美俄在网络军备控制上的共识与分歧

杜雁芸

内容提要：随着网络全球化的纵向横向扩展，世界各国尤其是美国、俄罗斯日益重视网络军事化的发展，美俄逐步加强网络军备建设。网络军备竞赛的凸显和网络安全事件频发迫使美俄重新开启网络军控谈判。目前，美俄在网络军备控制议题上存在着共识和分歧。美俄之所以不积极推行网络军备控制谈判，源于网络作战的军事诱惑性压倒网络军控谈判必要性的认知，这已成为双方心照不宣的共识；双方军控谈判的分歧为网络战略选择上的“自由”与“控制”之争。这些是导致网络军控谈判难以施行的主观层面的原因。当前美俄网络军控谈判前景黯淡，网络军备控制任重道远。

关键词：美俄　网络军备控制　共识与分歧　困境分析

随着网络技术的迅猛发展和国际社会对网络依赖逐步加深，各大国尤其是美国、俄罗斯将网络安全视为国家安全中的重要组成部分，更加重视网络军备建设和网络军事化发展。由于美俄网络军备竞赛凸显和网络攻击事件频发，美俄开始关注网络军备控制问题。双方就网络作战的军事诱惑性压倒网络军控谈判的必要性达成某种共识，但双方在网络战略定位上存在巨大差异，形成以美国为代表的“自由派”和以俄罗斯为代表的“控制派”两大阵营之争。当前，美俄是网络军控谈判的主角，美俄双边谈判能否顺利推进是关系到网络军控机制确立和网络空间国际秩序构建的重要因素。

美国和俄罗斯分别代表了“自由派”与“控制派”，是网络军控谈判的主角。

杜雁芸　国防科学技术大学国际问题研究中心、人文与社会科学学院讲师。

一、美俄网络军备控制的现状分析

当前，美国、俄罗斯非常重视网络在军事作战中的重要作用，不断加强网络军备建设。美俄积极组建网络部队，纷纷出台网络战略，加大网络武器的研发力度，在网络攻击和网络战中崭露头角。与此同时，基于不同的利益诉求，双方网络军控谈判已然展开。

（一）美俄加强网络军备建设

网络军备建设是网络军事化的建设。它包括网络战略的出台、网络部队的组建和网络设备、网络武器的研发。目前，网络战的实战能力成为各国军事实力的重要组成部分。因此，各国纷纷采取措施，加强自身网络军备建设，新一轮的网络军备竞赛正在拉开序幕，美俄竞相粉墨登场。早在1991年的海湾战争中，美军通过激活隐藏的病毒以瘫痪伊拉克的防空系统，开启了网络战的序幕；在1999年的科索沃战争和2003年的伊拉克战争中，美国和北约加强了网络攻击在战争中的运用；2007年爱沙尼亚政府网站和2008年格鲁吉亚政府网站先后遭到据说源自俄罗斯的网络攻击，这被视为国家间发动网络战争的开端；之后美国的“震网”病毒和“火焰”病毒对伊朗和中东国家的攻击，展示了网络武器的有效性和强大威力。可以看出，美俄网络军事化发展迅速，网络军备竞争愈演愈烈。

美军十分重视网络军备建设，其要想维持其在陆地、海洋、天空和太空的军事优势，强化在数字空间的行动能力是先决条件。[1] 为此，美军已将网络军备建设纳入国家战略层面，美国白宫和国防部相继在2011年5月、7月分别出台《网络空间国际战略》和《网络空间行动战略》报告，向国际社会宣告美国要在网络空间秩序构建中占据主导地位，并明确指出对美国发动的任意网络攻击都被视为战争行为，美国对此保留军事回击的权利。[2] 在网军建设方面，多年来美国致力于打造一支攻防能力强的网络部队。美国网络司令部于2010年5月21日正式启动。网络司令部和国家安全局由一人领导，既提高决策效率，又利于相互提供情报支持。[3] 2013年，美国热炒中国黑客攻击事件，借机将网络司令部由900人扩

1 李恒阳:《美国网络军事战略探析》,《国际政治研究》，2015年第1期，第116页。

2 The White House，“International Strategy for Cyberspace：Prosperity，Security，and Openness in a Networked World”，May 2011，http：//www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf，2016-03-22；Department of Defense Strategy for Operating in Cyberspace，July 2011，http：//www.defense.gob/home/features/2011/0411_cyberstrategy/docs/DoD_Strategy_for_Operating_in_Cyberspace_July_2011.pdf，2016-03-22.

3 Office of the Under Secretary of Defense，“Overview-FY 2014 Defense Budget，”http: / / comptroller. defense. gov/defbudget/fy2014/FY2014_Budget_Request_Overview_Book. pdf，2016-04-10.

编到4900人，宣布三年内扩建40支网络战部队。2014年9月美国网络司令部司令迈克尔·罗杰斯（Michael S. Rogers）指出，美军正在组建一支新的网络防御部队。这支拥有6200名成员的部队应在2016年之前具备完全作战能力，旨在强化对黑客活动以及由其他国家发起的网络攻击的防御。[1] 2015年4月23日新版国防部《网络空间战略》出台后，五角大楼随即调整了美国网军的结构，133支网络任务部队主要由以下三支部队组成：一类是执行进攻任务的作战部队，一类是保护国防部内部网络的网络保护部队，还有一类是保护美国国内电网、核电站等重要基础设施国家任务部队。一系列动作表明，美军突破了网络战在编制体制、装备设备、融入联合等一系列问题上的瓶颈，竭力探索网络攻防战斗力生成的有效模式。[2]

与此同时，美国加大力度进行网络武器的研发制造，仅病毒武器就已达到2000多种，这些病毒武器早已进入美军武器序列。“震网”、“火焰”病毒的出现显示出了网络武器的强大破坏力和威慑力。美国还在研制新概念、新机理网络战武器。例如，嗜食硅基电子芯片的细菌、用来破坏电子电路的微米/纳米机器人和“网络数字大炮”等设想，[3] 这些技术一旦实现，其有效破坏力将堪比原子弹，加剧美俄在网络武器技术上的竞赛。

俄罗斯加速筹建网络军事力量，网络力量组织架构基本成型，实战能力强。在网络战略方面，2013年2月俄联邦委员会提交《俄罗斯网络空间安全战略（草案）》，提出建立国家数字化主权，明确了俄罗斯联邦网络安全战略的原则、行动方向和优先事项。[4] 在部队组建方面，在网络力量“三驾马车”的基础上，俄罗斯已开始筹备组建网络部队，同时将建立专门应对网络战争的新兵种。目前，俄内务部设有“K”局，“K”局负责调查境内网络犯罪活动，将罪犯绳之以法；安全局设有信息安全中心，负责对抗利用虚拟空间危害俄国家和经济安全的外国情报机构、极端组织和犯罪组织；俄国防部的网络司令部将负责遏制其他国家在网络空间对俄国家利益的公然侵犯，其组建使俄在网络力量组织架构上的“三驾马车”基本成形。[5] 内务、安全与军队3大系统下辖的网络力量分工明确，各司其职。由此，真正意义上的“网军”在俄军序列中出现已是指日可待。网络战在俄罗斯被称作“第六代战争”，政府由此招徕大量网络精英。在技术研发方面，俄罗斯注重贴近实际和反制能力。如，2014年7月底，俄罗斯通信部组织了一次

1 “US Bolstering Cyber Defense with New Corps：NSA Chief Michael Rogers”，*The Economic Times*，September 16，2014，http://m.economictimes.com/news/international/world-news/us-bolstering-cyber-defense-with-new-corps-nsa-chief-michael-rogers/articleshow/42644102.cms，2016-02-23.

2 杜雁芸：《美国网络霸权的路径分析》，《太平洋学报》，2016年第2期，第73页。

3 袁艺等：《揭开网战武器的面纱》，《中国青年报》，2012年2月10日，第9版。

4 黄朝辉、刘杨：《2013年全球信息安全建设大扫描》，《中国信息安全》，2014年第1期，第83页。

5 马建光：《俄罗斯亮剑维护网络安全》，《世界知识》，2014年第17期，第43页。

网络演习，全面评估俄国内网络稳定性，在此基础上研究制定有效措施提升网络防护能力。此外，俄罗斯一直在发展自己的网络反制能力，根据美国私营网络安全公司的调查，俄罗斯黑客把大量西方石油和天然气公司作为攻击目标，并有能力远程操纵工业控制系统。[1]

俄罗斯的网络战部队起步虽然较晚，但其网络斗争能力和实战能力效果突出，这在爱沙尼亚和格鲁吉亚遭到网络攻击的案例中可见一斑。2007年4月，爱沙尼亚因苏联时期纪念铜像搬迁问题与俄罗斯交恶后，爱沙尼亚许多重要机构——包括议会、政府部门、银行、报纸和电视台等——的网站遭到大规模网络袭击，袭击者通过分布式服务拒止攻击（DDOS attacks）使目标网站短时间内承载过量访问而陷入瘫痪。爱沙尼亚政府指责袭击是俄罗斯指使或直接发动的，而许多战略分析人士更是将此次袭击视为第一场国家间的网络战争，俄罗斯也被西方视为“第一个发动国家间网络战争的国家”。[2] 类似的情景在俄罗斯—格鲁吉亚冲突中重现。2008年8月8日，俄罗斯和格鲁吉亚的军队因南奥塞梯问题交火后，格鲁吉亚互联网络受到大规模攻击，政府网站系统全面瘫痪，交通、通信、媒体和银行的网站纷纷遇袭。尽管俄罗斯政府对发动网络袭击的指责始终采取否认态度，但袭击恰恰发生在国家间的紧张对峙乃至武装冲突期间，其规模和破坏力远超出普通黑客间进行的网络攻击，这一点无可否认。《纽约时报》获取的一份2009年的美国国家安全局绝密文件中称，俄罗斯是美国在网络空间里最老辣的对手。火眼（计算机安全公司）的报告还指出，俄罗斯政府的攻击和俄罗斯网络犯罪分子的攻击是很难分辨的。[3] 可以看出，俄罗斯通过两次网络实战，已将网络攻防、网络战由概念设想变为实践操作，为其网军的建设和发展提供至关重要的实战经验。

（二）美俄网络军控的提出及现状

20世纪末网络军控议题就已提出。俄罗斯最早提出要在国际上建立网络军备控制机制，试图和美国或北约进行协商谈判，避免日后网络军备竞赛和网络攻击升级。1996年，美俄就此问题进行了秘密会商，双方并未达成任何协议，网络军控谈判就此搁置。[4] 此后，俄罗斯一直以联合国军控机制为平台，渐进推动

---

1 Nicole Perlroth，“ R ussian Hackers Targeting Oil and Gas Companies”，*The New York Times*，June 30，2014，http: / / www. nytimes. com /2014 /07 /01 / technology / energy-sector-faces-attacks-from-hackers-in-russia. Html，2016-03-26；“ Drag-onfly: Cyberespionage Attacks against Energy Suppliers”，July 2，2014，https: / / fujitsu. symantec. com / asset / down-load /9a701e2bc01035172574910d16e75d0f，2016-03-26.

2 程群：《网络军备控制的困境与出路》，《现代国际关系》，2012年第2期，第15页。

3《外媒：中美俄上演网络安全大博弈》，参考消息网，http://china.cankaoxiaoxi.com/2014/1101/549731.shtml，2016-03-04。

4 John Markoff，Andrew E. Kramer, “U. S. and Russia Differ on a Treaty for Cyberspace”, *New York Times*, June 28, 2009.

网络军控发展。自1998年以来，联合国大会裁军与国家安全委员会每年都会收到俄罗斯提交的有关网络军备控制的决议草案。1998年10月，俄罗斯联邦政府向联合国第一委员会提交了关于禁止信息战武器的议案，但该倡议并未得到美国等西方国家的积极响应。同年12月该委员会第79次全体会议达成了一个折中决议。2011年11月联合国大会以173票赞成、1票（美国）反对、1票（以色列）弃权，通过了题为《禁止发展和制造新型大规模毁灭性武器和此种武器新系统：裁军谈判会议的报告》的决议草案，该草案虽由白俄罗斯代表提案，但得到俄罗斯的强力支持。由此，在俄罗斯的推动下，网络军备控制正式列入联合国军控项目，网络军控成为军控项目中重要的议题之一。[1] 此外，2011年9月，以俄罗斯为主的几个发展中国家（包括中国、塔吉克斯坦和乌兹别克斯坦；2013年3月，哈萨克斯坦和吉尔吉斯斯坦加入“准则”共提）向第66届联合国大会共同提交了“信息安全国际行为准则”草案，为相关国际讨论提供基础。[2] 该草案是国际社会第一份规范网络空间和信息安全的提案。

俄罗斯在网络军备控制方面进行的努力没有得到美国的赞同和支持。早些年，美国对网络军备控制始终持消极否定态度，俄每年向联合国大会提交的网络军备控制决议草案，美国均投反对票。进入21世纪，美国对网络的依赖不断加深，美国愈加担心网络攻击使其基础设施受到破坏，在网络军控上的立场较之前有所松动，开始与其他国家对话。2009年11月，美国与俄罗斯、联合国军控委员会在日内瓦共同商讨网络空间的军事化问题。次年4月，美俄进行会晤，涉及网络犯罪、网络安全和网络战等问题。双方的军控谈判虽然进了一步，但仍存在原则性的分歧。俄方希望制定网络军控条约以防范网络军备竞赛，美方倾向于通过签署协议打击网络犯罪。美国政府及军方认为：（1）与其签订网络军控条约，不如强化打击网络犯罪的合作。网络空间安全属于非传统安全，因其非对称性导致军控条约不适用，打击网络犯罪——比如对网络黑客和网络恐怖分子的攻击行为进行控制——效益更高。（2）先建设关键性国家基础设施，然后进行网络军控谈判。美国政府对网络军备控制的态度取决于其关键性国家基础设施能否有效应对国家级的网络攻击。因此，克林顿执政时期就开始强调美国基础设施的重要性，在1998年5月发布了第63号总统令，即《克林顿政府对关键基础设施保护的政策》。时至今日，美国政府依旧在加强关键性基础设施的安全性。（3）网络空间合作的前提是具备相同的价值观理念。在美国出台的多份网络空间战略报告和前国务卿希拉里·克林顿（Hillary

俄方希望制定网络军控条约以防范网络军备竞赛，美方倾向于通过签署协议打击网络犯罪。

1 联合国大会文件 A/66/402，http://www.un.org/zh/documents/view_doc.asp?symbol= A/66/402。

2 “信息安全国际行为准则”，中华人民共和国外交部军控司，http://www.fmprc.gov.cn/chn/pds/wjb/zzjg/jks/fywj/t858317.htm，2016-02-12。

Clinton）的发言中可以看出，美国愿与有共同价值观的国家进行多边协作。在此理念下，美国在网络空间已经与具备“同等价值观理念的国家”中的英国、澳大利亚和加拿大等国进行了合作和磋商，并与其盟友在2006—2010年举行了系列“网络风暴”大规模网络攻击应对演习。随着网络攻击事件频频发生，以及斯诺登事件持续发酵带来一系列负面影响，美国在军控谈判上的立场再次松动软化，在防止网络冲突方面，美国同意与俄罗斯建立信任措施。2012年美俄达成共识，为防止逐步升级的敌对引发网络空间误判，美俄将核安全通信系统运用于网络空间。[1] 可以看出，美俄网络军控谈判虽然成效不佳，但逐步推进。

二、美俄在网络军控上的共识：网络作战的军事诱惑性高于网络军控谈判的必要性

网络军控谈判难以深入推进的一个重要原因，是美俄之间形成了心照不宣的共识与默契，即，与传统作战方式相比，运用网络武器、进行网络攻击的军事诱惑性更大。网络战争具有低投入、高效益、危害大、威慑强等特点，成本/效益比极高。而且，网络作战可能会建立一种新形式的“互相确保摧毁”的模式，美俄正试图建立有效的网络威慑。由此，美俄双方均认为，当前网络军事化发展的诱惑性远远高于网络军控谈判的必要性。[2]

美俄均偏好网络军事化发展而非网络军控谈判。

（一）网络军备建设具有投入较少、简便易施的特点，美俄意识到网络攻击可以用极低的成本获得非常高的军事效益

网络军备建设中，网络武器成本低廉、网络作战方便易施，美俄非常看重这些优势，并利用这种非对称来增强自己的攻击能力。事实证明，开发、操作网络武器的平台并不复杂，几台电脑就足够了，不需要大型制造设施和工业基础设施，也不需要传统作战行动中的社会化大生产；发动网络攻击，可以从世界上任一地点、在任一时间进行，不需要耗资巨大的远程奔袭和投送就可以对敌人进行快速打击，网络战部队可视为一种缩短对抗距离和减少武装打击成本的新型作战部队形式；与传统战争相比网络攻击的成本消耗极低，有时甚至不需要人为操作，计算机程序自行搜索并向预设目标发动攻击。美国一家专门研究网络流量机构的研究室主任比尔·伍德库克（Bill Woodcock）说：“网络攻击所需代价非常

1 “U.S., Russia Close to Agreement on Preventing Cyber Conflict”, *Top News*, April 28, 2012, http://www.topnews.in/usa/us-russia-close-cyber-conflict-preventing-agreement-217007, 2016-02-22.

2 吴翔、翟玉成：《网络军控倡议、问题与前景》，《现代国际关系》，2011年第12期，第19页。

小，一辆坦克履带的价格足够发动整场网络战争！”[1] 2009年12月，伊拉克武装分子用价值26美元的软件拦截了美军“捕食者”无人机的视频画面，据此监视美军的行动和逃避其打击。[2] 另外，美俄十分重视网络军备发展的非对称性，即国家发展网络军事实力可以不受经济实力和国力的影响。因为网络军事力量建设更多着眼于“操作技术”的研发，而并非“武器装备”的建设，这就使得小国也可以在网络空间发展军备抗衡大国。为避免国际网络军备发展的态势失衡，也为了保住自身网络军备的优势地位，美俄不断加强网络军备建设。

虽然网络军备投入小、成本低，但在未来作战行动中，网络战与传统军事行动密切结合，在摧毁敌方的经济和基础设施中起着至关重要的作用，网络破坏所造成的危害也愈大，有个别国家甚至将网络攻击定义为“大规模杀伤性武器”。美俄已将网络战的对抗上升到国家战略层次，可以兵不血刃地攻击破坏对方的指挥控制、情报信息等军用网络系统，最终达到不战而屈人之兵的效果。2007年以色列空军的战斗机成功绕开叙利亚军队苦心经营多年的防空体系，对叙方纵深100千米内的所谓“核设施”目标实施了毁灭性突击。以军制胜的秘诀，在于使用了美军的“舒特”攻击系统。网络攻击不仅威胁国家的战争体系，还可以渗透到政治、经济、金融、外交等各个领域。2010年，伊朗境内包括布什尔核电站在内的5个工业基础设施遭到攻击，导致其浓缩铀工厂内约1/5的离心机报废，其核计划因而大大延迟。美国国务卿希拉里称“超级工厂病毒”已使伊朗的核项目倒退了数年。“超级工厂病毒”就是被誉为“精确制导的网络导弹”的“震网”病毒（Stuxnet），是第一个专门定向攻击真实世界中基础设施（比如核电站、水坝、国家电网）的“蠕虫”病毒。这次攻击成为运用网电手段攻击国家电力能源等重要关键基础设施的先例。据《纽约时报》报道，“震网”病毒是美国和以色列情报官员在以色列绝密的迪莫纳核设施内联合研发的，旨在破坏伊朗核项目。该项目是美国前总统乔治·W. 布什卸任前启动的，贝拉克·奥巴马执政后，加速了该项目的实施。美国政界意识到，当前不少国家金融、能源、交通、电力等关键业务网络已基本实现信息化、网络化，但防护手段还不尽完善，能够“震颤”攻击伊朗核设施的病毒，也可以“震颤”攻击这些国家工业系统中的相关控制与采集系统，网络武器可以置国家重要的战略网于平时被控、战时被瘫的巨大风险之中。同样，俄罗斯在对格鲁吉亚和爱沙尼亚的网络攻击中获益颇多。这种成本低、投入小、获益高的军备建设深受美俄军方青睐。

---

1 李刚、杨国辉：《网络战现形记》，《中国信息安全》，2010年第7期，第49页。

2 Siobhan Gorman, Yochi J. Dreazen and August Cole, “Insurgents Hack U.S. Drones,”Dec. 17, 2009, http: / / online.wsj.com / news / articles / SB126102247889095011, 2016-03-10.

（二）网络作战可能会形成一种新形式的“互相确保摧毁”的模式，美俄试图确立各自网络空间的有效威慑

像核威慑一样，网络空间也具备威慑的条件：各国对网络空间依赖性增强、网络的脆弱性不断彰显，例如攻击技术的扩散、木马病毒的传播、电脑漏洞的存在和后门预设，等等，这决定了即使网络攻击能力强的国家也无法在这一领域取得压倒性的、不受惩罚的优势，也会遭到毁灭性的攻击，这就形成了一种新型的“互相确保摧毁”模式。网络空间的“互相确保摧毁”是指敌对双方均拥有可靠的二次网络打击能力时，在一方首先实施网络攻击后，另一方仍具有瘫痪对方基础设施的网络实力，并具备完全摧毁对方的报复能力，这使双方都不敢贸然发动全面的网络战袭击，从而避免大规模网络战争，实现了“稳定的恐怖和平”。各国建设网络军备的同时，注重网络威慑的实效，而强国和弱国实施网络威慑的方式不尽相同。美欧等网络强国在生产、生活的方方面面对网络依赖性极高，网络的脆弱性强，因此，美国采取的是防御性的威慑，即通过自身强大的进攻和防御能力，阻吓对手在网络空间发起不计后果的攻击，尽量将对手的攻击控制在网络空间之外，或者减弱对方攻击对自身的影响。而弱国的网络威慑更多体现为“光脚不怕穿鞋”的观念。弱国凭借强国对网络的高度依赖性，将这种依赖性作为某种“抵押品”进行“挟持绑架”，使对方感到难以承受打击的后果。因此，弱国在网络空间虽然处于劣势，但它却可以利用强国依赖性强的“软肋”，使其不敢对自己发起攻击，真正实现“以弱制强”的威慑。

美国政府十分重视网络威慑战略。一方面，通过高调发布网络威慑战略，申明其使用网络实力的决心。2011年5月美国政府发布了《网络空间国际战略》，明确指出美国将运用威慑方式回应敌方的网络攻击，并保留行使武力的权力。[1] 之后，军方在7月发布的《网络空间行动战略》再次强调，美军应有效慑止、击败对美军的网络进攻。[2] 2015年新版《网络空间战略》首次公开表示美国军方将把“网络战”用作针对敌人的作战方法，明确表示美军在与敌人发生冲突时，可以考虑实施“网络战”。[3] 较之2011年的《网络空间国际战略》，新版的网络战略基调已从重在防御转向“在必要的情况下”主动进攻，这体现出美国将对网络攻

1 The White House, “International Strategy for Cyberspace：Prosperity，Security，and Openness in a Networked World”, May 2011, http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf, 2016-03-22.

2 “Department of Defense Strategy for Operating in Cyberspace”, July 2011, http://www.defense.gob/home/features/2011/0411_cyberstrategy/docs/DoD_Strategy_for_Operating_in_Cyberspace_July_2011.pdf，2016-03-22.

3 The Department of Defense Cyber Strategy, April 2015, http:http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf, 2016-04-02.

击进行报复的决心。美国国防部部长阿什顿·卡特（Ashton Carter）宣布这一新战略时指出："尽管我们优先考虑威慑外来攻击，但我们的防卫部署不会削弱我们主动选择网络攻击的意愿，只要有需要，我们可以主动进攻。"[1]

另一方面，美国不断展示其自身的技术优势和威慑实力。基于网络攻击的速度和精确度，网络武器可以在危机期间警告对手或造成资产损失和人员伤亡的灾难后果，美国可以让对手遭受类似"长崎事件"的重创。而在对方没有网络预警和态势感知能力的前提下，美国具备快速进行大规模打击的能力，使敌国更加"胆战心惊"。因为在现实空间里，如果攻击者从陆、海、空、天发射导弹，受攻方的预警系统就会发出警示信号，决策者根据相应信息和战略目标进行决策，决定是否进行反击；而在网络空间中，目前很多国家不具备网络预警和网电态势感知能力，一旦遭到美军的网络攻击，由于几乎没有时空损耗，当其监测到异常的信息时，其被攻击的后果已经显现，决策者几乎没有决策反击的时间，这使得美国对他国的威慑效果更为明显。

俄罗斯也不断加强网络威慑能力建设，既秉持了强国网络威慑的方式，又沿用了弱国网络威慑的逻辑。俄罗斯是美国之后第一个将网络攻击运用到实战并取得网络威慑实际效果的国家。在俄格冲突中，俄罗斯运用了大规模"蜂群"式网络攻击方式，像运用手术刀一样割断了格鲁吉亚的"作战神经"，仅五天时间就迫使格鲁吉亚屈服。此种实战能力的展示和意志力的彰显，产生了强大的震慑力，在之后的美俄对抗中都起到了实质的威慑作用，这实质上是一种"惩罚性威慑"。[2] 另外，俄罗斯也沿用了弱国网络威慑的理念，即利用美国对网络的高度依赖性，使其明白受到网络报复后的损失大于其进攻的收益，以此慑止美国的网络攻击。

三、美俄在网络军控上的分歧：战略选择上的"自由"与"控制"之争

对于制定通信标准维护网络安全、打击网络犯罪、防范网络恐怖主义和保护信息基础设施等方面，美俄的态度都比较明确，容易开展合作。但在网络军备

1 "美国发布网络战争新战略"，光明日报网，2015年04月25日，http://epaper.gmw.cn/gmrb/html/2015-04/25/nw.D110000gmrb_20150425_6-05.htm，2016-04-06。

2 网络威慑分为惩罚威慑（报复性威慑）和拒止威慑（抵消性威慑）。惩罚威慑通过显示自身强大的攻击能力，以及遭受攻击后使用这种能力进行报复的决心，并采取迅速和压倒一切的报复行为，迫使进攻者认识到得不偿失，从而放弃攻击行为，其立足点是反击能力；拒止威慑则是通过显示其强大的防御能力，使潜在攻击者确信，其攻击将达不到预期效果，攻击的收益小于其攻击成本，从而放弃攻击行为。惩罚威慑强调的是二次打击的能力，即攻击能力，拒止威慑则更加强调防御能力和恢复能力。详见何奇松：《近年美国网络威慑理论研究述评》，《现代国际关系》，2012年第10期，第9页；何奇松：《美国网络威慑理论之争》，《国际政治研究》，2013年第2期，第62页。

控制方面，两国分歧凸显。分歧的主要原因是美俄之间在网络战略定位上存在差异，以美国为代表的西方国家和以俄罗斯为代表的包括中国在内的非西方国家形成了“自由派”与“控制派”两大阵营。美国等西方国家强调“网络自由”，对网络军控态度冷漠，认为不能以国家主权和社会安全为由损害网络自由。“从克林顿政府首次回绝俄罗斯的提议以来，美国一直是固执的网电军控反对者”。[1]而俄罗斯始终强调“网络主权”，积极推动网络军备控制，认为各国有权利根据自身国内情况对国内的网络进行管理，国家的网络主权不容侵犯，各国不得利用网络传播干涉他国内政。

（一）美国对网络军控态度冷漠，强调“网络自由”

为避免影响其意识形态渗透和追求网络霸权，美国对网络军控态度冷漠。

美国对网络军控态度冷漠，有以下两点原因。首先，美国倡导“网络自由”，经常通过信息“自由流动”侵犯别国主权，而军备控制会使他国的网络管控更加严格，影响美国意识形态的渗透。关于网络主权和网络自由的关系，长期以来一直是个存在争议的问题。以美国政治界、学术界和产业界精英为代表的互联网自由主义者主张，互联网无国界，对互联网的访问、管理都应超越单纯的民族国家的界限，达到一种不受限制的、完全自由的状态。对一些国家出于国家安全考虑而实施网络监管的做法，美国加以反对，它极力宣传“网络自由”，从法理上否定其他国家的网络主权。2011年2月15日，希拉里发表演讲，对别国网络治理横加指责，她认为，互联网自由为“普世权利，是加速政治、社会和经济变革的巨大力量”，由于“互联网继续在许多国家受到多种限制”，因此美国要在全球范围内大力推动互联网自由。[2] 美国发布的《网络空间国际战略》也明确说，“美国支持网络自由”，并明确表示“美国将不遗余力地推动网络空间中言论和结社的自由”，批评中国等国家搞网络过滤和网络审查。可以看出，所谓的网络自由，就是美国推行其价值观的政治工具。美国甚至以网络自由为幌子，通过互联网对他国公开进行煽动破坏和政治颠覆。为了实现信息的“自由流动”，美国不仅在政治上向相关国家施压，迫使其开放网络，而且还在技术上大力开发“翻墙”软件。奥巴马积极“支持正在利用尖端技术手段对抗互联网压制行为的新涌现的技术人员和活动人士”，在财政上提供大量支持，已投入数千万美元。当前，美国力推“互联网自由”是重蹈20世纪40年代美国主张

1［美］理查德·A. 克拉克:《网电空间战》，刘晓雪译，北京：国防工业出版社，2012年版，第212—218页。

2 Hillary Rodham Clinton, Secretary of State, U.S. Department of State,“Internet Rights and Wrongs: Choices & Challenges in a Networked World”, February 15 2011.http://www.state.gov/secretary/rm/2011/02/156619.htm, 2016-02-16.

“贸易自由化”的覆辙，是对其他国家网络主权的恣意侵犯。[1] 如若国际社会达成网络军备控制条约，各国就会更加严格地管控自身网络，美国信息无法“自由流动”，势必会弱化美国意识形态的渗透。

其次，美国在网络攻防技术和网络治理方面具有绝对优势，出台一个全面彻底的网络军控条约会限制美国的优势，束缚其称霸全球的脚步。以美国、英国为首的西方发达国家一直是网络信息技术领域的领头雁。美不仅具备超强网络攻防技术，而且在网络治理方面具有绝对优势：其独霸网络资源的分配权力，掌控着互联网主动脉，握有互联网核心技术；美国享有网络控制的主导权，其对互联网通讯干线、基础设施和关键设备具有控制能力，能够操控信息源并主导网络语言的形态；美国还有意主导网络规则的制定，等等。[2] 美国利用其技术优势，在增强自身网络安全的同时加强对参与国信息与安全的控制，从而实现其网络霸权图谋。[3] 美欧等国还凭借网络优势，一直占据着道德、技术和规则的制高点，把持着话语权和规则制定权。比如，美国通过发布相关文件，竖起了网络空间军事化发展的“风向标”；法国主办了首届“八国集团电子论坛”，并要将其打造为“数字达沃斯”。西方国家坚申“基本自由、个人隐私和信息自由流动”是网络空间的核心原则，将互联网自由作为普世权利，向全世界灌输网络空间“负责任的国家行为”和“国家义务”等理念，努力为“网络空间可接受的行为”制定标准。他们倚仗网络资源与技术上的压倒性优势，妄图实现其网络世界的独霸。由此，美国人认为，其技术能力和主导优势如若受到国际军控机制的约束，必然会影响其网络霸权的实现。美国前总统安全顾问理查德·A. 克拉克（Richard A. Clark）指出美国要慎重审视网络军控的立场，他认为“网电空间战武器是美国的优势，我们必须利用技术优势弥补兵力分散以及对手可能掌握尖端常规武器而带来的挑战”。他强调全面禁止网电空间战的网络军控不符合美国的利益，最重要的是要“从有利于美国的角度，仔细选择条约限制的范围”。[4]

（二）俄罗斯积极倡导制定网络军控条约，强调“网络主权”

与美国相异，以俄罗斯、中国为代表的新兴发展中国家出于对国家主权安全的考虑，认为应该加强战略防御，主张在联合国框架下制定互联网空间的行为规范，要对网络空间实施有效控制以抵御来自网络空间的攻击与威胁。俄罗斯认为，美国支持网络自由，就是想将网络攻击合法化，通过网络传播破坏别国稳定，甚至进行政权颠覆活动。美国国家安全局对时任总统梅德韦杰夫的电话监

1 崔建树：《美国网络空间战略研究》，《和平与发展》，2013年第5期，第71页。

2 杜雁芸、刘杨钺：《中美网络空间的博弈和竞争》，《国防科技》，2014年第3期，第70—72页。

3 刘勃然、黄凤志：《美国〈网络空间国际战略〉评析》，《东北亚论坛》，2012年第3期，第59页。

4［美］理查德·A. 克拉克：《网电空间战》，刘晓雪译，北京：国防工业出版社，2012年版，第212—218页。

控给俄罗斯敲响了警钟。[1] 俄罗斯积极倡导“网络主权”，以此应对西方通过网络进行网络窃密及意识形态侵蚀渗透。2014 年5月，俄罗斯总统普京签署“知名博主新规则法”，规范网络空间秩序。7月，俄罗斯议会通过了一项新的涉互联网法案，要求所有收集俄罗斯公民信息的互联网公司都将数据存储在俄罗斯国内。[2] 为了防止信息外泄，俄罗斯政府要求国内的大型互联网公司搬迁服务器，从而使俄罗斯用户的信息都存储于本国境内的数据中心。这些俄罗斯网络服务商也可拥有国外服务器，但其只能用来存储外国网站和用户的信息。对于社交网站、论坛、微博的管理方，俄国政府要求其将境内的服务器用户数据保留半年以备调查。对于在俄经营的外国公司，俄罗斯政府要求其在俄罗斯重新注册子公司并设立代表处以加强管理。俄罗斯还提出只使用自己的服务器、操作系统和搜索引擎。

另外，由于网络核心技术一直掌握在美国人手中，俄罗斯积极推动制定网络战国际条约，希望削减网络攻击性武器，并强调各国应签订某种条约，禁止向他国电脑或网络系统中秘密植入用于未来战争的恶意代码。俄罗斯军事科学院杜列夫斯基上校认为，应将网络战纳入“侵略”、“武力或以武力相威胁”的范畴，并认为一个国家应为其发起网络战相关的非法国际行动承担相应的责任，并建议签订国际网络安全的通用协议；美国对此表示了反对。[3] 俄罗斯方面同时还建议，各国应承诺不袭击网络上的非军事目标，不通过伪装手段发动网络袭击，同时加强对互联网的监控。2009年3月，俄委任安全委员会副秘书弗拉迪米尔·索科洛夫说明了俄国在网络军控中的基本立场：在计算机系统中禁止任何国家非法嵌入恶意芯片和代码，禁止对非战斗单位和人员发起军事性网络攻击，各地政府有权对互联网进行监管等。[4] 2011年，继俄罗斯等国向第66届联大提交《信息安全国际行为准则》之后，俄罗斯又于9月22日在各国情报机构首脑闭门会议上提出了《确保国际信息安全公约》的草案，提议禁止将互联网用于军事目的，禁止利用互联网推翻他国政权，同时各国政府可在本国网络自由行动。总之，俄方试图同美国达成一个类似生化武器协议那样的国际条约来约束双方在网络世界的所作所为，以免在网络空间领域中形成“军备竞赛”。[5]

俄方的提议和构想依然遭到美国的拒绝。以美国为首的西方国家坚定维护其

---

1 Ewen Mac Askill, et al., “G20 Summit: NSA Targeted Russian President Medvedev in London ”, *The Guardian*, June 16, 2013, http:// www.theguardian.com/world /2013/jun/16/nsa-dmitry-medvedev-g20-summit.

2 卢英佳、吕欣:《2014年 世界主要国家信息安全建设盘点》,《中国信息安全》,2015年第4期，第92页。

3 转引自李健、俞赛赛:《网络空间军备控制现状及思考》,2012年1月24日,http://www.knowfar.org.cn/article/201201/24/303.htm，2016-04-06。

4 John Markoff, Andrew E. Kramer, “U.S and Russia Differ on a Treaty for Cyberspace”, *New York Times*, June 28, 2009.

5 何湘、张亚妮:《举步维艰的网络军控》,《中国信息安全》，2011年第6期，第70页。

在网络世界中的优势地位，它们把持着网络空间的议题设置和话语体系，占据上风。2012年国际电信联盟召集的“世界电信大会”上，美英联合55国抵制中俄等国对“国际电信规则”提出的修订，表面上是担忧联合国接管和控制互联网，实则是要压制发展中国家愈发主动的势头。[1] 随着斯诺登事件的不断发酵，美国迫于国际压力，于2014年3月宣布美国政府将放弃对互联网数字分配机构 IANA（The Internet Assigned Numbers Authority）的监督权。2016年3月在ICANN（Internet Corporation for Assigned Names and Numbers）第55届会议上，最终就 IANA 职能监管权移交方案及加强 ICANN 问责制方案达成共识，至此 ICANN 社群就 IANA 职能监管权移交完成了实质性的一步。但美国放弃对 ICANN 的管理权，不是把这一权力移交给联合国，而是移交给“多利益攸关方”。由此，今后以中俄为代表的发展中国家和以美英为代表的西方发达国家围绕网络安全国际行为准则和网络治理等问题将展开激烈的博弈，这也为日后网络军备控制谈判埋下伏笔。

四、结语

当前，美俄对于网络军控问题均持有自相矛盾的立场：一方面，随着网络攻击事件频发，美俄意识到构建网络规则的重要性，呼吁网络军控谈判势在必行；另一方面，美俄看重网络空间的军事作战效用，网络军备竞赛升温，网络军事化日益凸显。目前来看，美俄更加倾向于强化自身的网络军备建设，并已做出实质性的举动。对于网络军控谈判，美俄双方并没有从构建网络空间国际秩序的视角考量，因此，双方谈判很有可能形成“议而不决”的局面。

客观上讲，当前网络军备控制谈判面临许多困境与难题，包括网络战等基本概念界定存在争议，现行的国际法对网络战的约束存在盲点，归因方面难以建立有效的网络核查机制，网络军备的特殊性不适用现行军备控制等。[2] 但美俄在网络军备控制的政治取向上的差异是网络军控谈判难以推进的最大障碍。只有美俄网络实力达到相互匹敌的境地，网络军控谈判才能有效进行。再者，加强以美国为代表的西方国家和以中俄为代表的非西方国家两大阵营之间的网络互信建设和各方的网络透明化，减少网络空间的误判和攻击，是推动网络军控建设的重中之重。

1 BBC, “US and UK Refuse to Sign UN’s Communications Treaty”, December 14, 2012, http：//www.bbc.co.uk/news/technology-20717774.

2 杜雁芸：《网络军备控制为何难以施行？——基于客观层面视角分析》，《国际论坛》，2015年第2期，第1—5页。