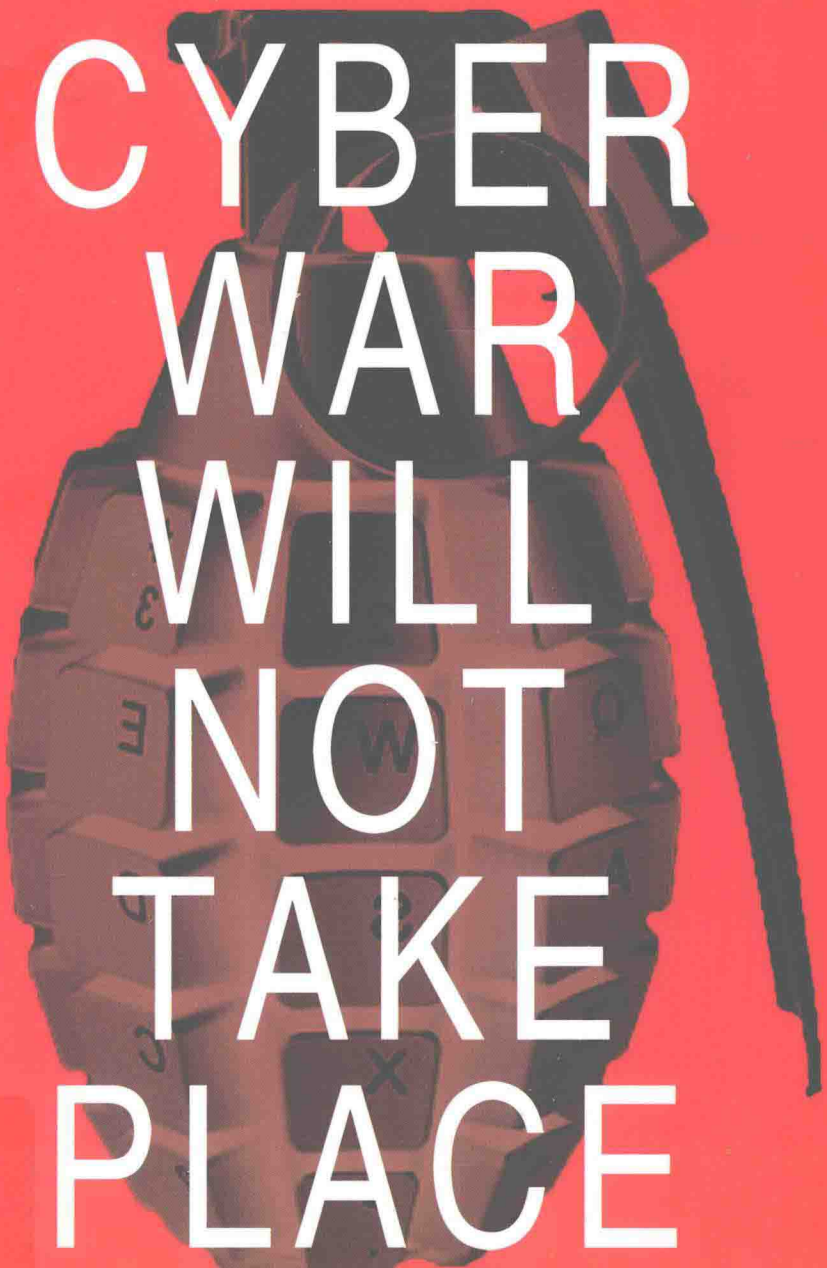
网络战争：不会发生

[英] 托马斯·里德 著　徐龙第 译

THOMAS RID

CYBER WAR WILL NOT TAKE PLACE



人民出版社

网络战争：不会发生

[英] 托马斯•里德 著　徐龙第 译

THOMAS RID

人民出版社

图书在版编目（CIP）数据

网络战争：不会发生/（英）托马斯·里德（Thomas Rid）著；徐龙第译. —北京：人民出版社，2017.5
书名原文：Cyber War Will Not Take Place
ISBN 978-7-01-017413-6

Ⅰ.①网… Ⅱ.①托… ②徐… Ⅲ.①计算机网络—应用—战争—研究 Ⅳ.①E919

中国版本图书馆 CIP 数据核字（2017）第 039402 号

网络战争：不会发生

WANGLUO ZHANZHENG：BU HUI FASHENG

[英]托马斯·里德（Thomas Rid）著　徐龙第 译

责任编辑：曹　利
出版发行：人民出版社
地　　址：北京市东城区隆福寺街 99 号
邮　　编：100706
邮购电话：（010）65250042　65258589
印　　刷：环球东方（北京）印务有限公司
网　　址：http://www.peoplepress.net
经　　销：新华书店
版　　次：2017 年 5 月第 1 版　2017 年 5 月北京第 1 次印刷
开　　本：710 毫米×1000 毫米　1/16
印　　张：15
字　　数：258 千字
书　　号：ISBN 978-7-01-017413-6
定　　价：36.00 元

前　言

网络战争（cyber war）的威胁已引起人们的想象。好莱坞迅速意识到人们的这些担忧，并为我们将之呈现出来。《战争游戏》（1983 年）和更近的《虎胆龙威 4.0》（2007 年）等影片走的都是明显的叙事路线：黑恶势力利用神秘而复杂的计算机网络肆行暴虐，把整个国家劫持为人质，并通过侵入五角大楼庞大且功能强大的计算机系统发动核战争。这种担忧深深地触动了人们的神经。我们大多数人都使用电脑，但并不真正了解硬件和软件是如何进行交互的。人类因对技术本身失去控制而导致的焦虑无处不在，这有力地体现在斯坦利·库布里克（Stanley Kubrick）的《2001 太空漫游》（1968 年）中宇宙飞船所载的可怕而控制一切的计算机“哈尔”身上。随着越来越多的人和物上网，这种担心比以往任何时候都更深了。

无论是年轻人还是老年人，大多数口袋里随时都揣着智能手机。很多人都上网成瘾，不停地、有时偷偷摸摸地查看电子邮件和社交媒体资讯，比如在饭桌上、沙滩上、商务会议的桌子底下（并非只是在那些无聊的商务会议上才这样）。整整一代人已成长起来，他们相信自己的个人和职业福祉将依赖于数字设备和持续的连网。在早咖啡准备好之前，如果你在摆弄触摸屏，那么你可能凭直觉就能理解，几乎所有使你在接下来的一天中所发生之事成为可能的东西都由电脑控制：水龙头流出的自来水，为水壶提供电力的电厂，帮忙过马路的交通信号灯，上班乘坐的火车，可

以取钱的自动取款机，在办公室使用的电梯，到柏林、德里或纽约的飞机，在不太熟悉的城市里用来寻找方向的导航系统，等等。只要这些都正常运行，生活的所有这些特征目前都司空见惯，并不引人注意。同样司空见惯而暗含危险的则是人们无处不在的担忧：恶意行为者埋伏其中，随时攻击和摧毁这些计算机及其运行的软件，从而使整个社会臣服。水停止流动，交通信号灯熄灭，列车出轨，银行丧失我们的财务记录，道路陷入混乱，电梯发生故障，飞机从空中坠落。俗话说，无人能免于这场即将到来的网络战争。我们的数字死亡只是一个时间问题。

这些担心转移了人们的注意力，偏离了网络安全（cyber security）的真正意义：在几个方面，网络攻击并未制造更多维度的暴力性互动；相反，它们却使之前暴力性互动的暴力性降低。只是在21世纪，武装力量才有可能摧毁敌方的雷达站和导弹发射器，而无须轰炸其防空系统并在此过程中杀死其人员，可能还有平民。现在，这可以通过网络攻击来完成。只是在21世纪，情报机构才有可能通过计算机攻击潜出和下载大量的机密数据，而不用派间谍到危险之地去贿赂、胁迫并可能首先会伤害信息员和信息源。只是在21世纪，反对派和叛乱分子才可能在网上动员勇于献身的支持者，让成千上万的人走上街头，而不用通过扩散暴力和恐惧来破坏政府对权力的控制。

网络化计算机（networked computers）的普遍兴起正在改变士兵、间谍和颠覆分子的业务。网络空间正在创造新的——经常是非暴力的——行动机会。但是，这些新机会也有其局限和挑战，这对那些试图抵御新攻击途径的人以及那些力图把新技术用于进攻目的的人同样适用。本书探讨了网络空间对那些把暴力用于政治目的的人来说所创造的机遇和挑战，而无论他们是否代表政府。

复杂计算机侵入（computer incursion）的兴起构成了重大风

险和威胁，了解这些风险和威胁并制定适当的对策来减轻它们是至关重要的。因此，在这里简单地说说不断发展的有关网络安全的讨论是适当的：关于网络安全的讨论存在缺陷，并且在许多方面其质量都低得可怜。更多的讨论发生在技术期刊、杂志、专业的网站论坛，当然也发生在主流媒体和学术界，以及博客和微博上。这些讨论也发生在无数的会议上，它们汇集了来自私营部门、政府、情报机构和军方的代表，以及黑客和不同学科的学者。这些讨论既发生在公开场合，也发生在闭门和保密场合。毫无疑问，来自不同背景的精深专家定期发表高质量的网络安全研究成果，倘若不使用他们的良好作品，本书可能就无法完成。但是，与政界、军界、智库、议会、部委、军事院校的接触越多，真正的专家似乎越少，夸张的调门似乎越高。一个古怪专业术语的出现——“网络”（cyber）一词越来越多地被政策专家和许多军官用作名词——极好地说明了政策讨论滞后的特征。例如，“我对网络感兴趣”或“网络的定义是什么”。我在英国议会的演讲中建议**不要使用**这个空洞而时尚的流行词作为名词，之后，一名公务员曾诚挚地向我提出上述问题。请注意，计算机科学家、程序员或软件安全专家都不倾向于把“网络”用作名词，技术记者和严肃的学者也不这么用。我逐渐对“名词使用者”极不信任，因为他们往往似乎只是不懂必要的技术细节，这种现象在华盛顿随处可见，在伦敦、巴黎和柏林等地也是如此。因此，提高讨论的质量也就更为重要。与迄今的讨论相比，公众应得到有更多信息、更细致入微、更实事求是的讨论，公众也应拥有更为深思熟虑和执行得更好的网络安全政策和立法。

本书志在向读者提供扎实而易于理解的著述，并试图巩固这场讨论，减少一些炒作，充分面对一些最紧迫的安全挑战。本书旨在成为学生、分析师和记者的参考来源。有关网络安全的专家讨论和讲授课程散布在各个学科，其中最重要的是政治学和计算

机科学，法学和社会学紧随其后。我希望，无论是哪个学科的读者都能发现本书富有洞见：工程师、极客（geeks）和技术爱好者可能会从其战略性“鸟瞰”的视野中受益；政策分析家和社会学家可能会从其通俗易懂的技术细节介绍中获益；而无论是哪个领域的学生对两者都能理解。但是，没有哪个作者甚至会希望涵盖网络安全的全部内容，我的长长的致谢就清楚地说明了这一点。为使本书更加易懂，其中的七章都可独立成章，每章都有各自的问题、论证以及说明某个观点的微型案例研究。

关于本书使用的资料来源，最近有关网络安全进展的最启发思考的讨论并非出现在学术期刊上，而是出现在许多技术博客上，以及其他不能称为博客的网站上。一些最重要的长篇论文和报告也未发表在根据既有学术惯例可以加以引用的期刊上，而是发表在公司网站上，有时是在个人网站上。我一般引用常用的详细信息，包括作者姓名、篇名、出版物和出版日期。读者可以通过谷歌搜索快速地找到这些资料。只有那些难找的条目才配上一个网址（URL）。但是，由于许多网址很长，存在时间也短，我便决定提供一个带有统计功能的 bitly. com 链路，如 http://bitly. com/OtcuJx +。[①]该链路把读者带到 bitly. com 页面，它将显示完整的链接、首次使用日期以及更多的使用统计数据——即使该链接已过期。

① Dillon Beresford, “Exploiting Siemens Simatic S7 PLCs”, a paper prepared for Black Hat USA +2011, 8 July 2011, http://bitly. com/OtcuJx +.

致　谢

本书的想法可以追溯到2012年1月发表在《战略研究杂志》（*Journal of Strategic Studies*）上的一篇同名文章。乔·马伊奥洛（Joe Maiolo）和汤姆·曼肯（Tom Mahken）都是非常优秀的编辑，他们给这篇文章增加了曝光度，使之成为该杂志即将在线上发表的第一篇文章，比实际的印刷版要早好几个月。接着，泰勒和弗朗西斯出版集团（Taylor & Francis）的米歇尔·菲利普斯（Michelle Philipps）决定使该文免于付费，可以公开访问。还要感谢布莱克·豪恩谢尔（Blake Hounshell）和苏珊·格拉瑟（Susan Glasser），他们让我在《外交政策》（*Foreign Policy*）杂志上发表了《战略研究杂志》原文的较短版本。“网络武器”一章的部分内容是与伦敦国王学院信息学系的同事彼得·麦克伯尼（Peter McBurney）教授合写的，最初发表时的题目与此相同。英国《皇家三军联合研究所杂志》（*The RUSI Journal*）的编辑阿德里安·约翰逊（Adrian Johnson）和艾玛·德·安杰利斯（Emma De Angelis）决定在2012年2月的那一期特别报道这篇引起争论的文章，他们的杂志销路很好。向丹·迪特尔（Dan Dieterle）和布鲁斯·施奈尔（Bruce Schneier）脱帽致敬。当论点还在初期阶段时，前者就是第一批报道“网络战争不会发生”的博客作者；后者把最初的文章推荐给了更多读者，这连我都不敢想望。

有几位同事帮忙扩展了本书的分析，有时是指出我自己不可能发现的晦涩细节或引用，有时是不同意书中的一些论点。我要

感谢以下人士，按字母顺序，他们是德米特里·阿尔普洛维奇（Dmitri Alperovitch）、戴维·贝茨（David Betz）、乔尔·布伦纳（Joel Brenner）、理查德·彻格温（Richard Chirgwin）、罗恩·戴伯特（Ron Deibert）、亚当·埃尔克斯（Adam Elkus）、埃米莉·戈德曼（Emily Goldman）、戴维·格里比（David Grebe）、克莱门特·吉东（Clement Guitton）、迈克尔·海登（Michael Hayden）、马克·赫克（Mark Hecker）、伊莱·杰伦克（Eli Jellenc）、帕万·卡特卡尔（Pavan Katkar）、丹尼尔·库尔（Daniel Kuehl）、赫伯特·林（Hebert Lin）、乔·马伊奥洛、彼得·麦克伯尼、加里·麦克格劳（Gary McGraw）、丹尼尔·穆尔（Daniel Moore）、理查德·奥弗里尔（Richard Overill）、戴维·奥曼德（David Omand）、戴尔·彼得森（Dale Peterson）、蒂姆·史蒂文斯（Tim Stevens）、约翰·斯通（John Stone）、罗恩·蒂拉（Ron Tira）、迈克尔·沃纳（Michael Warner）、马修·韦克斯曼（Matthew Waxman）、马丁·扎普夫（Martin Zapfe），还有那些不能说出名字的人士以及三位匿名评阅人。赫斯特（Hurst）出版社的迈克尔·德怀尔（Michael Dwyer）很有远见，建议把最初的文章扩展成书。非常高兴与他以及他在赫斯特出版社的团队共事，尤其是蒂姆·佩奇（Tim Page）。

伦敦国王学院战争研究系是一个非常激励人写作和教书的地方，感谢来自不同学科的许多同事，特别是斯特兰德大街（Strand）门厅六楼信息学系的同事。我的2012/13网络安全单元课程的出色学生是我一个真正的灵感（源泉）。本书在任何其他地方可能都写不出来。感谢美国国防部海军研究办公室（Office of Naval Research，亦称海军研究局）和密涅瓦项目（Mineva Program）的资助。我还要感谢德国康斯坦茨大学（University of Konstanz），特别是沃尔夫冈·赛贝尔（Wolfgang Seibel）和弗雷德·吉罗德（Fred Girod），让我有机会于2011年夏天在克罗伊茨林根

的塞堡（Seeburg in Kreuzlingen）安静和令人愉快的环境中构思了本书粗略的大纲。

一句非常特别的“谢谢你”送给安妮特（Annette）。

内容提要

在悲剧性的1914年夏天，欧洲在政治上陷入第一次世界大战。20世纪30年代中期，法国剧作家让·吉罗多（Jean Giraudoux）从中获得灵感，写下了著名的戏剧《特洛伊战争不会发生》。英国剧作家克里斯托弗·弗赖伊（Christopher Fry）后来在1955年把它的两幕翻译为《虎临城下》。[①]情节被设置在特洛伊城的城门之内。赫克托（Hector）是一名看破红尘的特洛伊指挥官，他徒劳地试图避免先知卡桑德拉（Cassandra）所预言的不可避免的事情：与希腊人的战争。吉罗多是1914年的老兵，后来在奥赛码头也就是法国外交部任职。他写的悲剧是对欧洲领导人、外交官和知识分子的有力批评，而他们即将再起战祸。该剧于1935年11月在巴黎的雅典剧院（Théatre de l’ Athénée）首演，距离这位剧作家的担忧成为现实几乎整整四年。

从最近有关网络战争的言论来看，世界似乎再次面临着1935年时的情形。1993年，兰德公司的约翰·阿奎拉（John Arquilla）和戴维·朗菲尔德（David Ronfeldt）曾宣称："网络战争来啦！"[②]政府机构花了一些时日才明白过来。2006年，美国空军部长迈克尔·韦恩（Michael Wynne）宣布，"网络空间是空军飞行

---

① Jean Giraudoux, *Tiger at the Gates* (*La guerre de Troie n’ aura pas lieu*), translated by Christopher Fry, New York: Oxford University Press, 1955.

② John Arquilla and David Ronfeldt, "Cyberwar is Coming!" *Comparative Strategy*, Vol. 12, No. 2, 1993, pp. 141–165.

和战斗的领域”。四年后，五角大楼的领导人加入进来。美国国防部副部长威廉·林恩（William Lynn）2010年在《外交》杂志的一篇文章中写道，“虽然网络空间是一个人造域”，但“对军事行动来说”，它已变得“与陆地、海洋、天空和太空一样重要”。[①]白宫前网络沙皇理查德·克拉克（Richard Clarke）则认为网络战争使人想起灾难，其严重程度使“9·11”事件都相形见绌，并敦促“同时并且现在”就采取多项措施，“以避免网络战争的灾难”。[②]2011年2月，时任中央情报局局长的莱昂·帕内塔（Leon Panetta）警告众议院常设特别情报委员会：“下一次珍珠港事件很可能是网络攻击。”[③]后来，作为五角大楼的负责人，帕内塔又重复了这个可怕的警告。迈克·麦康奈尔（Mike McConnell）曾任乔治·W. 布什（George W. Bush）的国家情报总监，直到2009年。2012年年底，他阴郁地警告说，美国不能“等待相当于世界贸易中心倒塌那样的网络崩溃”[④]。然而，当美国政客在警告数字末日的时候，美国的秘密间谍却忙着释放一个非常复杂的计算机蠕虫病毒——众所周知的“震网”病毒（Stuxnet）——以破坏伊朗在纳坦兹（Natanz）的核浓缩计划。《名利场》杂志上一篇非常有名的调查文章得出的结论认为，该事件预示着21世纪战争破坏性的新面孔，“震网病毒就是网络战争的广岛”[⑤]。

但是，果真如此吗？卡桑德拉们正确地预测历史了吗？网络冲突真的进入战争的“第五域”了吗？网络战争真的来了吗？

---

① William J. Lynn, “Defending a New Domain”, *Foreign Affairs*, Vol. 89, No. 5, 2010, pp. 97–108.

② Richard A. Clarke and Robert K. Knake, *Cyber War*, New York: Ecco, 2010, p. 261.

③ Lisa Daniel, “Panetta: Intelligence Community Needs to Predict Uprisings”, American Forces Press Service, 11 February 2011.

④ Paul Taylor, “Former US Spy Chief Warns on Cybersecurity”, *Financial Times*, 2 December 2012.

⑤ Michael Joseph Gross, “A Declaration of Cyber-War”, *Vanity Fair*, April 2011.

本书认为，网络战争不会发生，但这个观点未必就伴有吉罗多式的讽刺和扭曲。相反，它只是对过去、现在和可能的未来的评论：网络战争过去从未发生，现在也未发生，要扰乱我们的未来也极不可能。毋宁说，相反的事情正在发生：计算机所助力的对暴力本身的攻击。所有过去和现在的政治性网络攻击——与计算机犯罪相比——都是与人类冲突本身一样古老的三种活动的复杂版本：破坏、间谍和颠覆。仔细考察可以发现，网络攻击在三个不同的方面有助于减少而非加剧政治暴力。首先，在技术上，武器化的代码和复杂的**破坏**行动使得针对性很强的攻击成为可能，即攻击对手技术系统的运行，而非**直接**对这些系统的操作人员和管理者造成身体伤害。更为可能的情况是，代码引发的破坏可能造成重大的金融和声誉损失，但对硬件根本不会造成任何物理性破坏。其次，**间谍活动**正在发生变化：在高风险的行动中，计算机攻击使得潜出数据而不必首先潜出人员成为可能，而这些行动可能会危及那些人员。然而，自相矛盾的是，情报机构对“网络”越擅长，它们从事狭义网络间谍活动的可能性也就越低。最后，**颠覆**正在变得越来越不依赖直接的武装行动：联网电脑和智能手机使得动员追随者以和平方式从事政治事业成为可能。在一些情况下，削弱对既有秩序的集体信任和合法性比过去——那时国家可能垄断了大众传播手段——需要的暴力更少。这尤其适用于动荡的早期阶段。

但是，有进攻意识的技术爱好者应屏息以待，因为政治暴力性质的这些变化也有其局限性，而这些局限性将大大削弱网络攻击的效用。利用有组织的暴力并把训练有素的专业人员置于危险之地，也有网络空间难以或不可能复制的独特优势。这些局限性再次以不同的方式适用于所有三种类型的政治暴力。首先，对颠覆者来说，线上组织和动员的新形式也意味着更高的成员流动性、对目标的更高依赖以及更少的领导者角色——他们可能会通

过强制性手段保持内部的凝聚力和纪律。现在，发动一场运动更加容易，但要成功却更加困难。其次，采用纯粹的网络间谍而没有人力信息员，这对那些试图把数据放在上下文之中来解读和评估情报，并把它转化为政治（或商业）优势的人来说，产生了前所未有的困难。现在，获取数据更加容易了，但使用数据却并非如此。最后，在技术上，把网络武器用作服务于更广泛政治目标的工具也是一个巨大的挑战，而不只是在一次性却不可能重复的破坏任务中是如此，这些任务与“管中窥豹”的极客而非有宏观视野的政治家关联性更大。

本书分为八章。第一章概述何谓网络战争，或者说，如果发生网络战争的话，它将是什么样的。任何试图回答这个问题的尝试都必须从概念开始。进攻性行为必须符合一定的标准，才能称得上战争行为：它必须是工具性的；它必须是政治性的；最关键的是，它必须是暴力性的，或者至少具有潜在的暴力性。第二章探讨在网络攻击的背景下暴力含义的变化。第三章考察“网络武器”这个越来越流行的概念，并讨论以代码的方式负载的伤害性工具所具有的潜力和局限性。本书还将逐案探讨一些经常被引用的发生在网络空间中的进攻性和暴力性政治行为。第四章考察**破坏活动**。迄今，世界尚未经历过针对非常脆弱、安全防护不佳的工业控制系统——如发电厂、电网或其他关键公用设施——并造成重大物理破坏的攻击。本章对这种明显的不存在（或可能的推迟）给出解释，并评估具有潜在破坏性的未来攻击对发达社会的基础设施带来的真正风险。第五章审视以计算机网络攻击为手段的**间谍活动**。在许多方面，网络间谍都表现出一种悖论：它几乎总是一种非暴力形式的计算机攻击，也是对发达国家最根本而且可能是改变游戏规则的威胁，这主要是出于经济上的原因，而非严格和狭义的国家安全上的原因。第六章探讨网络空间中最普遍的一种激进主义和政治暴力——**颠覆**。本章发现，技术降低了颠

覆活动的进入成本，但也提高了持续成功的门槛。第七章评估溯源问题，这一直是网络安全的根本问题。如果承认溯源是个政治问题而非技术问题，那么就可以认为该问题本身就在于攻击的严重程度。结论部分（第八章）进行了总结，并希望使讨论超越令人厌倦而无用的“网络战争”比喻。①

① 自2010年以来，一些重要的论述已对有关讨论起到了促进作用。其中，最重要的包括安全专家布鲁斯·施奈尔（Bruce Schneier）、奥巴马的前网络安全协调员霍华德·施密特（Howard Schmidt）以及学者肖恩·劳森（Sean Lawson）。参见 Bruce Schneier, “The Threat of Cyberwar Has Been Grossly Exaggerated”, Schneier on Security, 7 July 2010; Ryan Singel, “White House Cyber Czar: ‘There Is No Cyberwar’”, *Wired*, 4 March 2010; Sean Lawson, “Beyond Cyber Doom”, Working Paper, Washington, DC: George Mason University, January 2011.

目录
Contents

第一章　何谓网络战争

卡尔·冯·克劳塞维茨的战争概念仍是最简洁、最基本的。孙子是一位古代的战略思想家，他在20世纪90年代关于信息战争的讨论中经常出现。但是，这位中国古代的将军和哲学家以铿锵有力的警句而非系统思想闻名——《孙子兵法》的很大部分读起来就像来自公元前500年波涛汹涌的“推特”（Twitter）简讯。孙子的现代普鲁士对手则提供了一个更为连贯一致和精致的工具，以用于严格分析。尽管在许多方面有其局限性，但克劳塞维茨的概念和理念仍是研究“武力的使用”的专业人士和专家的核心词汇。克劳塞维茨确定了三个主要标准，任何攻击性或防御性行动要成为或被理解为独立的战争行为，都必须满足所有三个标准。过去的网络攻击都不满足（这些标准）。

第一个要素是战争的暴力性。克劳塞维茨在《战争论》的首页写道，“战争是迫使敌人服从我们的意志的暴力行为”[①]。简言之，所有战争都是暴力性的。如果一个行为不具有潜在的暴力性，那么它就不是战争行为，也不是武装袭击——在这种情况下，使用该词就有了比喻的意味，如针对肥胖或癌症的“战争”。真正的战争行为常常具有潜在的或真实的致命性，至少对一方的某些参与者来说是如此。套用杰克·吉布斯（Jack Gibbs）的话

① Carl von Clausewitz, *Vom Kreige*, Berlin: Ullstein, 1832 (1980), p. 27.