和平發展觀察

2017 年第 1 期（总第 26 期）

中国社会科学院和平发展研究所　　2017 年 1 月 16 日

美俄网络战硝烟弥漫

陆忠伟

中国现代国际关系研究院原院长

“网络空间”与陆、海、空、天领域一样，与国防行动、军事安全乃至总体国家安全密切相关。与国家维护主权完整，领土、领海、领空安全的军事行动相对应，“网络空间”也被视为空、海、陆之外的“正式作战领域”。

目前，全世界有 100 多个国家拥有网络战实力。总体而言，网络力量对比呈现“一超多强”的格局：美国“一枝独

秀”、霸气十足，俄罗斯等国尚有差距，但奋起直追，不断缩小与“超”之差距，且拥有不对称作战的相对优势。

鉴于网络战争在现代战争中的现实性、重要性与日俱增，美俄等国均主动从国家安全战略高度审视网络空间安全态势，以及本国的涉网安全系数，不断完善国家网络空间安全战略，从而加剧了大国网络空间安全博弈。

可见，网络攻击对国家安全与发展利益的现实和潜在威胁不容小觑，威胁何在、如何应对？显然已成各国的安全要务。“多见者博，多闻者智。”当前，美俄“黑客门”愈演愈烈，对其前因后果作一多维扫描，显然大有裨益。

一、美俄侧重“主动防御”

不少网络安全专家认为，国家层面的网络攻击当属新形式战争。此类战争之特，在于“易攻难守”及“互相攻击”。这种不同于常规战争模式的特殊态势，导致网空力量强弱不同的国家或组织，均具有触发网络战争的危险——或倚强凌弱，抑或以小搏大，从而构成不同政治集团斗争的特殊形式。

网络空间安全的战略属性及美俄关系全面恶化，导致两国围绕网络空间展开的攻防愈演愈烈。“黑客门”的升级，除围绕国际话语权、网络战争规则的争夺，以及网络核心技术开发竞争等大深远的层面外，此番涉网斗争还波及政权安

全、舆情社情等领域，凸显此轮网络战的全面与综合性。

美国的网络空间安全战略最具进攻性，俄罗斯迄今在表面上强调注重防御、后发制人；但透过表象看实质，俄罗斯的网络安全战略，明里暗里带有“进攻性防御”色彩，盘马弯弓、不露锋芒，军方坚信对网络攻击采取有效反击乃降低威胁的重要手段。

从世界范围看，美俄甚或包括其他国家的网络空间安全战略，逐渐在由“被动防御”转向“主动防御”，重点打造网络空间战略威慑力量。美国大力打造三位一体的“网络威慑力”：攻防兼备的网军、开发储备秘密攻击武器，甚或必要时不惜动用常规实体军力。

美国国家安全局与五角大楼围绕即将到来的“网络空间战争”，一直谋划如何“在进攻侧加强实力以实现威慑”。2013年的爱德华·斯诺登曝光的“棱镜”项目，折射美乃“全球网络空间唯一具有进攻能力的国家”。时任美军参联会副主席詹姆斯·卡特赖特表示，今后 10 年，美军加强网络空间安全，应从全方位防御转向战略威慑；不再局限于打造更坚固的“防火墙”，而要主动侦查攻击对手，并严加防范及报复。

为了迎战一触即发的网络空间战争，美俄两国将网络战争规则视为网络空间规则体系的核心，亟欲主抓战争规则主导权，既为发动网络战争寻找法理依据；更以建章立制延缓

对方的网络军力建设。在这方面，美国联合北约推出的《塔林网络战国际法手册》，实乃为其网络战争服务的霸王条款。强权政治色彩浓厚。因大国立场迥异，决策过程充满玄机。

二、美国力争“战而胜之”

美国是网络空间战争思想的创始者，力推建设一支符合其霸权地位的新型战力。在网络空间的攻防力量及组织体制建设上捷足先登。五角大楼及国家安全局围绕“网络空间战”，一直在做“战而胜之”的准备：在网战实力的建制成军、搭建全球网络攻击和监控系统、开发可攻击性秘密网战武器等方面，不遗余力，旨在“为任何一种战争做好准备”。

2011 年美军颁布《网络空间行动战略》，提出“主动防御”和“网络威慑”两大“核心概念”。2015 年美军颁布《网络空间安全战略》，把网络空间定为“正式作战领域”，将网络空间行动作为军事冲突的战术选项，明确指出美军在网络空间的同盟、威慑、进攻能力和发展方向。

美国国防部长阿什顿·卡特称，“美军未来的作战方式会与在伊拉克、阿富汗战争的作战方式有很大不同”。言外之意，网络空间将是美军未来作战的重要领域。五角大楼于 2016 年承认，其曾成立代号“战神”的特战小组，开发新数码武器对付“伊斯兰国”，用网络炸弹对该组织发动网络战。

2010 年美国正式成立“网络司令部”（以下简称网司）。此乃美国甚或世界军事史上首个三军统一的司令部。此举折射美国对第五维作战领域的重视，以及对网络空间军事力量的集权——通过“网司”与作战司令部、各军政部门等单位的密切合作，进行“进攻性网络战”的试探研究。

“网司”成立约 7 年来，在培训网空作战分队方面进展颇大；其公开的网战部队从 2013 年的 40 支扩展至 133 支；其中分为 13 支国家任务小组、68 支保护小组、27 支作战任务小组和 25 支供给小组。这支实力雄厚的网战队伍将于 2018 年 9 月 30 日之前，全面按计划建成并投入使用。

此外，美国还在酝酿将“网司”升级为独立的司令部。目前，“网司”为战略司令部管辖，从某种意义上说，实乃为统筹而统筹，为整合而整合的急就章，解决不了统一指挥及联合作战问题。因为，“网司”没有足够权力与其他作战司令部平起平坐。各军种都不愿与平级机构分享权力。

为此，整合及调度网络空间作战能力成为当务之急。在卡特、罗杰斯等高级将领看来，单独设立“网络作战司令部”，并使之纳入国防部联合作战指挥系统，在制定预算、优先项目、战略和政策时，可有机会直接提供意见，以便“行动更迅速，更好地执行任务”。

“网络司令部”与“网络作战司令部”虽仅两字之差，但标志着美国网络空间力量建设已从思想到行动、从培训到

实战、从单兵种到大兵团作战的新阶段。加上“作战”两字，旨在调整及升级网络作战指挥机构。此乃美军网络空间作战力量体系建设的重要步伐。

三、俄奉行“格拉西莫夫理论”

俄罗斯被美视为网络空间领域的重要对手——能将 21 世纪高超黑客技术和情搜能力加以结合的一支劲旅。俄在诸如互联网基础设施与产业竞争力、网络人才储备、网战实力建军、秘密网战武器开发、涉网外交能力、国际规则主导权等方面，有较强实力。

有网络空间安全专家认为，俄罗斯民族的“战斗性”及爱国性，在独特的“黑客文化”熏陶之下，其网络空间战力不容小觑。“拥有先进的网络空间计划，对美国广泛利益构成严重威胁”；俄结合本国网络空间战略和战术能力所形成的“网络威慑力”，足以令对手掂量轻启战端的后果，并思谋避免两败俱伤之策。

2013 年，俄罗斯武装力量总参谋长瓦列里·格拉西莫夫在某专业杂志刊文，描绘了俄军绘就的网络战蓝图。该文认为，网络空间“打开了广阔的不对称能力的可能性，足以削弱敌人的战斗力”；文章还详细阐述俄军希望提升自己的黑客能力，作为常规战争和政治冲突的延伸。

这一阐释网络空间安全观的文章，被西方媒体上升到“格拉西莫夫理论”的高度。在美国国防部和国家安全局看来，早在该理论出台之前，俄罗斯即已经使用网络攻击对付邻国。例如，2008 年俄格战争爆发时，俄对格鲁吉亚发起通信阻塞网络攻击。俄罗斯的网络民兵——掌握必备设备和技能的民众——攻击第比利斯的通信、媒体、银行等信息网络，使格军不能进入重要交通枢纽、无法发布战争信息。

2016 年夏，美国副总统拜登等政要及美国情报机构扬言，“美军方黑客侵入俄电力、通信及克里姆林宫指挥系统”。俄罗斯针锋相对，公然宣称，毫不惧怕美国策动秘密网络战，声称已为此采取严密防范措施。

目前，俄罗斯海军着手推进铺设“水下互联网”。俄看到了苏联解体之后，在研发军用与民用水声学通信系统上与美西方的差距，尽全力追赶，俄海军用水下高速互联网将深水设备、潜艇、水下机器人和潜水员联系起来。特制的声学信号设备能将声音或数字信息在水下最远传输到 35 公里之外，最深传输至水下 6 公里；由于运用了独特的数据处理方法，用户能在水下随心所欲地传递数据包。

美国白宫与国会一口咬定俄罗斯黑客干扰了美国大选。中情局、国土安全部等出笼的秘密评估报告也支撑了如下看法：俄黑客在美总统选举中抛出“脏弹”，不但“黑”了民主党候选人希拉里·克林顿，甚至“黑”了美国国家利益。

奥巴马的国土安全和反恐顾问萨莉·莫纳科表示，黑客事件的严重性已跨越“新门槛”——不可接受的“侵略性骚扰”。

四、世界“正经历首次网络战”

2016 年 12 月 30 日，英国老牌纸质媒体《卫报》刊文认为：当今世界“正经历第一次世界网络战争”，“战争的时间线可以 2007 年为起点”：当年，爱沙尼亚遭密集网络攻击；2010 年，伊朗核项目受到称之为“震网”的蠕虫病毒攻击；同年，维基解密网站公布美国使馆的电文；2014 年美国联邦调查局指责朝鲜对索尼影像娱乐公司实施网络攻击；2016 年，号称韩国军事情报“神经中枢”的国防部数据中心服务器被黑客攻破。

实际上，2010 年以来，美军“网司”即已对盘踞伊拉克、叙利亚两国的极端势力展开网络战。不少案例显示，这种网络战争已非简单的情报配合或信息保障，网络攻击构成打击极端势力的核心作战。2015 年，美国“网司”对“伊斯兰国”也发起网络攻击行动。可见，网络空间战场早就“硝烟弥漫”、“战火绵延”，只是听不到震耳欲聋的枪炮声罢了。

针对 2015 年美国对 IS 发动的网络攻击，华盛顿著名智库——新美国基金会的网络安全专家彼得·辛格坦承：“我们不仅在使用这种能力，而且还承认正在使用这种能力；这

是网络战正常化的一部分，此乃历史性时刻”。

北约秘书长斯托尔滕贝格 2016 年曾扬言，若北约成员国遭受大规模网络攻击，或会作出集体回应，“就像防御来自陆、海、空领域的攻击一样”。这两段言论，从不同方面对世界网络战争做了最佳注脚。

2017 年 1 月 7 日的美国参议院听证会上，国家情报总监詹姆斯·克拉珀代表 17 家情报机构表示，坚信俄对两党全国委员会、白宫和国务院发起网络攻击，窃取数千份民主党全国委员会的电子邮件，由化名“古奇弗 2·0”的黑客提供给维基解密网站。此外，还有美国网络安全专家称，在侦破的黑客使用的 8 个 IP 地址中，6 个来自俄罗斯的国王服务器公司。据情报机构拦截的通讯记录显示，俄高官庆祝特朗普获胜。

美国情报机构认为，“从黑客攻击的规模和敏感度判断，惟俄最高层才能批准”。两党领袖口诛笔伐，将之上升到“破坏美国网络安全”的高度展开调查。围绕“黑客门”事件，美俄从“外交战”升级为“网络战”。公开材料显示，早在 2016 年，中情局即已获指令：筛选袭击目标、开启网络端口、提交作战方案，做好对俄网战准备，对攻击源头（计算机服务器所在地）采取秘密反制。

特朗普对俄黑客干扰大选的结论一直抵制。但 2017 年 1 月上旬，特在听取情报机构秘密调查报告后承诺，在就职 90

天内制定网络反制计划。特朗普态度急剧拐弯，或是认同了简报关于俄黑客掌握了其材料的结论。

美俄均系全球网络安全实力最强国家，俄被美视为网络空间领域的重要对手。两国围绕“致人而不致于人”势将展开殊死攻防，美国或将升级对俄的政治经济制裁，甚或网络空间真刀真枪反击，对国际网络空间安全产生深远影响。

五、美俄网络战回响深远

“知己知彼”是兵学大家孙子对无数次战争的概括、总结，抽象出的重要概念。关于“知战”的论述，具有全维认知的性质。换言之，“识虚实之势，则无不胜；鲜识虚实，反为敌致”。而今，网络空间安全——网络空间中的国家安全问题，上升为战略界的关注重点。

美俄此轮网络空间较量，也给人留下颇多思考。美国力推符合其霸权地位的新型战力建设，不失为各国网络力量建设的他山之石。美国是“全球网络村”中的强龙。其在网络空间攻防力量、安全战略、合作政策及体制建设等方面，捷足先登，引领潮流，或将为大国网络力量建设借鉴。

于国际政治而言，网络空间乃极富地缘战略价值、关乎国家安全的战略博弈工具。由于互联网落胎于美国军事科技领域，美国军队是在互联网“马背”上发展起来的，美国倾

力紧抓该领域的掌控，大力推进新质战力建设，也已引起各国高度重视，或激活一轮建设“主动网络防御”的网络“军备”竞赛，发展“合法”的网络攻击能力，打击和威慑来自外部的侵略性威胁。

欧盟和北约担心俄罗斯对美网络袭击或是对欧网络攻击的前奏，为汲取教训、未雨绸缪，荷兰、德国和法国等国政府正在抓紧工作，推动盟国加强相关涉网空的规划，统筹资源、训练人员，加强自身网络防御能力，促进欧洲集体网络防御能力建设。

日本政府作为“战略创新创造项目”的重要一环，决定在 2017 年度斥资 25.5 亿日元（约合 2162 万美元）经费，促进大企业的研发合作，针对输电网、铁路运行控制系统等方面开展专项技术研发，加快网络防御系统技术装备的国产化，以便对网络攻击给予更快速应对。

综上所述，“网络空间正成为大国竞争的主战场，网络空间安全成为国家战略的重中之重”。让网络空间更安全是国际社会的共同责任。中国思想、中国方案正在引领、影响网络空间的未来。“应之以治则吉，应之以乱则凶”。

（责任编辑：刘琨仑）

稿 约

《和平发展观察》是展示和平发展研究所动态的窗口，也是业界同仁交流思想和研究成果的平台。欢迎各位同仁围绕影响当代和平发展的国际国内重大问题，自选题目，惠赐佳作。希望来稿以学理为基，以形势、政策研究为干，立足解决当前现实问题。观点鲜明、立论有据、逻辑清晰、简明晓畅、直奔主题，字数以 5000 字为宜。来稿一经采用，稿酬从优。

来稿请邮：hpfzs@cass.org.cn

请勿一稿多投，两周内未收到回信可自行处理。

和平發展觀察
执行主编：廖峥嵘
中国社会科学院和平发展研究所
地址：北京市海淀区北洼西里颐安嘉园 11 号楼
邮编：100089　传真：010-88515507
电话：010-88515505
邮箱：hpfzs@cass.org.cn
发刊日期：2017.1.16