兰德报告

Cyberdeterrence and Cyberwar

美国如何打赢网络战争

[美] 马丁·C·利比基（Martin C. Libicki） 著
薄建禄 译

人民东方出版传媒
People's Oriental Publishing & Media
東方出版社
The Oriental Press

兰德报告

Cyberdeterrence and Cyberwar

美国如何打赢网络战争

[美] 马丁·C·利比基（Martin C. Libicki） 著

薄建禄 译

人民东方出版传媒
People's Oriental Publishing & Media
東方出版社
The Oriental Press

图书在版编目（CIP）数据

兰德报告：美国如何打赢网络战争／（美）利比基（Libicki，M. C.）著；薄建禄 译. —北京：东方出版社，2013. 7

书名原文：Cyberdeterrence and cyberwar

ISBN 978-7-5060-6517-7

Ⅰ. ①兰… Ⅱ. ①利… ②薄… Ⅲ. ①计算机网络-安全技术-研究-美国 Ⅳ. ①TP393. 08

中国版本图书馆 CIP 数据核字（2013）第 155010 号

兰德报告：美国如何打赢网络战争
（LANDE BAOGAO：MEIGUO RUHE DAYING WANGLUO ZHANZHENG）

作　　者：［美］马丁·C·利比基
译　　者：薄建禄
责任编辑：崔雁行　王思扬
出　　版：东方出版社
发　　行：人民东方出版传媒有限公司
地　　址：北京市东城区朝阳门内大街 166 号
邮政编码：100706
印　　刷：北京市大兴县新魏印刷厂
版　　次：2013 年 8 月第 1 版
印　　次：2013 年 8 月第 1 次印刷
印　　数：1—10 000 册
开　　本：710 毫米×1000 毫米　1/16
印　　张：13. 25
字　　数：154 千字
书　　号：ISBN 978-7-5060-6517-7
定　　价：39. 00 元
发行电话：（010）65210056　65210060　65210062　65210063

序　言

本书是一项2008财年研究项目的成果，项目名称为“网络命令与网络战争的定义与执行”。人们认为网络空间也是一种存在潜在冲突的媒介，与天空和太空空间非常类似。文章讨论了如何利用网络空间的能量，以及该能量的局限性。本研究旨在帮助澄清相关疑问，并聚焦于“网络空间飞行和战斗”能力背后的军事实际。

基本结论很简单：网络空间是一种独特的媒介，有着自身独特的规律。例如，网络攻击不是通过施加暴力而是通过发掘敌人的漏洞并进行利用来完成的。网络战很难达到持久的效果。这种媒介里面充满了各种不明确性，比如“谁攻击了谁”、“原因是什么”、“攻击的效果如何”、“他们能再次得手吗”等等。今天有效的东西可能明天就不再有效了（正是因为今天发挥了效用才如此）。因此，其他媒介中的威慑与战争原则并不必然适用于网络空间。我们必须重新考虑这些原则，本文就是这种思考的初步尝试。

本文的研究由美国空军第八航空军司令官（8AF/CC）、美国战略司令部空间与全球打击联合机能司令部司令官小罗伯特·埃尔德（Robert Elder, Jr.）中将发

起。项目的执行包括在兰德公司的美国空军项目(Project AIR FORCE,简称 PAF)之中的兵力现代化与运用专案(Force Modernization and Employment program)。网络战领域的决策者与政策研究人员,以及空军的规划设计层有可能会对本项目感兴趣。

兰德公司美国空军项目

兰德公司美国空军项目是兰德公司的一个部门,是由联邦政府资助的美国空军研究开发中心,主要进行研究、分析工作。PAF 向美国空军提供独立的政策选项分析,包括美国空军的发展、运用、备战以及对当前和将来的太空部队的支持等方面。具体的研究分为四个项目:兵力现代化与运用,人力、人事与训练,资源管理,战略与条令。

如果需要关于 PAF 的更多信息,请访问我们的网站:

http://www.rand.org/paf/

概 述

美国空军第24航空队及美国网络战司令部的成立，标志着网络空间与传统的陆地、海洋、天空及太空一样，成为军事领域的一种。由此我们相信，军队的进攻、防御与威慑等传统战争要素都完全适用于网络空间。不仅如此，我们还必须理解网络空间独有的特点，并将之应用于此类司令部以及其他新司令部的决策中。倘若生搬硬套地运用其他战争形式的决策方式，不仅会导致决策失败，还将阻碍正常的决策与规划。

本文将重点研究与网络战决策相关的内容：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。美国空军在发展网络战新能力时必须考虑这些问题。

网络可攻击只因系统存在缺陷

随着国家军队与经济建设对计算机网络基础设施依赖性的增强，以及计算机网络本身具备的外部可访问性，使得计算机网络存在着风险。黑客可以由此窃取秘密信息，并可以发送虚假指令以使系统瘫痪，或者注入虚假信息来误导操作员与机器做出错误判断，从而做出错误决定或者不做任何决定。

信息系统存在漏洞的原因不是因为不可抗拒的物理定理，而是因为理论与实践之间存在鸿沟。理论上讲，计算机系统只能严格按照其设计者与操作员的

意愿来执行各种功能，但事实上它的一切行动只依赖于自身指令或系统设置。存在这种差异的原因在于计算机系统非常复杂，并且它的发展变化更加复杂。

这种状况亦有好的一面。我们的所有错误都是可以纠正的，尤其是在被攻击时我们可以更加容易地发现需要留意的漏洞。我们也可以精确指定计算机网络中可被外部访问的部分及其可被访问的程度。需要指出的是，几乎所有的敌人都来自计算机网络的外部。因此归根结底，除非系统自身存在缺陷，否则敌人无法暴力入侵电脑系统。所有攻击系统的路径都是由系统自身提供的①。稍作夸张地说，信息组织可能遭受到的网络攻击的严重程度，完全取决于自身，这种情况在其他战争领域中是不成立的。

战术网络战应占据重要一席，但仅限于此

战术网络战指的是在战争期间针对敌方军事目标发动的网络攻击，其成功的前提在于行动目标可以被访问，并且存在漏洞——攻击者可以采取各种有效的方法来利用这些攻击点。此外，如果网络攻击的结果可以被监测到，那么网络战行动将更加有效。

在网络战行动中，网络攻击是否可行取决于目标的复杂性，并且我们对攻击效果进行预测的准确程度也受该复杂性影响。攻击者可以通过前期调查来发现某一目标系统中存在的具体漏洞。但是对后期攻击效果的预测还取决于对目标系统更深入的了解，如在发现遭受攻击的征兆时系统与操作员的反应策略，以及其他与被攻击目标系统相关联的系统与功能流程此时的行为。即便攻击得手，战术网络战的效果也是比较有限的。它既无法直接伤害敌方人员，也无法

① 从某种程度上讲，分布式拒绝服务攻击是个例外。2007 年爱沙尼亚遭受的就是此类攻击，攻击者通过阻断目标系统的所有外部访问路径来达成攻击目的，而非进入目标系统。但是由于很多组织（如军事、电力提供商）大体上都可以在与外界很少交互的情况下正常运转，分布式拒绝服务攻击在最坏情况下只是网络攻击危害中的次要因素。

破坏敌方装备（也有极少例外）。在最理想的情况下，网络战行动也只能迷惑、阻挠敌方军事系统的操作人员，并且这种效果也是暂时的。因此网络战只能用于对其他战争行动进行辅助支援，比如可以用于解除对方的战斗能力。

网络攻击有两个显著特征：其效果具有临时性，且攻击方式容易被反制，这决定了我们必须谨慎而精确地利用它。网络攻击更适合用于一次性打击行动，而非长期的战役。比如它适用于在空袭敌方的在建核设施时使对方的地空导弹防御系统瘫痪，而不适用于对一个国家的金融系统施加持续压力。因此更明智的做法是利用网络战来辅助其他战斗行动，但是不应该指望能够达成某些特定的结果。

战略网络战并非决定性的

目前我们尚不知道一次战略网络战的破坏性到底有多大。据估计，当前美国内部每年因网络攻击造成的经济损失约在数十亿美元至数千亿美元之间。

战略网络战就是针对敌方国家基础民用设施进行的网络战，数千亿美元这个数字说明我们可以将战略网络战作为常规军事行动的辅助手段，也可以作为逼迫对方屈服以避免更严重损失的手段。但是，战略网络战是否真的如同战略制空权一样，可以逼迫对方做出政治让步？由于敌方民众会坚信失去制空权只会导致更糟糕的结果发生，因此获取制空权就可以获得我们想要的战略效果。但是战略网络战的效果很可能恰恰相反。因为从被攻击方角度来看，当系统受到攻击后，他们可以很快发现系统中的漏洞并进行修复或隔离。如此一来本方的系统变得更加牢固、难以击破，民众由于系统安全性的增强会更加坚持，而非减少后期的抵抗。

从攻击者角度来看，必须要考虑如何防止网络战争升级为武力对抗，即使是战略性的武力对抗。此外如何结束网络战争也是个麻烦：由于难以对攻击进行溯源，且可能存在大量第三方的攻击者（见后文），因此该如何确定交战中的一方真的已经停火了呢？

网络威慑可能无法像核威慑一样有效

网络威慑的不确定性与核威慑的确定性形成鲜明对比。冷战期间的核领域有如下特性：（1）人们可以很容易地对核攻击进行溯源；（2）攻击造成的破坏是易于预测的；（3）攻击方第1000枚核弹的杀伤力与第一枚无异；（4）被攻击方发起反击的可能性是存在的；（5）不会出现第三方加入战争的情况；（6）私有企业无法进行自我防卫；（7）任何国家对核武器的恶意使用都会越过对手的忍耐极限，这个底线也是众所周知的；（8）不存在比核战争更高级别的战争形式；（9）交战的双方都会因为战争而遭受严重损失。虽然以报复作为威胁可能能够劝阻攻击者发起网络攻击，但是报复的难度与风险会使对方尝试做出反应，至少是对等的反应。确实，即使威慑立场很明确，但假若遭受的网络攻击危害很明显而攻击者身份不确定，会使威慑方陷入苦恼的窘境：积极响应则可能会犯下错误，保持克制则会削弱威慑的说服力。

网络威慑的重要性基于如下假设：网络攻击的成本很低，而网络防御的成本很高。如果网络攻击可以不受任何惩戒，那么攻击者毫无需要停止攻击的理由。此外，冷战期间的核威慑成功阻止了核冲突的爆发。那么在网络空间内，是什么在阻止同样的立场无法发挥同样的作用呢？ 这样的因素太多了。在网络攻击的目标（也就是下文中的“我们”）考虑网络报复时，很多在核威慑甚至是传统威慑领域都丝毫不构成问题的，在网络空间内就成了问题。

我们知道是谁攻击了我们吗？确切地讲，敌人可能在任何地方发起网络攻击，诸如网吧、开放的Wi-Fi节点以及非法控制的第三方电脑等。他们不需要昂贵或稀有的设备。他们几乎不会留下唯一的物理路径信息。因此，对攻击的溯源往往陷入臆测。确实，倘若采用威慑力场，只要攻击者因为意识到他们的攻击行动将会招致报复而放弃攻击，那么严格地溯源也就不再有必要了。但是在这之前我们需要证明如下问题：（1）攻击者也可能会认为他们可以动摇报复者的信念，即使对方溯源成功而发起报复时，攻击者可以做出完全类似于无辜者的回应（“谁干的？ 难道是我？”）来迷惑对方；（2）错误的溯源将树立新的

敌人；（3）需要令中立的观察者确信报复行动并不是侵犯行为。

报复者能够置对方资产于风险之下吗？我们有可能掌握目标的系统结构情况，并且可以使用攻击软件进行活体测试，但是对于目标在攻击下的反应却不得而知。目标系统每一微秒都在发生变化。可能有未知的系统进程可以检测、处理系统出现的错误操作，或者向人工操作员报警。系统能够失灵多长时间（决定了攻击需要投入多大的花费）取决于管理员对系统错误的理解程度以及解决问题的能力。此外，我们无法保证攻击者在网络空间内必然拥有我们能够进行破坏的资产。

他们可以重复行动吗？很难想象会有一次网络报复行动的预期破坏非常可怕，以至于没有一个潜在的攻击者会愿意冒险尝试招致此类打击（这是核报复极其重要的特征）。因此有必要重复行动，但是重复行动并不必然可行。如果攻击者认为己方在经受报复之后会变得更加安全，那么即使报复方的行动很成功，也不足以令攻击者信服。

网络攻击能使网络攻击者失去战斗力吗？在一个电脑廉价、网络普及且黑客可能无处不在的世界里，答案是否定的。

第三方国家会按兵不动吗？当前网络攻击工具随处可见。如果非政府的黑客加入此类对抗，将会使溯源更加复杂，或者使报复驱退攻击者的可能性更加难以确定。

报复行动会传达错误信息吗？大部分的美国关键网络基础设施都是私有的。如果国家使用明确的网络威慑策略，则会将网络攻击定义为战争行为，这样会使得第三方赔付网络基础设施所有者的战争损失，因此可能会降低他们在互联网安全方面的投资积极性。

国家能够设定做出回应的忍耐极限吗？除非一个国家宣称不论遭受到的网络攻击程度如何，都将展开报复，否则它必须定义一个可行的忍耐极限。但是如何确定一次攻击是否越过了该极限，则是一个棘手的问题。

能够避免冲突升级吗？即使网络报复是对等的，由此引来的反报复行动可

能并不是对等的。网络空间中的战争可能会引起真实世界中的战争，由此产生严重后果。

回应网络攻击前须权衡众多因素

在许多方面，网络战都是在处理不确定性。成功的网络攻击不仅仅会威胁到系统未被触及部分的可信性（谁能确定它们未被破坏？），而且整个单位都会被不确定性包围。因此网络战领域会出现其他媒介中所不曾出现的问题。

攻击者想要获得什么？由于网络战破坏的东西很少，获取的东西更少，这与更明显的战争动机不同。如果攻击者的意图是在隐蔽身份的情况下进行施压，那么传达出的信息是否依然明确？ 如果攻击的意图是暂时性地解除对方战斗能力，那么攻击者在对方丧失战斗力期间意欲获取什么？ 网络攻击及其结果能否服务于商业、行政领域，成为其竞争战略的一部分？ 在攻击国高层的表述中，网络攻击又扮演着什么角色？

目标国应该披露哪些攻击详情？许多网络攻击——对某组织核心内部系统的破坏、腐蚀攻击——的效果从表面上看并不明显。披露攻击的实情显得更真实，并且有必要以此来证明公开报复是应当的。不过保持沉默可以减轻民众的恐慌情绪，使民众保持对已修复系统的信心，并有利于实施非对立策略（比如先由民众揭发，再由政府施压）或非公开报复策略。是否以及何时披露攻击者的姓名也值得斟酌。太早披露可能会招致尴尬，但是假若在攻击发生很久之后才进行披露，则会使初始攻击与报复行动间的关联的可信性降低。在报复行动之前很久就披露的话将会给攻击者充分的时间来搞好防御，实施反威胁或开展内部动员，由此来避开报复行动。

国家该如何回应自由黑客的攻击？一个保护攻击者的国家对于追溯攻击来源来说是另一种障碍，但是这种保护会不会导致黑客失去活力呢？ 报复这样的国家会不会让其对手渔翁得利，又或者引火烧身？

网络威慑可以扩展至盟国吗？盟国的系统遭受攻击时，对攻击国身份与攻击效果的判断需要深入探测盟国的系统，这是盟友所不欢迎的（“难道你们不

相信我们？”）。此外在认定某一特定攻击者时，可能会有自己秘而不宣的立场。

军事网络防御与平民网络防御相似但不相同

由于军事网络使用了与民用网络几乎完全一样的硬件与软件，因此它们有着几乎完全一样的漏洞。军事网络的防御与民用网络的防御很相似——都是一项实践性极强的艺术。但是军事网络有着自身独有的特征：真实的敌人、明确的网络威胁以及许多封闭系统。

军事网络最重要的目标在于遭受网络攻击时能够和平日一样正常运转——毕竟评估军事系统的依据就是其在遭受军事攻击时的性能。坚固性是其关键，但是想要在子系统故障时使用各种方法保证大系统（军队本身）正常工作，则超出了网络安全工程学的范畴。对于那些可能是破坏性最大或最流行的系统故障模式，军队必须比其他行业更重视。

由于网络攻击的效果是暂时性的，军队在遭遇对方一次成功的网络攻击之后，紧随其后的首要任务就是判明敌人是否会利用被攻击系统失效后所带来的便利来进行实体攻击。其次的任务是伪装系统，使其看似未遭受到破坏，因为这里要假定攻击者在监控受攻击系统，以判断是否进行攻击。随后是进行系统恢复。之后才能考虑其他的事情（包括网络报复）。

对美国空军的启示

美国政府不应该将战略网络战置于优先发展的地位，该结论也可扩展至美国空军。单独依靠战略网络战，我们只能骚扰敌人，但并不能解除他们的战斗力。任何值得以战略网络战役来对其施压的国家，同样很可能会拥有反击的能力，并且反击的力度可能还不仅仅是骚扰那么简单。

考虑网络威慑时，我们同样有必要关注相关问题。溯源、预期反映、持续攻击能力以及反击选择有限等问题都是影响网络威慑的重要障碍。美国政府或

许应考虑先用尽其他手段：外交手段、经济手段及法律手段。

战术网络战有潜力服务于军事行动——但是有多大帮助我们尚不知道，并且在很大程度上是不可知的。由于破坏性的网络攻击能够推进或放大实体攻击的效果，并且战术网络战的成本相对低廉，因此值得发展。需要指出的是，实施成功的网络战不仅仅需要技术，还需要充分了解敌人的网络，包括技术层面与战术层面（潜在的敌人如何利用信息进行战争），后者甚至更重要。同时美国空军需要意识到最有效的网络攻击也有有限的有效期，因此应该保守使用。

纵观全文，网络防御仍然是美国空军在网络空间内最重要的活动。虽然保护军事网络所需要的大部分知识都与民用网络的防御知识相同，但是二者还是有很多不同。因此，美国空军在规划建设网络战目标、体系结构、政策、战略以及战术能力时，必须认真考虑。

缩略语列表

AT&T	current corporate identity	美国电话电报公司
BDA	battle damage assessment	战斗损伤评估
CNE	computer network exploitation	计算机网络情报获取
CNN	Cable News Network	美国有线电视新闻网
DDOS	distributed denial-of-service	分布式拒绝服务攻击
DEC	Digital Equipment Corporation	数字设备公司
DNA	Deoxyribonucleic acid	脱氧核糖核酸
DNS	Domain Name Service	域名服务
DoD	Department of Defense	国防部
FBI	Federal Bureau of Investigation	联邦调查局
HD DVD	high-definition digital video disc	高清数字视频光盘
IBM	International Business Machines	国际商用机器公司
IO	information operations	信息作战
IPv6	Internet Protocol version 6Internet	协议第六版
MO	modus operandi	做法，方法
NATO	North Atlantic Treaty Organization	北大西洋公约组织
NSA	National Security Agency	国家安全局
PLA	Peoples' Liberation Army	中国人民解放军

RF	radio frequency	射频
RSA	a corporation name	信息安全公司
SAM	surface-to-air missile	地空导弹
sysadmin	system administrator	系统管理员
Wi-Fi	trademark	无线网路通信技术品牌

目录