

《兰德报告：美国如何打赢网络战争》

图书基本信息

书名：《兰德报告：美国如何打赢网络战争》

13位ISBN编号：9787506065177

10位ISBN编号：7506065177

出版时间：2013-9-1

出版社：东方出版社

作者：马丁·C·利比基

页数：212

译者：薄建禄

版权说明：本站所提供下载的PDF图书仅提供预览和简介以及在线试读，请支持正版图书。

更多资源请访问：www.tushu111.com

《兰德报告：美国如何打赢网络战争》

作者简介

《兰德报告：美国如何打赢网络战争》

书籍目录

序言
概述
缩略语列表
第一章 引言
目的
基本观点与内容组织
第二章 概念模型
网络空间机制
外部威胁
内部威胁
定义网络攻击
定义网络威慑
第三章 为什么网络威慑是不同的
我们知道攻击方是谁吗？
我们有能力破坏他们的资产吗？
我们可以重复攻击对手吗？
如果报复未能成功威慑，那它能否至少解除对方武装？
会有第三方加入战斗吗？
报复会向我们自己一方传达正确的信息吗？
我们有一个忍耐极限吗？
我们能阻止冲突升级吗？
如果攻击方没有什么值得攻击的资产怎么办？
不过网络空间中报复的意愿更可信
优秀的防御能力能够进一步增强威慑的可信性
第四章 为什么初始网络攻击的目的很重要
错误
施压
武力
其他
启示
第五章 反应策略
目标放应该曝光网络攻击事件吗？
应该何时公布溯源的结果？
网络报复应该是显而易见的吗？
报复行动是“迟做总比不做好”吗？
对别国政府容忍的自由黑客进行报复
对CNE进行的报复情况如何？
威慑政策可以扩展到盟国吗？
网络威慑政策应该挑明吗？
漠视策略能够挫败攻击方的战略吗？
报复之外的应对方法
攻击方视角
发出停火信号
第六章 战略网络战
网络战的目的
网络战的合理性
网络战的局限性

《兰德报告：美国如何打赢网络战争》

网络战的管理

以战防战

保留二次进攻的能力

秘密网络战？

政府在防御网络战时的角色

管理网络战的效果

结束网络战

结论

第七章 战术网络战

把网络战用作晴天霹雳

向网络中心站泼冷水

袭击民用目标

对战争中网络战的组织

结论

第八章 网络防御

网络防御的目标

体系结构

政策

策略

操作

总结

第九章 情况复杂

附录A 网络空间内战争行为由何组成？

附录B 明示型威慑与默示型威慑之间的对比计算

附录C 网络军备控制的暗淡前景

致谢

《兰德报告：美国如何打赢网络战争》

精彩短评

- 1、太学术了!关于网络战争的理论知识体系。
- 2、比较实战。
- 3、识货的人太少
- 4、我可能有点落伍了
- 5、Think tank 編出來，避免政客滿嘴跑火車的「小學生」識字課本。
- 6、普通报告而已，没什么亮点。都是大家稍微用力能搜到的

《兰德报告：美国如何打赢网络战争》

精彩书评

1、前一段，美国棱镜计划的曝光着实让美国尴尬了一阵，更是让美国诸多的盟友为之一惊，并重新审视安全问题。而在斯诺登去留问题上，曾经让美国头疼的维基解密也站出来瞎起哄，更是让人们联想到当年的泄密案。网络，离国家安全、甚至战争并不遥远。《兰德报告：美国如何打赢网络战争》是兰德公司应美国军方要求作出的一份调研报告，详细描述了兰德公司关于网络战争的看法。如果我们把海陆空和太空，比作战争发生的四个空间，那么网络战争无疑就是第五空间。人们关注这份报告的原因，或许就跟人们当年关注星球计划一样，想看看当代的罗马帝国如何在这个第五空间建立自己的霸权。不过兰德的报告或许一开始就让大家失望了：网络战争是有限战，威力并没有像核威慑那么大。虽然，文章一开始就引述了爱沙尼亚网络遭俄罗斯攻击的案例，而且近年来关于中美网络暗战的消息不断，但正如兰德报告所言，网络战争是一个不知道谁发起、在哪发起的战争。所以，我们至今还没有看到中国网军蓝翔技术学校出面承认，攻击白宫网页的就是他们。而另一方面，网络战争既不可控，又可治。什么意思？人们之所以能发动网络战争，就是因为网络天然具有漏洞，可以说哪里有网络，哪里就存在黑客入侵的可能。但另一方面，如果一旦发生攻击，那么也就表明下一次发动攻击的可能性消失。因为网络利用的就是漏洞，一次打击就暴露了漏洞的所在，下一次打击的可能性就降到了最低。当然，更为气馁的是，任何值得以战略网络战役对其施压的国家，同样很可能拥有反击的能力，并且反击的力度可能还不仅仅是骚扰那么简单。这就好像你拥有了对手的把柄，但你却不敢确定别人拥有你的把柄是不是比你还多，投鼠忌器。于是，这个时候，外交手段、经济手段和法律手段都比网络战更为有效。当然，尽管说了半天，这份报告似乎等于什么都没有说，对于习惯听取政府调研报告的人而言，这一点建设性都没有。（要是能调研出个什么可行性方案，那才算有成果嘛。）但或许这才是兰德公司能一直独立运作的资本，绝不因为他人的无知，而吹嘘先进的科技。在这点上，如果当年美国政府听取兰德公司的报告，或许就不会愚蠢地出兵朝鲜半岛了。—————欢迎关注

【读客】，微信号：Duker4u

2、十五分钟之内，计算机病毒让军方的Email系统瘫痪，造成炼油厂和输油管道爆炸，空中交通管制系统瘫痪，货运和城市铁路列车出轨，金融数据被涂改，电网断电，轨道卫星运转失控……随着食物紧缺，资金链断裂，公众心理恐慌，整个社会很快分崩离析……这不是科幻片中的场景，而是美国国防部助理、服务过七届美国总统的理查德·克拉克在他的《网络战争：国家安全的下一个威胁及应对》一书中对网络战争所造成的灾难性后果作的形象化描述。没有战火硝烟，却照样可以毁灭一切——我对于网络战争的这种威力和后果确信不疑。网络战争作为在信息技术的支持下，通过网络来攻击敌方信息系统的一种战争手段，相对于动用动辄千万美元的飞机、导弹等昂贵武器的传统战争而言，更少依赖现实力量，成本非常低廉，只需动用几台电脑、简单的轻按几个指令即可，而且可以直接攻击敌方的指挥系统核心，事半功倍。我对于这一新的战争形态的出现是深感欢欣鼓舞的，将其视为传统实力不对称的战争双方弱者一方出奇致胜的战争利器，我们或许可以就此与有些国家抗衡。果真如此吗？手头这本《兰德报告——美国如何打赢网络战争》看法没有如此乐观。它是世界著名的军事战略智库兰德公司美国空军项目2008财年“网络命令与网络战争的定义与执行”项目的研究成果。它对网络战是什么、网络战需要什么，网络威胁能否阻止网络战，以及网络防御能否降低其危害等进行了理论化、系统化的分析。它在对传统战争形式加以对比的基础上，探讨了网络战争自身的规律，并据此对美国空军在规划建设网络战争目标、体系结构、政策、战略以及战术能力等方面提出了相应的建议。最后指出，对于美国空军而言，由于网络战作用效果的局限性，网络攻击必须保守使用，更重要的是加强网络防御。由此来看，我对网络战争的认识是片面的、模糊的，夸大了其有利的一面，存在不切实际的幻想。从书中的论述可以看出，网络自身的特点和规律使其无法通过施加暴力毁灭敌人，而是通过发掘敌方的漏洞并进行利用来完成攻击，效果具有临时性，而且其攻击方式容易被反制，只能用来骚扰或者短时间瘫痪敌方的指挥系统，但并不能解除其战斗力，因而只能用于对其他战争行动进行辅助支援，适合一次性打击而非长期的战役。兰德公司的研究非常全面，对网络战的分析非常深刻，从某种意义上可以视作是一本非常现实的网络战争教课书。虽然网络战争有着极大的局限性，但这样一本教课书对我们是非常有意义的，书中兰德公司给美国空军提出的如何打赢网络战争的建议对于我们同样有用，对于网络战争必须高度重视，作出相应的部署。当前，网络已经被定义为陆地、海洋、天空和太空之外的第五维空间，美国仍然掌握着网络时代最关键、最核心的资源，拥有最新的理念，最强的技术，美国专门成立了网络战司令部。其正是凭借于此不断的对其他国家进行网络入侵，近

《兰德报告：美国如何打赢网络战争》

来不断发酵的美国监听门事件就是例证。搜索网络战争，就会发现，国家层面的网络战争虽然没有出现，但民间早已经硝烟弥漫——中美黑客大战、中日黑客大战等等消息不绝于耳。但是，即便如此，网络本身的不透明性，网络战争的不对称性，还是为综合实力落后的国家带来了一丝希望，争相占领先机。当然，这也包括我们，要把本书作为我们的网络战争教课书——提高警惕，及早准备，从战略、人才、技术、资源、政策等等各个方面着手，奋起直追，大力发展我们自己的网络力量，不断提高网络战争的应对能力，增强综合实力，以在未来的战争中占得先机，立于不败之地。

3、拿到《兰德报告》关于网络战争的一系列分析时，正赶上周小平对李开复的公开质疑。两者当然不能视为一回事，但是却相同牵动着中国和美国两个国家。《兰德报告》的出版，似乎让我们看到了美国政府通过民间智库来化解斯诺登事件以来的舆论危局，找到替美国辩护的途径。当然，纵观全书给人的印象是，网络战争对于国家危害甚小，如果控制得当并不会造成巨大的威胁。这些辩护用兰德公司特有的报告术语强调出来，似乎别一番说服力。报告是以《美国如何打赢网络战争》为标题，就意味着对于网络战争的重视。这在屡次美国领导人对于中国政府外教威胁中，经常会以中国军方对于美国的网络战争为名义。似乎，美国是网络攻击的受害者。《兰德报告》也似乎强化了这种印象，但是我们知道当斯诺登公开美国对于世界各国的监听后，似乎网络战争的主动方已经不再是中国，而是由美国一手策划的。而对于中国政治讹诈，反而像是一场贼喊捉贼的闹剧。在这个背景下，我们翻开《兰德报告》就需要加上一些理性的思考能力，有些时候美国的智库也在做另一种宣传。本书的前言说，作为2008财年研究项目的成果，是由美国政府支持进行的国家安全方面的研究，类似于国内的国家课题报告。这种报告政治色彩非常浓厚。在这部报告中，作者分析了网络战争的定义，及其危害以及战争的震慑手段。不过分析的结果，似乎是由于网络能够造成的危害极少，而且仅能一次性攻击，所以政府对于网络战争并不需要太多的资金投入。这种说法，个人觉得是似是而非，并不是所有人都能接受。不过，也可以算是一家之言了。面对网络战争，国家应该采取什么样的方式来反应，应如何制定网络战争的策略，建立进攻和防御的手段，都是本书着重描写的对象。不过，我想他似乎回避了一种网络战争的手段。虽然，这种手段在伊斯兰之春中，屡次被运用，但是却没有进入作者的眼界。在作者眼里，似乎只网络技术攻击，才算是网络战争，而网络中通过公共交友软件进行组织和制定政治活动，并没被视作网络战争的手段。斯诺登事件爆发后，似乎美国一直都在试图淡化网络监听造成的负面政治影响，并试图说明网络战争没有什么可怕。但是，国内似乎并不这么看，在中国互联网上，大规模地谈论政治话题，并试图通过网络舆论来左右政治决策、司法判决、经济政策。这种手段，表面上看似乎与网络战争没有半点联系，但是如果将战争意义扩大，通过网络手段攻击一个国家的文化与生活方式，并对立宣传某种特定的价值观念。这种舆论战，在历次战争中并不罕见，但是由于身处和平生活中，似乎并不会将其作为战争的手段看待。在周小平对于李开复的公开质疑声中，我们似乎看到了某些被掩藏的事实。虽然有人将其作为政治事件，但是背后所透露出的价值观念的冲突，恰恰说明了政治意识形态的斗争，其实如火如荼地进行，网络站队还在继续。因此，当我们看这本书时，当然可以视作政治斗争，在网络工具上的延续，而不仅仅时网络技术上的国与国之间的斗争。如果网络战争只是指战争技术上的斗争，我想这并不可怕。我想最可怕的还是通过网络技术为手段，而以思想文化斗争为主体的网络战争才是更应该重视和警惕的。

4、昨天（10月25日）英国《卫报》凌晨称，从斯诺登处获悉，至少35名国际政要的电话曾被美国监听，当中不乏其老牌盟友。这则消息无疑是“棱镜”事件的延续，而正是这一事件催生了现在在我面前这本《兰德报告：美国如何打赢网络战争》中译本。说实话，这本原题为《Cyberdeterrence and Cyberwar（网络威慑和网络战争）》的报告中并没有多少吸引人眼球的内容。因为这本书只是一本战略分析。在我看来，我们可以从以下三个问题来理解这本书：一、“网络战争”真的存在吗？的确，从远古到现代一来，人类一直没有离开“战争”这一形式，但人类的战争往往是以拥有客观事物为基础的。而网络则是一个虚拟且开放的平台，其自身的性状和开发的初衷，既违背拥有“战利品”的事实，也与宣称占有的战争原则相违背，如果排除网络攻击造成的不便和连带的民事损失，那么网络战争毫无意义。这种虚拟的争斗，岂不近乎“戏”了吗？从这点上来看，网络战争其实尚未真正出现过，而宣称它存在的原因，恐怕是随着科技网络的应用范围的不断扩大，人们在越来越依赖网络的快速与便捷的前提下，出于不想失去这种“优势”的心理，才会设想其存在的结果。二、兰德公司为什么要写这个报告？这个问题其实好回答，兰德公司是目前最具权威的决策咨询机构，曾经以在朝鲜战争中准确预测中国会出兵朝鲜而备受世界瞩目——在这一点上，甚至可以说是当年的志愿军成就了兰德公司的成功。且不管“网络战争”实际存在与否，这一课题都可算是一个有前瞻性的研究项目，所以

《兰德报告：美国如何打赢网络战争》

兰德公司从事这方面的研究工作，有利而无害。在这个报告中，兰德公司的作者充分展示出了在战略战术方面的纯属和精细，从确定网络战争的损害到网络威慑的可能性，从区分网络攻击的等级到网络防御的策略，从确定攻击源头的准确性到网络还击的困难度……可以说，面面俱到且细致详尽。退一步说，单从这些内容来看，兰德公司确实是实力不凡。三、美国为何想“打赢”网络战争？“网络威慑”是这本书中经常提到的一个词语，不言而喻，能够发出威慑的自然是强者，也就是美国，但美国为什么要进行威慑呢？自二战以来，美国的战争威慑力一直延续到今，这无疑是科技发展的结果，然而在互连网络快速迅速崛起的今天，美国的科技领先的地位面临着严峻的挑战，而这个领域与传统军事领域不同，因为它既看见又摸不着，就仿佛是一知有丰富阵地战经验的军队，却要面对擅长打游击战或运动战对手一样，美国心虚了。中国足球队曾多次向我们展示什么叫“想赢怕输”，而这句话如果点颠倒过来就成了“怕输想赢”——我想这句话也许可以作为对这个报告出台原因的一种推测吧。然而，无论计划如何周详、策略如何完美，在任何战争中，最大的变量其实是人，从某种意义上说，2006年上映的《虎胆龙威4》已经向世人间接预言了今天的“棱镜”事件，这种祸起萧墙之内的事情，恐怕才是最令美国挠头的。

《兰德报告：美国如何打赢网络战争》

版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：www.tushu111.com