网络战的中国视角

张　力*著

关键词:网络战;中国视角;网络实力;网络空间

2007 年 4 月,爱沙尼亚遭遇的网络攻击被西方国家普遍认为是网络空间爆发的第一次国家层面上的网络袭击;而 2008 年 8 月格鲁吉亚遭遇的网络攻击则被看作人类第一场与传统战争相结合的网络战争。以美国为首的西方国家对这两场网络战均予以高度关注和反思,认为尽管一直担心的"数字珍珠港"事件未发生,但是网络战已经成为国际社会的现实。

2011 年 5 月 16 日,美国高调发布《网络空间国际战略》[1],一石激起千层浪。对于此次美国网空新战略的出台,国际社会有各种解读,但是有两点不容否认,一是新战略非常重要且内涵丰富,美国的此次政策宣示决定着网空未来的发展走向;二是美国的新战略并非一蹴而就,而是多年来美国在网空全力打造网络实力,并以此为基础精心谋划的必然结果。

美国在新战略中称必要时将"动用军事力量来应对网络空间的敌对

---

* 张力是中国现代国际关系研究院信息与社会发展研究所所长。他也是由中国现代国际关系研究院和美国战略与国际研究中心主持的中美网络安全对话的共同发起人之一。

〔1〕 'International strategy for Cyberspace – Prosperity, Security and Openness in a Networked World', White House, May 2011, available at: http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf.

行为”[2],并首次把自卫权作为网空的根本行为准则,从而将美国在网空的军事战略构想公之于世。

网络战的基础——网络实力

面对一些媒体对网络战的炒作,中国一直持冷静观察的立场,中国不赞成盲目炒作网络战的行为,同时中国学者和专家也与国际同行在学术交流时就此进行了积极研讨。其实早在 2009 年,中日两国的学者在围绕“网络时代的霸权”进行合作研究时,就在充分借鉴欧美同行研究成果的基础上,共同提出了“网络实力”的概念。[3] 根据这一概念,一国的网络战能力必须以该国的网络实力做基础。所谓的“网络实力”,是指一国在网络空间的综合能力和影响力,其构成要素主要包括:

1. 网络与信息技术能力:具体包括技术的研发及创新能力、技术向产业转移并推广应用的能力……

2. 信息产业能力:看一国是否拥有像 IBM、微软、英特尔、谷歌、苹果等具有垄断性的 IT 巨头……这些巨头在 80 年代主要业务是生产通信设备、半导体、计算机;90 年代以来是软、硬件产业,包括自主生产计算机、移动电话及半导体芯片;而目前则还需要垄断相关的应用及服务;未来的发展方向是垄断全球的信息流和数据。

3. 网络市场能力:包括一国国内网络的规模大小、相关关键信息基础设施的整合度、网络用户的数量、计算机拥有量等。

4. 网络文化影响力:是否属于互联网的流行语种(英文、中文还是其

---

[2] ‘International strategy for Cyberspace – Prosperity, Security and Openness in a Networked World’, White House, May 2011, p. 14.

[3] In 1990s, some scholars in the UK and US proposed the concept of ’cyber power’ or ‘information power’. See Tim Jordan, *Cyberpower: The Culture and Politics of Cyberspace and the Internet*, Routledge, London and New York, 1999; Joseph Nye, *The Paradox of American Power: Why the World’s Only Superpower Can’t Go it Alone*, Oxford University Press, 2002; Franklin Kramer, Stuart Starr and Larry K. Wentz (eds.), *Cyberpower and National Security*, National Defense University Press, Potomac Book Inc., 2009.

他语种),网站使用的语言、内容、数量和质量,门户网站在国内外的影响力,等等。

5. 网络外交能力:该国在互联网名称与数字地址分配机构(ICANN)、互联网治理论坛(IGF)以及国际电联(ITU)等现有的国际互联网治理机构中的交涉能力及影响力,能否在互联网国际治理、打击网络犯罪、构建全球下一代网络、域名分配等事务上发挥影响力甚至主导作用等。

6. 网络军力:即国家关键信息基础设施网络及军用网络的防御能力、网络威慑和进攻能力以及网络窃密与反窃密能力等。

7. 网络空间的国家意志与战略:单纯拥有了以上全部或者部分能力还不够,还要看一国是否有将拥有的网络能力转化为行动的决心和意图。即在网络空间的国家行为要有理论指导,要有行动准则,要有战略规划。

我们只需将包括美国、中国等国家在内的全球各主要信息化大国用上述的指标体系予以考量,即可得出对这些国家网络实力的初步估量。不难得出结论:即美国在网络空间拥有无可匹敌的实力优势,居于超强地位。

冷静看待网络战

中国主张世界各国应当珍视网空这一人类社会的第一个人造空间,坚决反对网络空间军事化。主张和平使用网络空间、不首先使用网络武器、不攻击民用目标。主张现有《联合国宪章》、武装冲突法及国际人道法中有关战争、使用或威胁使用武力等的基本原则仍然适用,如"不得使用武力"、"和平解决国际争端"、对作战手法和方法加以限制的区分原则和比例原则等。

既然网络是人造的全新空间,技术性、虚拟性特点明显。而且与网络相关的新技术、新服务、新应用不断涌现。那么人类社会一些传统的理念、认识和规则,现有的国际法框架等都不能完全照搬到网络这个全新的世界中。它是以信息通信等新技术为支撑建立起来的。与人类以往的活动空间相比十分独特,人类对此的认识与理解远远滞后,甚至是管理措施都毫无经验可循。新情况新问题层出不穷,因此,在具体实践

中,相关法律的具体规则势必要不断做出相应调整。对信息社会的管理如此,对网络空间的武力使用更应如此。

中国认为,对原有国际规则的调整可以是适用,可以是解释,也可以是新建。但要保持国际法律框架与体系足够的"开放性"与"灵活性"。无论是探讨网络战、网络冲突、网络武器使用、网络军控及自卫权等概念和内涵,还是探讨网络空间的中立、第三方的权利与责任、非国家行为体的义务等,最根本的目的只有一个,即最大可能避免在网空使用武力或以武力相威胁,避免网络战的发生。网络战界定的门槛一定要高,不能让网络战这一概念泛滥使用,否则媒体不负责任的炒作、民众的误解等只能使国家间的不信任更深,误判更多,所谓的网络军备竞赛更趋激烈。

应该看到,中国自身面临严重的网络威胁,根据中国国家互联网应急中心的统计数据称,中国遭受的互联网攻击持续增长,2012 年上半年,境外有 2.79 万个 IP 地址对中国境内 780 万台计算机实施了攻击,24% 来自美国,17.2% 来自日本,11.4% 来自韩国。[4] 根据中国国防部新闻发言人指出的,2012 年 1 月至 3 月,中国国防部网和中国军网每月平均遭受来自境外的攻击达 8 万余次。

采取必要的网络防御措施和安全手段合乎国家利益和国家安全,也是国际上通行的做法。目前美、法、英、韩、日、印、以等国都成立了网络司令部,建立了网空作战力量,而且都毫不讳言要提升网络攻击能力,又如美国、法国、韩国、日本以及北约等均进行了系列网络战演习,美国、澳大利亚、新西兰等国最近首次将网络战写入国家防务条约中,意欲打造"网络盾牌",再加上西方媒体又不停炒作"网络战爆发在即",中国在网络空间自身的危机感和不安全感也必然在增加。但是,中国"网络蓝军"建设的消息一经公布,就引发国外媒体及官员学者的评论。一些国家趁机在国际上制造舆论,对中国的网空军事力量建设实施牵制和防范;借树中国为敌,为他们自己发展网战能力和在网空扩军备战提供口实。

---

〔4〕 available (only in Chinese) at: http://www.donews.com/net/201210/1678402.shtm.

中国注意到,美国等西方国家已经开始利用国防承包商积极从事网络武器的研发和部署,如洛克希德·马丁、波音、诺思罗普·格鲁曼、雷神公司等军工企业纷纷瞄准网络武器市场。《金融时报》日前称,一系列公司组成了"网络安全军工复合体","都向美国政府出售软件,这些软件可以侵入、降级或破坏敌人的计算机网络,以及用来阻止此类袭击的计划"。[5] 据业界统计,加上私人公司的开支,仅美国的网络武器市场就接近1000亿美元。2011年9月,美、澳、新三国签署文件,将网络攻击纳入防务条约(ANZUS)[6]中规定的冲突范畴,美官员称,这是美国第一次在双边防务条约中正式涉及网络战。在这种日趋严重的网络安全形势之下,中国更担忧网空的和平前景。

加强与各国在网络空间的合作对话

我个人主张,中国应在中俄新近提出的《信息安全国际行为准则》[7]基础上,进一步提出构建"安全、可靠、公正、有序和和平"网络空间的主张,推出网空八条基本原则:即充分尊重网空权利和自由的原则(包括在遵守各国法律的前提下寻找、获得、传播信息的权利和自由;尊重人权和基本自由等)、网络主权原则(强调国家对境内所有信息行为及境外可能危及国家安全的信息行为有管辖权,对境内网络空间有管理权,有保护本国网空安全的权利和责任,这是传统国际关系准则中国家主权、领土完整和政治独立在网空上的延伸),合作原则,均衡原则(强调基于国家间互信基础上的国际合作。技术本身是中性的,而其善恶后果往往取决于使用者。

---

〔5〕 Joseph Menn, 'Defence groups turn to cybersecurity', *The Financial Times*, 10 October 2011, available at: http://www.ft.com/intl/cms/s/0/84697a96-b834-11e0-8d23-00144feabdc0.html#axzz2BeHfWRvK.

〔6〕 'U.S., Australia to add cyber realm to defense treaty', *Reuters*, 14 September 2011, available at: http://www.reuters.com/article/2011/09/15/us-usa-cyber-australia-idUSTRE78E05I20110915.

〔7〕 http://www.fmprc.gov.cn/mfa_chn/ziliao_611306/tytj_611312/zcwj_611316/t858317.shtml.

因此,必须要在自由与管理、权利与义务、安全与发展间求得平衡,既不阻碍技术的创新和正当使用,又能制止有害信息的蔓延及各种危及社会公共安全乃至国际安全事件的泛滥)、和平使用网络空间原则(对全球关键信息基础设施等民用信息系统保护,不以这些设施为目标;不利用信息通信技术包括网络实施敌对行动、侵略和制造对国际和平与安全的威胁,不扩散网络武器及相关技术,反对网空军事化;无论是国家、非国家主体甚至是网民个人都应采取负责任的网空行为,任何危害网空和平有序发展的行为都应受到制止。在涉及上述准则的活动时任何争端,都以和平方式解决,不得使用武力或以武力相威胁,等等)、公平发展原则(包括解决数字鸿沟;对弱势国家权利和利益的保障;反对利用在信息领域的领先地位,包括对国际信息网络基础资源、关键基础设施、核心技术产品和服务的优势,削弱他国对信息技术产品和服务的自主控制权,威胁他国政治、经济和社会安全等)、保护个人信息、尊重隐私原则以及包容性原则(尊重各国历史、文化和社会制度的多样性等)。

美国副总统拜登先生在 2011 年 11 月初的伦敦网络空间国际会议上通过视频演说指出:"网络是 21 世纪的公共空间……预计未来二十年,全球 50 亿人上网,下一代人的生存空间也将向网络转换,这种技术发展的趋势目前我们难以想象的……网空是中立的,但是人类的所作所为不中立。各国有义务不能让网络受到损害,不能让网络战发生。如何才能做到网络更安全、更开放、更可信、更具有可操作性? 除了制定规则,耐心解释说明之外,没有捷径可走。"〔8〕与此同时,中国也主张:"世界各国应当携起手来,大力加强网络领域的国际交流与合作,共同构建一个和平安全、开放有序的和谐网络空间。"〔9〕

---

〔8〕 此部分讲话内容,是本人根据在伦敦现场的听译,正式文本请参见 Office of the Vice President, 'VP's Remarks to London Cyberspace Conference', The White House, 1 November 2011, transcript and video available at: http://www.whitehouse.gov/the-press-office/2011/11/01/vps-remarks-london-cyberspace-conference。

〔9〕 Secretary of Treaty and Law of Ministry of Foreign Affairs of China Huang Huikang's speech in Budapest. available at: http://news.xinhuanet.com/tech/2012-10/05/c_113280788.htm.