网络战的艺术：超限战争的典范

布赖恩•M•马赞内克 撰文
石海明 译

布赖恩•M•马赞内克是国际《科学研究文摘》的一位高级情报分析师，曾在美国情报界、参谋长联席会议联合参谋部、国防部部长办公厅、国防威胁削减局和国土安全部担任不同职务。

美英两国近日发出了筹划应对网络战争的强烈信息，其中，美国在一份战略报告中将网络攻击视同“战争行为”，宣称要用传统军事力量“对等”报复来自互联网的攻击，“如果你关掉我们的电网，我们也许会向你的烟囱里扔枚导弹。”英国则选择发展网络武器针锋相对，英国官员2011年5月30日首次证明了这一计划的存在。而就在5月25日，我国国防部也证实，广州军区为提高部队网络安全防护水平建立了“网络蓝军”。消息一出，西方舆论又掀起一片质疑与责难之声：这个“网络蓝军”是否就是网络部队？网络战争究竟是什么样子，目前学界仍众说纷纭，但美国、英国等西方国家对网络军事化的关注与渲染，却颇值我们重视。布赖恩•M•马赞内克撰写的“网络战的艺术”一文，对我国网络空间发展战略进行了猜测与剖析。尽管有诸多不客观之处，但却有助于我们了解国外学者的思维和想法。实际上，考虑到美国在诸多国际问题中所表现出的霸权主义和双重标准，我们认为，文中阐述的中国对美国网络基础设施的战略突袭，在现实中可能恰恰相反。而作者提出的美国的应对之道，对我们也具有参考价值，这也恰恰是本刊编发此文的一个初衷。

有关网络空间的主导权问题正日益引发中国的关注，这种关注不仅聚焦于中国如何提高自己传统的情报搜集能力，而且旨在谋求一种新型的军事作战力量，一种对他国经济和关键基础设施等领域的有效打击力。

换而言之，中国当前对网络空间的严重关切，目的在于谋求获得一种网络作战能力。在美国国防部今年提交国会的“中国军力报告”中，相关人员就明确提到了，“中国军力发展的重心正在从传统的陆、海、空等物理空间向网络空间进行拓展。”对中国网络战这种整体战略的深刻理解，将有助于我们更好地洞察，中国军队未来发展的走向及企图。尤其是考虑到当前美国（无论是军方还是民间）严重依赖网络这一现实，上述这一点的战略意义就更加凸显了。

中国网络战争的根源

就某种意义而言，当前中国对网络战的关注，是其传统军事战略思想的延伸，如可追溯到孙子的“以弱胜强”思想以及毛泽东的“人民战争”概念。当前中国军事战略思想的变革，与其不断拓展的地缘战略利益密切相关，如维护政权的生存，主导亚太区域，增强全球影响力，以及防止台湾独立并最终完成国家统一。

自20世纪90年代早期以来，网络战已经成为中国军事战略的核心思想之一。在1991年，透过美伊之间的海湾战争，中国领导人不无痛苦但又极其清晰地认识到，高科技对于打赢现代战争至关重要。可以讲，哪支军队拥有信息优势，哪支军队就能轻而易举地战胜对手。正是在这种背景下，中国的军事战略专家迅速接纳了“军事革命”这一概念，认定未来的战争将不再仅仅是比拼火力，转而变为制信息权的较量。考虑到在未来的一场中美军事冲突中，中国不太可能从正面击败美国，于是，在1999年，两位中国空军的大校军官——乔良和王湘穗——系统阐述了“超限战”思想，认为未来的战争将“超越一切界线和限度”，并且提到网络空间的利用也将在未来军事冲突中扮演重要角色。

10年后的今天，中国军事变革的成果是惊人的。尤其是在近年来，依托其快速发展的国家经济，中国在网络空间的作战能力得以逐步增强。正如美国国防部主管亚太安全事务的助理副部长理查德·劳利斯在2007年所指出的：“中国在网络空间的军事实力已经从单纯的防御他国攻击转变为有能力对他国发起攻击，在这种巨大的转变背后，中国蓬勃发展的经济显然起到了至关重要的作用。”

我们很难评估中国的网络战能力，不过，可以肯定的是，中国一定在网络战的相关领域投入不少。同样明显的是，他们的投资目前正在逐步增加。根达特茅斯学院技术安全研究所2008年的一份研究报告显示，在美国的潜在竞争者中，中国在网络战方面已经独立发展起了全面的实战能力。

1. 2010年5月21日，美国网络司令部形成初始作战能力。

当然，中国并非是在一夜之间就获得这种能力的。他们对网络战关注的兴趣导致了对其持续的、倾向性的投资。早在2003年，中国人民解放军就已经建立起它的第一支网络战部队。从那时起，中国就主要通过经济手段迫使IT类公司（尤其是微软）解密有关计算机软件及应用方面的敏感信息和专有信息。这些信息使中国人民解放军能在微软开发出一些应用程序的补丁之前就掌握了一些软件的安全漏洞。此外，它还大大加强了中国通过植入恶意软件搜集敏感信息，以及对网络和基础设施进行攻击的能力。

或许，能展示中国网络战能力蓬勃发展的一个最好案例，就是“泰坦雨”（titanrain）网络攻击事件。“泰坦雨”发生在2003~2005年之间，在此期间，美国政府的数百台计算机以及美国和西欧盟国联接的计算机网络遭到了全面入侵。据美国一些媒体报导，发起网络侵袭的3个路由器都来自中国广东。尽管这些网络攻击造成了一些破坏，并对美国的国家安全构成了严重威胁，但把这些间谍性质的攻击与若隐若现的大规模网络攻击相比时，就会发现前者还真算不了什么大麻烦，后者正致力于超越网络间谍的功能，试图在通过网络空间的攻击达到与现实世界中一样的军事作战效果。

为什么发动网络战？

我们认为，中国通过网络战达到军事作战效果的兴趣开始于战略威慑。其目的不是吓阻其它国家对中国发动网络战，而是想利用网络战的威慑效果，慑止那些试图挑战中国国家战略利益的国家。当然，在短期内，中国的主要聚焦点是台独问题。中国试图利用网络战阻止美国军方介入台海冲突。就威慑效果而言，网络战威慑战略的一个优点是，相对于其它战略武器威胁（如核武器威胁），它是一种更为实际的战略威胁。中国不会利用其有限的核力量来阻止美


1

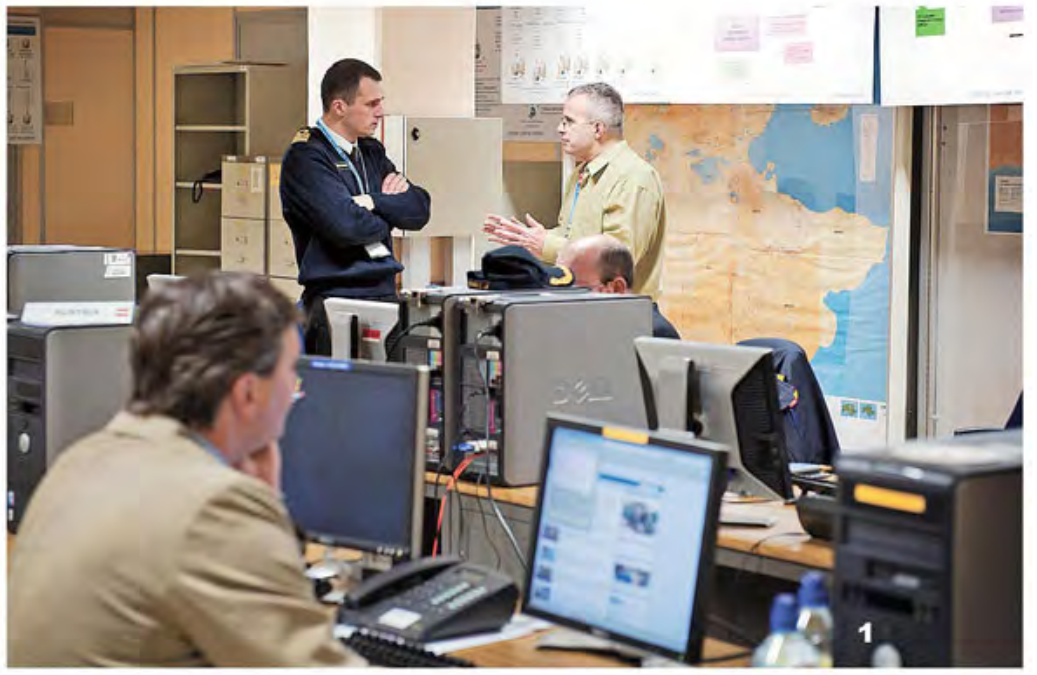
国染指台海问题，尤其是在其宣称不首先使用的核武器的政策约束下。但是，作为一种较克制的报复性反应，中国发起一次战略性的网络战攻击，因为较少受到国际舆论的指责，这是完全可能的。此外，网络空间归属性的问题也给了袭击发动者一个否认机会，这就使得网络战更加具有吸引力。于是，中国培育起一支管理较为松散的“反台独黑客”，他们被称作21世纪版本的毛泽东“人民战争”力量。显然，中国因此而获得了一种网络战战略威慑力量。

传统的威慑理论主要是围绕核战争而构建的，但其应用却能够扩展到今天的网络战。在冷战期间，美国和苏联采用了一种“确保生存”的核力量理论，以保持一种适度的、可信的威慑。这种理论先是由赫尔曼·卡恩提出，后来被托马斯·谢林（因《冲突的战略》一书而获得诺贝尔经济学奖）所发展，其意义在于保持一种相对的战略平衡。这种做法虽然存有争议，但却通过大规模核报复–相互确保摧毁的恐怖平衡防止了世界大战的爆发。当然，威慑既可以是进攻性的，也可以是防御性的。

人们在评价中国的网络战威慑能力时，往往会关注其网络攻击力。威慑要真起作用，威慑的对象就必须是一个理性行为者，美国就是如此。实际上，美国社会和政府决策的内在透明，保证了在一场军事冲突中（如涉及台湾的冲突），美国对威慑是可以认知的。威慑目标可分为“反击军事目标”和“反击价值目标”两种，前者以军事目标为对象，后者以民用基础设施、民众或对方其它任何有价值的设施为对象。中国相信，网络战威慑对这上述这两种目标都能起到明显的战略威慑效果。然而，中国的网络战威胁还不仅仅局限于威慑敌对国家——如美国——的军事目标和一切有价值的目标。为达到以上所讨论的威慑效果，中国还有在威慑失效以后实施惩罚或采取实际行动的准备。在以下3种冲突中，中国必然会这么做。

对台作战

最有可能的一种情况就是对台作战。在军事冲突发生的情况下，解放军一定会对台湾的防御系统实施快速打击，同时拖延美军进入台湾海峡的时间，并在他们到达的时候，削弱其作战能力。美国的中国网络战专家詹姆斯·马尔韦农简述了可能发生的情况：“对解放军来说，针对美国的信息作战系统打信息战，以削弱甚或迟滞他们在台湾的军事力量部署，这是一种有吸引力的非对称战略。美国武装力量体系高度依赖复杂的信息系统和物流供应网络……如果解放军的信息作战力量能够侵入甚或破坏这些系统，从而延缓美军航母编队到达事发地，同时对台湾的核心目标，实施一场近程弹道导弹、“第五纵队”以及信息战协同攻击，那么，台北很快就会向北京屈膝投降……“



1. 2010年11月16~18日，来自25个北约成员国的计算机专家实施了“赛博联军2010”的网络电磁防御演习，内容包括网络电磁事件响应，跨局合作以及战略决策。

在中国看来，美国的后勤系统是其军事力量链条中最薄弱的环节，而且在战争的最初阶段也最易被攻击。因此，中国有限的网络战力量一定会以美国的后勤系统作为主要攻击点。这种“先发制人”式的针对性攻击，可以说是中国军事战略中“在敌人之前掌握主动权”的体现。如此，中国发动的网络战就可以通过减缓美国援军的来达，达到使解放军对台湾军事力量的局部压倒性优势。

此外，由于美国对作战人员伤亡的极端厌恶，以及对所谓“鲍威尔主义”的迷信，美国必定会谋求依托对敌绝对优势的兵力来取得速胜。因此，除非部署更多的军事力量并建立起完善的物资供应系统，否则美国不会大规模展开军事行动。而这可能最终会使美国白白送给中国一个星期或更多时间，从而使中国获得控制台海的绝佳机遇，相对应的，美国介入台海冲突危机的代价自然就变大了。

假如这种“先发制人”的攻击不能成功，中国可能就会放手利用网络战直接攻击美国的军事技术体系。这种攻击将集中于美国所依赖的准确的、实时的信息系统，譬如C^4ISR系统。

中国对这种战术的运用是毛泽东主席那句名言的升级版，中国必须“封住敌人的眼睛和耳朵，使他们成为瞎子、聋子，并尽量迷惑他们的指挥官，令其变成疯子，以此获得胜利。如果我们没有忘记克劳塞维茨所言的“战争迷雾”的话，中国的这种军事理论将有效地对增加美国军队的战争迷雾，而使中国军队的战争迷雾减少。

亚洲的地区性冲突

中国人民解放军提高网络战作战能力的背后有美国的因素，但不仅仅是针对美国的。由于中国还可

能会与美国之外的其它国家发生有限战争，显然，在那些场合，中国针对美国的这些网络战作战能力也将会给它提供军事优势。

印度是中国在区域范围内最有可能的敌人。中国和印度的政治紧张局势始于1962年发生在喜马拉雅山争议地带的战争。当时，中国人民解放军对印军取得了决定性的胜利，但是此后小规模的军事冲突却一直持续到了20世纪80年代后期，相关争议问题至今仍悬而未决。20世纪90年代中期，中国与印度签订了中印两国国家安全和平协议，抑制了“实际控制线”一带军事冲突的爆发。尽管如此，解放军仍然在不断加强对这一地带的控制。在这两个快速崛起的经济巨人之间，未来肯定还会发生冲突。

印度是一个越来越依赖网络高科技的国家。它拥有6000万以上的网络用户，而且其增长速度超过中国。印度经济令人瞩目的增长得益于全球化进程及其与世界其它国家在网络和计算机领域的可靠联系。如果中国能够在网络空间有效地对印度的民用目标实施网络战威慑，它就有能力成功地吓阻印度损害其国家战略利益。如果威慑失效，中国依然有能力打击印度经济的增长，使其丧失抵抗意志。

新德里的军事体系也很脆弱，是一支现代化程度较低的武装力量，它拥有所有可能的弱点。显然，印度的军队不可与美军同日而语。中国解放军显然能够利用其网络战能力攻击印度军队的弱点，而这将是中印之间一场有限的局部战争的一部分。在边境争议地带之外，潜在的印巴军事冲突中，中国还有可能在使用其网络战能力或明或暗地帮助巴基斯坦。中印两国军事冲突的可能性会随着两国在未来10年中相对力量的变化而增大。

伴随着印度谋求成为一支有影响的全球武装力量，其对网络空间的依赖将日益加剧，对此，中国的网络战实力将使其在未来的中印军事冲突中获得优势和益处。总之，中国的网络战实力，将不仅为其在与美国和印度的冲突中提供战略优势，面对任何可能和中国发生冲突的现代化国家，中国的网络战实力都将使其在冲突中保持战略优势地位。

全面战争

中国对网络战作战力量的充分运用，很显然地会发生在一场与美国的全面无限战争中。这场军事冲突将会全面展示中国人民解放军传统战争和现代非对称战争方面的水平，甚至还可能包括核力量的运用。当然，我们必须认识到，这种情况发生的概率很小。根据美中经济与安全审查委员会的说法，中国领导人相信，未来的战争“将发生在有限的地区、时间，具有有限的政治目的，并将强烈依赖于指挥、控制、通信和计算机（C4系统）。不过，考虑到这种中美两国军事对抗的灾难性后果，无论其多么遥远，都值得认真加以研究。

对中国而言，中美两国全面战争中的战略网络战，将是一个以美国本土为目标的一个巨大的网络战场。早在2001年，美国计算机紧急响应小组(US-CERT)的高级分析师和北约组织，曾联合发表了一篇文章，强调了这一分布广泛而又不受限制的战略网络战的特性：

这样一个不受限的网络空间战场，将包括目标国家的关键基础设施、能源、交通、金融、供水、通信、应急服务以及信息基础设施等众多方面。它将很可能跨越政府和私人部门的界限，并且，如果关联足够复杂，将同时产生直接的战争效果和后续的持久影响。最终，不受限制的网络袭击将导致大量伤亡以及经济和社会的全面衰退。

这样一个战场将会以什么面孔出现呢？早在2002年，美国网络防御研究小组——一个私人网络安全研究群体就专门组织模拟了一场真实的对美国的战略性网络战攻击。他们给这一模拟攻击起名叫“黑天使”，该模拟演习假设敌方拥有一定的经费（5亿美元），并致力于扰乱美国社会，削弱其军事力量，瓦解其抵抗意志。“黑天使”被用来攻击铁路交通系统、石油和天然气管道、难以取代的电力基础设施、金融服务系统和应急服务系统，就像“9·11”那样，它旨在导致通用网络系统失效，进而打击美国。

中国的网络战很可能会像“黑天使”这样展开，并且不受诸多限制的约束。在与美国的全面战争中，中国可能不再需要掩饰其行动，并全面运用其网络战攻击能力（甚至远远超出“黑天使”的能力）。如果没有在金融和政治方面的限制，中国将竭力破坏尽可能多的网络基础设施，使美国的经济陷入混乱，从而消解美国打持久的全面战争的能力和意志。这种攻击很可能会为前面我提到的中国人民解放军倡导的“人民战争”注入新的活力。

此外，中国还拥有超过2.5亿互联网用户，他们当中的许多人都可被雇用为“爱国黑客”，他们的计算机也可被政府用来作为分布式节点攻击系统的一部分。所有这些个人和计算机都可以参与一场战略网络战的首次打击，一举击溃美国，就像几十年前日本人袭击珍珠港那样。中国还可以通过基于电子战的网络战，或者运用非核武器甚或电磁脉冲武器，达到放大这些网络攻击效果的目的，从而对北美的关键基础设施进行隐蔽性攻击。

此外，由于全世界计算机和网络系统都是互相联通的，这样一次袭击事件的影响将波及全球。在与美国的全面战争中，这样的战略网络战袭击将破坏关键的基础设施，并使美国经济遭到毁灭性打击，但是它们最严重的影响恐怕还在于对美国民众的意志的摧毁。通过造成一场遍布美国的服务系统——动力、应急反应、视听等系统——的失效，它将使民众对美国政府产生信任危机。人们将对其个人财产和养老金的安全性、稳定性产生担忧，而社会的不稳定将进一步导致囤积居奇，这又将起到一种放大器的作用，使本来严重受损的国家基础设施雪上加霜。显然，中国将能够借此发动一场针对美国的秘密的战略心理战，从而把美国社会推向彻底混乱的边缘。

要做的反应

通过以上论述，我们不难发现，中国对网络的兴趣远远不止仅仅把它作为一个情报工具。中国热切地希望通过提高网络战作战能力，取得在战略威慑、有限战争甚或无限战争中的军事优势。我提到的这些情况，以及中国相应的网络战作战能力，值得美国国防规划人员和高级领导人严重关切。

我认为美国的应对举措，应该从对网络的全面保护开始。这一步是必须的，因为网络战的作战效果全球可及，所以必须迅速做出反应。为了达到全面而有效的防御效果，就需要在众多国家组成的联盟以及众多不同层次之间开展联合作战行动。这一建议得到了美中经济与安全审查委员会的采纳，该委员会在其2007年的一份报告中说，国会应当“敦促政府基于联盟来促成各国联合应对中国的网络攻击。”

这种多边联合防御计划的好处在于，与美国的联盟将不会耗费如提高传统军事能力那样巨大的投资，就可以达到效果。它只要相关网络信息系统在授权访问、修改信息等方面进行适当的技术变革，就将起到巨大作用。显然，这对许多北约成员国是一个受欢迎的消息，这些国家的预算已经由于应对人口结构的变化和巨大的社会安全问题而显得捉襟见肘。

事实上，这样一场联合军事防御行动已经出现了。继2007年俄罗斯对爱沙尼亚的网络战攻击以来，北约已开始投资于网络空间的防御。尤其是在中国网络入侵迫在眉睫的威胁情况下。盟国有更多的网络安全需要公开承认、协商并寻求应对。这些前期的尝试做法，将会被那些旨在赢得未来网络战的国家日渐认可，并逐步推进下去。毕竟，在世界网络一体的情况下，单独地面对网络战将比单独地面对传统战争更加危险。

与此同时，美国也需要承诺未来会加强保卫台湾。目前美国对保卫台湾的态度非常模棱两可。“台湾关系法”也未能对其提供明确的安全承诺，仅仅是声明任何对台湾的威胁将引起美国的“严重关注”。有人说这种模糊的承诺是有用的，因为它给华盛顿提供了一个“战略模糊”的必要，使美国能够灵活应对各种情况。然而，这种模糊性将被中国认为，“对美国而言，台湾并非如冷战时期的欧洲那样。”我们需要重建一个类似1955年共同防御条约一样的协议，以此给中国一个强烈而明确的信号：不论解放军在网络空间或其它领域具有何种打击能力，美国都将保卫台湾。

此外，就台湾来说，为减少误判的可能性，美国应当努力形成一个“宣言性质”的政策，以确保美国在应对与其自身利益相关的网络战时，有一个清晰的战略思维。这一政策应当不只承诺一种类型反应——以网络战回应网络战，还应当包括全面的军事应对措施。它将给世界发出这样一个信号，即美国对网络战可能给其国家关键基础设施造成威胁的考虑，和对传统大规模杀伤性武器相关威胁的考虑，给予同等的重视。就核武器而言，战略模糊性在冷战时期，面对以常规武力占优的苏联，还是有用的。但是，如今网络战的威胁，要求美国做出更明确回应的保证。这一政策还应包括一项明确规定，即窝藏“独立的”网络战袭击者就意味着对美国的军事进攻。

1. 2011年2月1日~3月4日，驻德美军进行了名为“恶魔闪电”的计算机网络演习，旨在评估作战网络的可靠性、灵活性，图为2名美军士兵在网络控制中心进行操作。

当然，美国也应该与中国直接对话，以便全面探讨美国对网络战如何做出反应。这种双边对话应该包括一些重要议题，诸如威胁削减机制、战争法。就后者而言，特别需要指出是，战争法如何应用于网络战及其它可能存在的威胁问题。

也许强调应对中国网络战威胁最显而易见的建议，就是加强美国在网络空间的攻防能力。在美军中，美国战略司令部是全球网络作战的整体规划协调者，且据称已经在其联合特遣队——全球网络作战司令部的指导下寻求更强的网络攻击能力。目前，美国空军司令部（其网络战任务最近得到了重新部署）、海军网络部队司令部和临时成立的陆军网络战大队的军事设施都在与美国网络战专业力量合作，致力于建立一个持久的跨部门联合机构，以应对网络战威胁。因为在网络空间，最好的进攻就是防御这一道理相比其它领域更甚。

最后，美军必须继续革新以促进其自身的灵活性，从而使其军人能够在信息战或网络战袭击导致信息设备失效的情况下也能够积极应对，做出敏捷的反应。这一努力可以被视为，是对原来依靠网络的全体战士的一种能力的强化。此外，老式的印刷性实地手册、电话、铅笔、图纸必须仍然能够保持使用，尽管效率低下，但也能够在系统被网络战进攻摧毁的情况下继续发挥作用。对这些“B计划”战术，我们更应该经常进行演练。

正如国防部长罗伯特·盖茨最近所告诫的，美国应该对我们用来实现目标而且也能实现目标的所有技术保持谦虚态度：“……精确度的优势、传感器、信息与卫星技术已经使美军获得了传统军事能力之外的力量……但绝不要忽视心理、文化、政治和人的因素，它们可能会带来悲剧性的、低效的和不确定性的影响。”罗伯特·盖茨的建议尽管不是针对网络战，但也应该被那些致力于避免或减轻对美国进行电子攻击效果的人们牢记在心。

严肃对待网络战

来自中国的网络战威胁是实实在在的，并且还在不断增大。美国不能对来自这个亚洲竞争者不断增长的非对称性威胁视而不见。强有力的证据表明，中国的网络战作战力量，将在技术的复杂性和攻击力的强度，以及外空网络防御措施等方面加大力度。中国对网络战的兴趣已经从情报的搜集扩展到在战略和战术两个层面破坏美国的企图，旨在谋求获得非对称性军事优势。而且，北京在这方面的投资也不会减少。所有这些都使得美国对网络空间攻防能力建设的持续性投资成为必要，以便保护美国的国家安全，以及美国在这一领域行动的自由。