-north-korea-cyber-capabilities.

[②] 丛培影、黄日涵：《网络恐怖主义对国家安全的新挑战》，载《江南社会学院学报》2012 年第 2 期，第 2 页。

[③] John Leyden, “Polish Teen Derails Tram after Hacking Train Network,” *The Register*, January 11, 2008, http://www.theregister.co.uk/2008/01/11/tram_hack/.

[④] Kelvin P. Chilton, “Cyberspace Leadership Towards New Culture, Conduct and Capabilities,” *Air & Space Power Journal*, Fall 2009, p. 7.

[⑤] Kenneth Lieberthal and Peter W. Singer, “Cybersecurity and U.S.-China Relations,” Brookings Institution, February 23, 2012, http://www.brookings.edu/~/media/research/files/papers/2012/2/23%20cybersecurity%20china%20us%20singer%20lieberthal/0223_cybersecurity_china_us_lieberthal_singer_pdf_english.pdf.

[⑥] Erik M. Mudrinich, “Cyber 3.0: The Department of Defense Strategy for Operating in Cyberspace and Attribution Problem,” *The Air Force Law Review*, Vol. 68, p. 181.

绝式服务（denial of service）等。低端网络武器的目标只是简单的窃取信息、获取密码、修改程序等，一般不会产生重大危害。相比较而言，高端网络武器能够造成数据和关键设施的中断或严重受损。一系列的网络攻击能够演变为重大突发事件，在一段时期内中断关键服务，包括破坏军事指挥或信息系统，关闭电力供应或石油管道，停止金融服务等。2008 年，美国国防部储存加密军事信息的电脑网络就曾感染恶意代码。恶意代码在未被察觉的情况下扩散到加密和未加密文件系统。虽然被及时发现，但美国军方对此十分恐慌，认为此类事件可能会使其军事机密文件被上传给国外情报机构，甚至是未知的敌对势力，后果将不堪设想。[①]

复杂高端的恶意代码具有很强的自我伪装能力，很难被发现，往往是在已经造成严重伤害后才会被发现。2010 年，伊朗核设施受到“震网病毒”（Stuxnet）的攻击，使伊朗纳坦兹铀浓缩工厂的 1 000 多台 IR-1 型离心机由于非正常运转并遭到破坏而不得不更换。事实表明，“震网病毒”的攻击目标非常精确或单一，即德国西门子公司控制系统（SIMATIC WinCC）。这是一款数据采集与监视控制（SCADA）系统，被伊朗广泛使用于国防基础工业设施。“震网病毒”在入侵一台电脑后，就会自动寻找西门子软件，确认找到软件后，这种病毒会在无人察觉的状态下控制工业用的电脑系统，并控制电脑软件对工厂其他电脑发出既定指令。网络安全专家认为，“震网病毒”是第一个以物理世界基础设施为攻击目标的“精确制导”蠕虫病毒。[②] 作为第一个披露“震网病毒”的德国著名网络安全问题专家，拉尔夫·朗纳（Ralph Langner）经过系统分析，认为“震网病毒”的结构比想象中的还要复杂，包含两个不同的“数字弹头”（digital warhead），分别针对不同的进攻目标，铀浓缩设施和布什尔核电站的外部涡轮机。他认为第二个弹头的威力相当于对布什尔核电站进行一次精确的空中打击。[③] 美国信息安全问题专

[①] William J. Lynn, “Defending a New Domain: The Pentagon’s Cyber Strategy,” *Foreign Affairs*, September/October 2010, Vol. 89, No. 5, p. 97.

[②] 樊高月、赵力昌主编：《不流血的战争：网络攻防经典之战》，第 123 页。

[③] Jerusalem Post, “Stuxnet Specifically Targeted Iranian Nuclear Program,” *The Jerusalem Post*, November 20, 2010, http://www.jpost.com/Iranian-Threat/News/Stuxnet-specifically-targeted-Iranian-nuclear-program.

家凯文·克莱曼（Kevin Coleman）2010 年在美国国防科技网上发表的文章认为，网络袭击的数量将会急剧升级。为支持这一论断，他提到 2009 年恶意软件的数量达到了此前 20 年来的最高水平，多份报告显示超过 2 500 万个恶意软件被确认，而且这种增长趋势还将继续。[①]

通过以上事例，不难看出网络空间中的进攻武器技术含量高且具有极强的针对性。这样的武器比常规武器更隐蔽、更精准、更具进攻性和破坏性。与此同时，网络进攻性武器不能重复使用，必须不断升级换代。美国著名智库兰德公司的数字战专家马丁·利比奇（Matin Libici）认为，一旦有人了解了网络战武器的工作原理，它就不再是一种武器了。最好的武器是敌人所不知，但自己却已拥有的。[②]

（三）冲突后果不可预知

传统冲突中的对手是清晰可见的，冲突的结果也是可以预测的。在网络空间的冲突中，进攻武器一旦发挥威力，所造成的破坏规模和影响力一般都会不断地复制和散播，很难像传统冲突那样能够得到有效控制。更为严重的是，网络袭击会给社会带来严重恐慌，其后果比传统战争更为严重。现代社会中的各类基础设施都是由计算机和互联网系统控制，一旦网络袭击波及水、电、金融控制系统，带来的损失将是无法估量的，甚至可能造成严重的社会动荡。美国学者设想了网络攻击可能引发的严重后果：没有航空控制系统或者机场安监系统，没有电子管控的铁路交通，没有依赖电子计算机日夜投递的包裹或邮件，没有雇主通过支付软件支付工人工资的电子支票，没有电子取款记录，没有自动取款机，医院或者健康中心没有可信赖的数字记录，没有电力导致没有灯光，没有热力，没有加油系统或者燃料、汽油，没有交通信号灯，没有电话，没有网络服务，没有警察有效的治安管理，这一系列问题将使美国社会陷入短时瘫痪。[③] 据美国中央情报局透露的发生在 2007

[①] Paul A. Matus, “Strategic Impact of Cyber Warfare Rules for the United States,” *Homeland Security Digital Library*, March 23, 2010, http://www.handle.dtic.mil/100.2/ADA522001.

[②]《源代码之战》，载《国际金融报》2011 年 8 月 1 日，第 4 版，http://paper.people.com.cn/gjjrb/html/2011-08/01/content_885812.htm?div=-1。

[③] Michael J. Glennon, “State-level Cybersecurity,” *Policy Review*, February/March, 2012, p. 85.

年针对美国公用电力网的多起网络袭击事件表明，由于担心会造成严重的社会恐慌，电力公司的负责人甚至不愿谈及这些事件的风险。

此外，网络空间的开放性特征使网络袭击一旦发生，其影响范围将具有扩散性。2013 年 4 月，黑客窃取了美联社的推特账号，发布了美国总统奥巴马在白宫的一次爆炸中受伤的虚假消息。几分钟后，美联社官方使用另一个推特账号声明之前的账户已被盗。白宫发言人也通过广播澄清奥巴马总统没有受伤。但已有很多人看到了被盗推特账号发布的消息，该事件导致道琼斯工业指数和 S&P500 指数双双下挫，之后两个交易指数又快速反弹。据称美联社的推特账号有 200 万受众，其发布的即时消息影响力十分巨大。[①] 这一事件也给美国政府敲响了警钟，一起简单的账户被盗事件很可能引发一场金融恐慌，从而严重扰乱社会秩序。

网络冲突治理的上述新特点产生了严重的后果。行为体的多样性使人们很难在短时间内转变观念，克服认知差异与分歧；网络攻击手段的不断革新使国际法律制度和威慑很难发挥作用；而后果的难以预测则加重了国家间的相互猜疑。这些因素将严重阻碍网络空间冲突治理机制的形成并发挥作用。

二、网络空间冲突治理机制的困境

网络空间冲突与传统意义上的国际冲突有很大差异。现行全球治理机制的主要行为体是主权国家，它们在对传统武装冲突理解和认知的基础上提出一系列管控规则。但在网络空间中，对非国家行为体的行为进行有效规范在法律和道德方面是一个空白。而“结构性困境”等现实问题也加剧了网络空间冲突治理的难度。

（一）认知分歧阻碍有效治理

当前，各国对网络安全核心概念的理解以及对网络安全事件的归因（attribution）和认定都存在深刻分歧。例如，美、英、日、德、法和欧盟等

[①] “Hacked AP Twitter Account Sends Dow Jones Down,” *Southern California Public Radio*, April 24, 2013, http://www.scpr.org/programs/airtalk/2013/04/23/31465/hacked-ap-twitter-account-sends-dow-jones-down/.

都制定了网络安全战略，通过对比可以发现，各方对“网络空间”、“网络安全”、“网络战争”等核心概念的界定存在明显差别。[①] 在网络空间中，如何确定一些行为已经违反了国际法基本准则，并可以实施武力打击？个人和组织是否可以成为国家发动网络进攻的目标？如何界定网络空间的国家主权？对于这些问题，现行的国际法律体系没有现成答案。联合国作为维护国际和平与安全的具有广泛代表性的国际组织，自身也存在局限性，突出表现在《联合国宪章》的制定远早于网络信息时代的到来，因此并没有考虑到网络袭击的问题。根据现行的国际法准则很难将网络袭击定义为使用武力。在 2008 年格俄战争前的三周时间中，未知行为体利用商业 IP 地址在多个国家发动分散拒绝式服务袭击格鲁吉亚总统网站。外界认为，相关恶意软件（被命名为 MachBo）是在俄罗斯编写并被俄罗斯黑客所普遍使用，尽管没有确切证明表明是俄罗斯政府策划并实施了网络袭击。现行国际法律规范面临的另一困境是网络犯罪与网络战之间的模糊界限。现实的认知分歧突出表现为，受攻击的国家认为网络攻击行为是一种网络犯罪，而鼓励实施或在背后提供支持的国家则认为网络攻击行为是为维护本国利益的网络战。由此可见，缺少统一的认知标准和行动准则使网络空间冲突治理难于开展。

一般而言，网络空间行为可以分为三类，一是合法的（公认的是合法的）；二是犯罪（非法的，现行法律规范认定其为犯罪）；三是不合法的（被国家和非国家行为体认定为恶意的，但现行法律框架却没有明确界定的）。可以确定的是，网络袭击首先应该属于国内法管辖范畴。如果袭击者触犯了国内法律，所属国政府必然会实施管辖。如果袭击者对他国目标实施攻击，同时目标国与所在国的关系并不友好，就存在一个现实认定的问题。尤其是对于情报收集（intelligence gathering）、中断通信（disruption of communications）或者是对敌军发布错误指令等网络行为，就很容易出现实施者由于受到所在国的偏袒，不被认定为是网络袭击，从而不会受到应有的惩罚。[②]

[①] 蒋丽、张晓兰、徐飞彪：《国际网络安全合作的困境与出路》，载《现代国际关系》2013 年第 9 期，第 56 页。

[②] Yoram Dinstein, “Cyber War and International Law: Concluding Remarks at the 2012 Naval War College International Law Conference,” *International Law Studies,* Vol. 89, 2013, p. 284.

（二）国际法律规范难以有效管辖

现行国际法律体系和治理机制确实存在诸多问题。第一，存在将现行的关于武装冲突的规则应用到网络空间的问题；第二，现行国际规则能否适用于网络空间治理，多数国际规则聚焦国家间冲突，而网络空间中的非常规性冲突却越来越多；第三，缺少法律专家；第四，现行规则关注聚焦如何限制网络战，但对物理和附带性伤害等潜在问题关注较少。[①] 这些问题使现行的国际法律制度既无法对网络冲突行为实施有效管控，更无法为民用基础设施和普通平民提供法律保护。

“战争与武装冲突法”（简称“武装冲突法”）起源于 19 世纪中叶，是规范暴力与冲突的人道主义规范。武装冲突法专门适用于国家之间的正规军队的冲突。各国于 1864 年对《日内瓦公约》达成共识，于 1868 年在圣彼得堡正式签订。但武装冲突法、《联合国宪章》中的政府参战的法律制约和战时战争行为的约束都不适用于网络空间。而且现行法律规范都没有明确界定“战争行为”（war of act）的概念。一般意义上，战争是指国家间相互使用武力的法律后果。武装冲突法建立在使用武力和侵略概念上。在网络空间中，对于网络袭击是否等同于使用武力而应受到武装冲突法的管辖存在较大争议。一方面，虽然没有明确界定，但通常认为，网络袭击是在网络空间中带有敌意（hostile）的使用网络和信息技术来达到一定目的或者效果的行为；另一方面，网络袭击能否被称为冲突或战争，仍需国际社会的普遍认定。[②]

现行国际法律规范对于管控网络空间冲突存在空白区。在现行国际法律框架下，治理冲突的国际法律准则是武装冲突法，其主要的法律渊源是国际条约和国际习惯。它是在战争和武装冲突中调整交战各方之间以及交战各方同中立国之间的关系以及交战行为的有约束力的原则、规则和规章、制度的总和。[③] 武装冲突法约束的主体是国家，而不涉及对个人和国际组织实施管辖权的问题。另外，在网络袭击中，如何有效区分军事与非军事目标也是个

[①] Duncan B. Hollis, “Why States Need an International Law for Information Operations,” *Lewis & Clark Law Review*, Vol. 11, No. 4, 2007, pp. 1023-1024.

[②] Scott W. Beidleman, “Defining and Deterring Cyber War,” *Military Technology*, Vol. 11, 2011, p. 60.

[③] 顾德欣编：《战争法概论》，国防大学出版社 1991 年版，第 9 页。

现实挑战。在传统的战争领域，军事与非军事目标界限分明，就像绿色坦克运载士兵，黄色汽车运载学生一样。但在没有明确界限的网络空间中，两者的界限是模糊的。界限的模糊化将会造成进攻目标的偏向与转移，如对一国军事设施的打击很可能转移到民用基础设施目标上。在网络战争中，对于指挥者来说，很难区分哪些网络有军事战略目的，哪些目标是民用的。更棘手的问题是，很难确定袭击者的远距离攻击。即使能确定实施袭击者和袭击本身的存在，仍很难确定袭击者身份。

网络空间冲突还存在对传统战争中自卫权的适用问题。如果针对一个国家的网络袭击已经发生，按照《联合国宪章》的规定，受到攻击的国家拥有自卫权。但如何确定实施主体、判定网络袭击是否为对国家的攻击、界定攻击的程度等，都没有统一的标准。虽然现行国际法律制度明确规定，常规战争不能使用大规模杀伤性武器，但如果从恶意代码和恶意软件可能产生的破坏程度看，它们几乎等同于使用大规模杀伤性武器。如果这一假设成立，将对上述原则构成严重挑战。而网络军队如果在公用网站上嵌入恶意代码，而感染代码的非军事系统要比军事系统多，这应该被认为是违反了武器滥用原则。网络空间中是否也存在“网络大规模杀伤性武器”，对这些能够造成严重后果的武器，国际社会还没有达成禁止使用、共同打击的共识。另外，21世纪网络信息技术的发展使得士兵与他们的战争行为相分离。与战争行为分离得越彻底，也就越难保留武装冲突法中暗含的人道主义精神。同时，网络空间的开放性，使得公共与私人、政府与民间网络相互渗透、相互重叠。这将造成网络袭击后果的连带性，并可能引发物理性的损失与伤害。

（三）网络威慑失去效用

网络空间国际法律制度尚不健全已是一个既存事实，那么网络威慑战略是否可以有效实施并达到预期目的呢？威慑战略讲求实力与意志力的较量。威慑是指一方的实力足够强，以使其对手不敢发动袭击，否则将付出重大代价。威慑的前提是可能性和可信性：可能性意味着一方拥有发动报复与还击的绝对能力，可信性意味着在关键时刻一方决定对其对手实施必要打击。要实现影响对手决策的目的，就需要让对手明确地了解和感知到威慑实施方的

绝对实力和报复决心。现实中，在网络空间中运用威慑战略存在严重局限：

首先，威慑理论一般应用于两个强大的对手之间，威慑之所以能够有效是假定对方是理性的，无法承受发动攻击而产生的代价。但在网络空间中，发动袭击的实体与受攻击的对象之间可能实力严重不对称，即使实施有效的报复，也无法达到威慑目的。

其次，报复手段的非对称性，会扰乱现行国际规则。假若网络攻击者只发动了一般的分散性拒绝式攻击、仅导致受攻击国网络系统瘫痪，如果受攻击国使用常规军力与核军力加以回击，将会造成大量的经济损失和人员伤亡，这将背离国际法中的“相称原则”，其回击行为将因此丧失法律正当性。

最后，网络攻击是瞬时、一次性的，成功或失败只是在转瞬之间，攻击实施成功，就会造成伤害，受害者在遭受攻击后再实施报复，威慑将彻底丧失意义，因为伤害已经产生。在网络环境中，发动网络袭击的一方通常会通过“僵尸电脑”（被侵入后受到劫持的电脑）间接发动袭击，这就对受害国确定袭击者增加了很大难度。此外，确定袭击者身份的过程需要花费很长时间，待确认无误后，损失已经产生且无法挽回。在这样的条件下再实施报复行动，将会挑战国际法规定的“自卫原则”，因为《联合国宪章》第 51 条明确规定“自卫”的前提是正在遭受武力攻击的情况下才能采取行动。更具挑战性的问题是，如果袭击者被确定为是一个组织或个人，各种国际法准则将无法发挥作用。美国国防部前副部长威廉·林恩（William Lynn）也提到了网络威慑的难度，“威慑可信的前提条件是对于敌手身份确认无疑，但是在网络空间几乎没有这样的案例”。[①]

（四）“结构性难题”威胁国际合作

与现实世界一样，网络空间也处于无政府状态。在这种状态下，不存在绝对的权威，因而网络空间的国家间关系面临着“结构性难题”。这突出表现为两方面：

一是网络发达国家和新兴网络大国之间的竞争关系，这具体表现在网络安全议题上的两大阵营的“不同声音”。第一阵营是以美国为首的西方国家

[①] William Lynn, “Cyber Security,” Speech at the Center for Strategic and International Studies, June 15, 2009.

集团，它们都出台了相应的国家网络安全战略，并提出反映西方国家价值观的合作方式和治理理念。2014 年 3 月，美国表示与欧盟加强在与网络相关事务上的双边与多边协调与合作。美国明确表示，美欧合作建立在共有价值、共同利益，多利益攸关方（multi-stakeholders）治理理念，网络自由和保护网络空间人权的基础之上。[①] 2015 年年初，美国和英国表示要在保护关键基础设施、加强网络防御、支持网络学术研究等方面开展务实合作。[②] 同年 6 月，美国和日本就提升网络威慑而加强信息和情报共享达成协议。[③] 不难发现，以美国为首的第一阵营更加强调网络空间中自由、民主的价值理念和加强自身的网络威慑能力。第二阵营是中国、俄罗斯等新兴国家集团。“棱镜门事件”发生后，中、俄等国十分关注维护网络国家主权问题，呼吁国际社会关注美国以网络空间开放、自由为名、实际侵犯别国主权的行径。2014 年在巴西召开的金砖国家峰会上，俄罗斯建议加强金砖国家的网络安全合作。[④] 以俄罗斯和中国为代表的金砖国家认为，“维基解密”和“棱镜门事件”表明，美国等西方国家在网络安全问题上推行双重标准：一方面倡导所谓的网络空间绝对自由，另一方面又利用网络窃取别国信息。两大阵营中一方主张“网络自由至上”，另一方主张“网络主权至上”，双方意见分歧明显且难以消除。

二是发达国家与发展中国家的不平等关系。发达国家因先期发展优势，已在网络信息技术方面拥有了主动权；而广大发展中国家因历史、经济发展和技术条件等因素的限制，网络信息技术长期处于落后地位。国际电信联盟与其他相关机构的统计数据显示，截至 2011 年，全球在线网民人数已达到 23 亿，发展中国家的互联网渗透率约为 25%，发达国家的互联网渗透达到

[①] “Fact Sheet: U.S.-EU Cyber Cooperation,” The White House Office of the Press Secretary, March 26, 2014, https://www.whitehouse.gov/the-press-office/2014/03/26/fact-sheet-us-eu-cyber-cooperation.

[②] “Fact Sheet: U.S.-United Kingdom Cybersecurity Cooperation,” The White House Office of the Press Secretary, January 16, 2015, https://www.whitehouse.gov/the-press-office/2015/01/16/fact-sheet-us-united-kingdom-cybersecurity-cooperation.

[③] Franz-Stefan Gady, “Japan and the United States to Deepen Cybersecurity Cooperation,” *The Diplomat*, June 2, 2015, http://thediplomat.com/2015/06/japan-and-the-united-states-to-deepen-cybersecurity-cooperation.

[④]“China, Russia to Sign Information Security Pact: Report,” *The Brics Post*, October 21, 2014, http://thebricspost.com/china-russia-to-sign-information-security-pact-report/#.Vg4sYi-hdMs.

70%，欧洲互联网用户人均带宽相当于非洲人均带宽的 25 倍。[①] 地位上的不平等，将使广大发展中国家长期处于边缘和被动地位。虽然美国等西方国家提出在网络安全议题上向广大发展中国家提供必要的援助，但由于它们在实施援助的同时还附带宣扬西方价值理念，实际上是对广大发展中国家进行“价值观输出”。广大发展中国家十分担心与美国等西方国家形成网络安全技术层面的“依附关系”，网络空间冲突治理的南北合作也难于实现。

三、网络空间冲突治理机制的路径探索

战争已进入信息化时代，应该对现行国际法进行必要的改进和升级。多元的行为体、进攻技术的不断升级以及后果的不确定性，都呼唤网络空间冲突的全球治理。人们意识到网络犯罪、网络黑客、网络恐怖主义这些问题已经成为全球性问题，仅靠单个国家力量无法解决。因而，网络安全问题不仅仅是个别国家的国内安全问题，必须开展长期、广泛和深入的国际合作。与此同时，现行国际法律规范亟待更新完善。对于治理国际冲突的国际法律准则而言，应增加网络空间冲突的防范与管控条例。同时，网络空间合作需要培育和平与合作、发展与共赢的治理理念。只有治理理念深入人心，国际网络空间冲突治理行动才会受到关注，也才能在国际社会被广泛认可。

（一）全球治理意识的转变

虽然存在爱沙尼亚、格鲁吉亚网络遭袭和“震网病毒”对伊朗核设施造成严重破坏等典型案例，但到目前为止尚未发生大规模国家间网络冲突。尽管如此，人们仍高度担忧网络空间冲突，迫切需要转变相应的治理意识。

首先，参与网络空间冲突治理的最重要主体仍是主权国家。尽管个人和群体的作用被网络空间所放大，但其力量仍是有限的。个人与群体引发大规模网络冲突甚至战争的可能性仍微乎其微。因此，对网络冲突的聚焦仍应是国家。只有各国依据法律有效管理和规范自身及其国内组织、个人的行为，

[①] 复旦国务智库编：《增量改进——全球治理体系的改进和升级》，复旦全球治理报告 2014，复旦大学国际关系与公共事务学院，2014 年，http://www.sirpa.fudan.edu.cn/_upload/article/8e/7e/f72c6ae04f998c052fe4230493c5/b3ef8190-df38-40fb-829f-1a0c6f6f49a5.pdf，第 36 页。

国家间的合作才能够发挥作用。

其次，要协调和整合各方力量和资源。需要特别注意的是，网络空间本身超越国界，不能完全依托政府和国家力量。美欧等西方国家在网络防御中最值得借鉴的经验是充分整合民间资源，实现官方与民间的有效互动。应该意识到非国家行为体在网络安全领域中的重要作用，而非国家行为体也希望与政府合作降低网络风险。[①] 2010 年，美国国家安全局（National Security Agency, NSA）曾在谷歌公司遭受高持续性攻击（Advanced Persistent Threat, APT）情况下，为其提供情报和技术帮助。[②] 网络空间的基本元素是个人和社会团体，只有激发个人和社会组织的活力，提升其网络安全与合作意识，网络空间才会更加安全。在政府的积极推动下，整合技术人员、专家学者、社会团体、企业、政府等各方面资源，才能有效消除网络空间中的各类威胁。在某些情况下，对待网络空间问题也需要在网络中寻找答案。现实中，对于“白客”的利用就是重要的战略选择。2014 年 1 月，俄罗斯联邦委员会提出利用“白客”（无犯罪前科、能够发现系统漏洞且具有丰富经验的网络专家）的服务，以应对复杂多变的网络攻击。[③] 美国网络安全软件供应商的专家也强调，应关注“白客”群体，不能让其为黑暗势力所诱惑甚至利用。[④]

第三，要对网络行为实施分层级管控。国际社会面临的最大挑战是各国在很多网络空间治理问题上无法达成一致。从危害程度来看，从低到高的行为包括网络破坏（cyber vandalism）、网络间谍和网络犯罪、拒绝式服务、网络袭击和大规模网络攻击。前三类业已存在，而网络袭击和大规模网络攻击尚未发生，尽管它是最受关注、也是最可能引发网络冲突的行为。由于网络袭击和大规模网络攻击针对的都是关键性基础设施，可能引发受攻击国家严重的社会动荡。因此，这种行为几乎无法容忍，并会引发受害国的报复。

---

① Salma Shaheen: “Offense-Defense Balance in Cyber Warfare,” in Jan-Frederik Kremer and Benedikt Muller, eds., *Cyberspace and International Relations*, Berlin: Springer, 2014, p. 91.

② Jon R. Lindsay: “The Impact of China on Cybersecurity,” *International Security*, Vol. 39, No. 3, 2014, p. 27.

③ 《俄联邦委员会拟利用“白色黑客”应对网络攻击》，人民网，2014 年 1 月 26 日，http://world.people.com.cn/n/2014/0126/c157278-24226902.html。

④ “The Chinese Cyber Threat: Challenges and Solutions,” AEI, July 22, 2015, http://www.aei.org/events/the-chinese-cyber-threat-challenges-and-sollutions/.

对于前三类相对较轻的破坏行为，各方可通过协商合作予以解决；对于可能产生严重后果的网络袭击和大规模攻击，各国应通过协商，达成明确禁止此类行为的网络空间国际行为准则。

（二）培育合作理念

网络空间中的“攻方压倒守方”现实使网络空间威慑难以实现，这会从另一个方向鼓励网络入侵者，最终导致网络军备竞赛。从表面上看，进攻能够带来一定收益并产生安全感，但后果将是网络空间行为体间相互竞争、相互敌视的状态。因此，在互联、开放的网络空间中是不可能获得绝对安全的。

相反，如果防守方占优，各行为体会更倾向于合作。任何有威胁的入侵，都是在成功绕开防御措施的基础上进行的。因此，提升防御能力才能获得积极和持久的安全。这要求建立两类机制：一是早期预警机制，使受攻击的国家能够尽早发现并采取必要的防范措施。从“震网病毒”袭击案例中可以看到，病毒入侵必须绕开受害国的安全防火墙。如果采取了安全防御措施，“震网病毒”是无法实施破坏的。二是信息共享机制，各方相互协调与配合将有助于实现共同安全。这首先要求国家间实现信息共享，这可以增加彼此信任，有利于开展务实有效的合作，实现互利双赢的目标。其次，政府和私人企业之间的信息共享也十分必要。很多情况下，国家的基础设施都是由私人企业负责运营，但与国家相比，企业在信息和情报收集渠道、数量和质量上存在明显不足。其三，在网络空间冲突治理中也要注重培育“人道主义”精神，在物理空间中发动袭击的一方有义务将平民的伤害最小化。任何技术能力超强的国家在使用网络武器时，也必须考虑将平民伤害降至最低。有学者甚至认为，网络武器造成的伤害程度应该限制在小于一枚炸弹的损伤。[①]

（三）构建冲突治理机制

国际社会一直在倡导创立治理冲突的国际机制，其目的在于通过国家之间的政策协调，在达成共识的基础上形成网络冲突治理机制，并逐渐建立网络空间国际秩序，进而培育全球网络空间治理文化。[②] 国际社会高度重视网

[①] “Cyber Security and International Law,” Chatham House, May 29, 2012, https://www.chathamhouse.org/sites/files/chathamhouse/public/Research/International%20Law/290512summary.pdf.

[②] 黄日涵：《网络战山雨欲来 安全困境亟须破局》，载《中国社会科学报》2014 年 12

络空间冲突难以估量的破坏力和影响力，在实践中尝试双边和多边合作并取得了一些成果，这可为全球性网络空间治理机制的建设提供必要借鉴。

作为最具影响力的政府间组织，联合国应在网络空间冲突治理中发挥主导作用。抛开联合国的网络空间冲突治理机制不具有广泛的代表性，也无法获得国际社会的普遍认可。早在 2006 年，联合国成立了开放性的互联网治理论坛（Internet Governance Forum, IGF）。[①] 截至 2014 年，互联网治理论坛已经连续举办 9 届。2015 年 4 月，联合国围绕俄罗斯提出的“网络犯罪”国际公约展开对话，但由于发展中国家和美国、加拿大、欧盟等发达国家和组织的严重分歧，没有达成共识。这表明各国已经为达成全球性协议打开了对话的大门。[②] 作为联合国的专门机构，国际电信联盟（ITU）也发挥了重要作用，正积极倡导“利益相关方”（stakeholder）理念，号召全球各国参与维护国际社会网络安全的进程中来。国际社会的探索与尝试都表明，网络空间治理本身是全球治理的一部分，每个国家都面临网络袭击、网络冲突乃至网络战争的威胁，因此参与多边合作是各国维护自身利益的最优选择。

同时，区域性国际组织也在探索网络空间治理的新模式。2007 年召开的上海合作组织（SCO）第七次首脑理事会提出了针对信息安全的“行动方案”（Action Plan），强调国家对网络系统和信息内容的管控权。2008 年初，北约针对爱沙尼亚事件专门召开了北大西洋理事会紧急会议，并出台了网络防御政策（cyber-defense policy），第一次将网络安全问题确立为其集体防御义务的内容。北约声称，如果其成员国遭受灾难性的网络袭击，新的网络安全政策将为其提供有效的回击工具。同年 3 月，北约网络防御管理机构（NATO Cyber Defense Management Authority, CDMA）成立，旨在形成对盟国网络行动能力的统一调配；5 月，北约协作网络空间防御卓越中心（Cooperative Cyber Defense Centre of Excellence, CCS COE）正式在塔林

月 10 日，第 B02 版。

[①] 《联合国互联网治理论坛（IGF）简介》，国家工信部网站，2008 年 2 月 21 日，http://www.miit.gov.cn/n11293472/n11295361/n11296722/11642344.html。

[②] Mark Ballard, “UN Rejects International Cybercrime Treaty,” *ComputerWeekly.com*, April 20, 2010, http://www.computerweekly.com/news/1280092617/UN-rejects-international-cyber crime-treaty.

（Tallinn）成立，旨在加强北约网络防御的综合能力，两大机构的设置成为北约网络防御事业迈向机制化的标志。[①] 北约官方也表达了与韩国和其他东亚国家在网络空间进行安全合作的意图。

现行全球治理机制中，网络空间冲突治理较为成功的案例是多边法律互助条约（Mutual Legal Assistance Treaties, MLATs)。它针对的是各国公认的网络犯罪，规定参与国分享信息、证据及其他形式的合作。该条约主要适用于利用网络系统实施的犯罪。欧洲理事会于 2001 年签订《网络犯罪公约》（Council of Europe Convention on Cybercrime, CEC），以定义和惩治进而威慑相关网络犯罪。《网络犯罪公约》是针对网络袭击最为重要的多边合作协定，也是世界上第一个打击网络犯罪的国际公约，必将对很多国家的立法产生重要影响。有学者建议依据该公约开展打击网络犯罪的国际司法合作。[②] 约瑟夫·奈认为，限制所有的网络入侵是不可能的，但可以从打击网络犯罪和网络恐怖主义方面进行合作，而大国在这些问题上存在很多共同利益。[③]

无论是联合国还是其他区域性国际组织，都通过自身的实践探索网络空间全球治理的模式。这些实践将极大丰富网络空间冲突治理的理论基础和现实经验，对推动国际社会构建相关治理机制有着重要意义。网络空间冲突治理要达到的终极目标是突破观念分歧，在共同利益的基础上，实现超越国界、领域、层级的全方位、立体式合作，最终净化网络空间，达至善治。这个过程可能需要很长时间，而且需要国际社会的共同努力。

四、中国在网络空间冲突治理中的角色及贡献

据中国互联网中心（CNNIC）发布的第 36 次《中国网络发展统计报告》显示，到 2015 年 6 月，中国的网民数量已经达到 6.68 亿，互联网普及率达到 48.4%。这表明中国已经是全球网民数量最多的国家，也说明中国人的生

[①] 毛雨：《北约网络安全战略及其启示》，载《国际安全研究》2014 年第 4 期，第 112 页。

[②] 王孔祥：《网络安全的国际合作机制探析》，载《国际论坛》2013 年第 5 期，第 4 页。

[③] Joseph S. Nye, Jr, “From Bombs to Bytes: Can Our Nuclear History Inform Our Cyber Future?” *Bulletin of the Atomic Scientists*, 2013, Vol. 69, No. 5, p. 13.

产生活、经济的增长和创新都与网络密切相关，中国已经成为一个名副其实的全球网络大国。作为一个全球大国，中国始终都将自身在网络空间安全治理中的角色定位为：参与者、建设者和实践者。中国的国家战略是从一个网络大国发展为一个网络强国，并为推进建设平衡发展、规则健全和秩序合理的全球网络空间而不懈努力。作为最大的发展中国家，中国长期致力于为广大发展中国家争取权利，并积极参与构建和平、安全、开放、合作的网络空间，推动建立多边、民主、透明的全球互联网治理体系。[①] 与此同时，中国政府在既有治理经验的基础上提出了具有中国特色的网络治理原则，如依法治网、秩序优先和积极融入等，这些对于那些与中国国情相似的广大发展中国家具有重要的参考价值和借鉴意义。[②] 2015 年 9 月，中国国家主席访问美国期间，在接受《华尔街日报》书面采访时表示，中国是网络安全的坚定维护者。一方面，中国将加强与美国、欧盟、俄罗斯的合作，通过建立双边与多边合作机制，以增加互信，并致力于构建网络安全行为准则。另一方面，中国将在网络空间全球治理中更加主动，努力将中国所倡导的维护网络主权，重视网络公平，开展务实合作等理念纳入网络空间国际准则中。同时，中国也将履行承诺，积极推动网络空间全球秩序的构建。

此外，中国正着手制定适合本国网络安全的相关法律规范。2015 年 6 月，全国人大首次审议了《中华人民共和国网络安全法（草案）》。法案总则第 5 条明确提出“中国将积极加强在网络空间治理、网络技术研发和标准制定、打击网络违法犯罪等方面的国际交流与合作，推动构建和平、安全、开放、合作的网络空间。”[③] 这表明中国致力于通过法律界定网络安全、维护网络主权、规范网络行为，推动网络空间国际合作。同时，中国也积极主张在网络空间治理中发挥联合国的主导作用。2011 年，中国和俄罗斯等国共

[①] 《共同构建和平、安全、开放、合作的网络空间　建立多边、民主、透明的国际互联网治理体系》，人民网，2014 年 11 月 20 日，http://politics.people.com.cn/n/2014/1120/c1024-26057363.html。

[②] 丛培影、黄日涵：《中国网络治理模式的世界意义》，光明网，2014 年 12 月 15 日，http://theory.gmw.cn/2015-12/15/content_18098761.htm。

[③]《中华人民共和国网络安全法（草案）》，中国人大网，2015 年 7 月 6 日，http://www.npc.gov.cn/npc/xinwen/lfgz/flca/2015-07/06/content_1940614.htm。

同向第 66 届联大提交了“信息安全国际行为准则”，就维护信息和网络安全提出一系列国家行为基本原则，并呼吁各国在联合国框架内开展进一步讨论。[①] 2013 年 6 月，中国与美国等 15 个国家在联合国举行的网络安全对话中，明确主张《联合国宪章》适用于网络空间。[②] 2014 年，中国与联合国共同举办信息与网络安全国际研讨会，这是中国为推动网络空间国际规则制定的重要体现。2015 年 12 月，中国国家主席习近平在第二届世界互联网大会上发表讲话，全面阐述了中国关于网络空间发展和安全的基本立场，展示了中国对网络空间人类未来发展的前瞻性思考，并呼吁全球各国应加强沟通、扩大共识、深化合作，共同构建网络空间命运共同体。[③]此外，中国也积极维护发展中国家的网络空间利益和“网络主权”。中国在多个国际场合主张弥合数字鸿沟。网络空间威胁是无国界的，其影响也是跨国性的。很多发展中国家的网络漏洞将成为被袭击目标，同样它们也可能被操控变成“僵尸网络”（bonnet）而向其他国家发起攻击。在互联网技术应用和开发领域，中国与西方国家还存在明显差距。中国主张网络主要用于商业目的，而不应用于政治和军事目的。未来，中国将继续在网络安全技术方面进行自主研发和创新，这些网络安全技术可以成为中国对外技术援助的重要内容。目前中国正在推进“一带一路”建设，其中的合作重点就包括推进沿线国家和地区网络基础设施建设。同时，中国也愿意在网络空间合作中承担更多责任，发挥积极作用。

[收稿日期：2015-10-20]
[修回日期：2015-12-15]
[责任编辑：石晨霞]

[①] 《中俄等国向联合国提交“信息安全国际行为准则”文件》，新华网，2011 年 9 月 13 日，http://news.xinhuanet.com/2011-09/13/c_122022390.htm。

[②] Patrick Goodenough, “U.S., China Among 15 Countries Agreeing U.N. Charter Applies in Cyberspace,” *CNS News*, June 10, 2013, http://cnsnews.com/news/article/us-china-among-15-countries-agreeing-un-charter-applies-cyberspace.

[③] 《习近平在第二届世界互联网大会开幕式上的讲话》，新华网，2015 年 12 月 17 日，http://news.xinhuanet.com/zgjx/2015-12/17/c_134925295.htm。