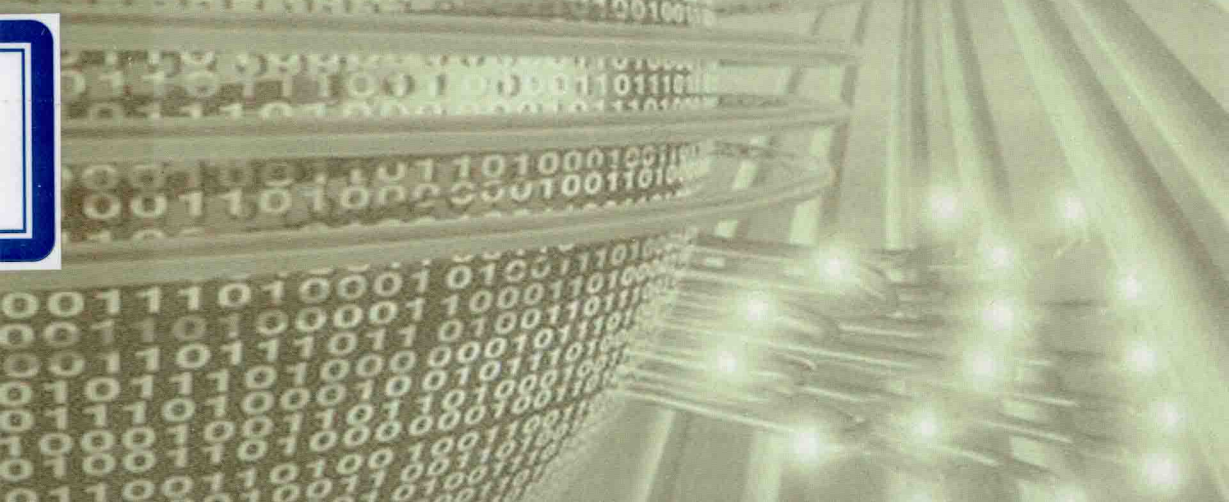
网络空间作战与安全丛书

战略网络空间安全

肯尼斯·吉尔斯 著

王陶然 张菊 严志刚 郭宏生 李捷 译



网络空间作战与安全丛书

战略网络空间安全

肯尼斯·吉尔斯 著

王陶然 张 菊 严志刚 郭宏生 李 捷 译

译　序

《战略网络空间安全》是应美国国会研究部要求撰写的专题研究报告，重点阐述了网络安全对国家安全的影响、战略网络安全概念、国家级网络防御策略等内容。该报告作者肯尼斯·吉尔斯曾获国际研究专业文学学士、硕士及信息与通信技术专业博士学位，先后任职于美国家安全局、国防情报局、华盛顿特区美国海军刑事调查局、北约协作网络空间防御发展中心等涉网安全部门。现将该报告全文翻译如后，供研究参考。

译　者

二〇一五年一月

目　录

概　要

该书研究证明计算机安全已从一个技术学科发展成为一种战略概念。当今世界是越来越依赖强大但易受攻击的互联网，结合网络攻击者的破坏能力，现在已经威胁到国家和国际安全。

战略挑战需要战略解决方案。该书作者研究了民族国家减轻网络攻击的四种方法。

- 下一代互联网协议（IPv6）；
- 孙子著《孙子兵法》；
- 网络攻击威慑；
- 网络军备控制。

这四种减轻威胁战略又分成多种类型。IPv6 是一种技术解决方案。中国最古老、最杰出的兵书《孙子兵法》是军事战略。第三和第四种战略是混合型战略：威慑是一种军事与政治的综合考虑，而军备控制则是一种政治和技术手段。

决策试验与实验评估法（DEMATEL）把主要研究概念放入影响矩阵进行分析。通过这种方法分析证明：IPv6 是目前改善国家网络防御态势的四种被研究战略中的上上策。

为什么 IPv6 在这项研究中能够胜出呢？这里面主要有两个原因：第一，作为一种技术，IPv6 比其他推荐的举措更能抵抗外部影响，特别是威慑和军备控制方面，所以对其投资更为可靠；第

二，IPv6 技术能够克服当今网络攻击者的重大优势——匿名。

作者简介

肯尼斯·吉尔斯博士，美国海军刑事调查局（NCIS）信息系统安全认证专业人员（CISSP）、科学家、美国驻爱沙尼亚塔林北约协作网络空间防御卓越中心（NATO CCD COE）代表。

致谢

这项研究顺利完成了，在此我要感谢信任、希望、爱情、家庭、朋友、海军刑事调查局、北约协作网络空间防御卓越中心、东京大学、我的博士学位顾问教授利奥·沃汉杜教授（退休）和瓦纳·塔林教授。

第一章　绪论：网络安全与国家安全

网络安全已经很快从一个技术学科发展成为一种战略概念。全球化和互联网已经赋予个人、组织和国家基于连续发展联网技术的惊人新能力。对每个学员、士兵、间谍、宣传员、黑客和恐怖分子来说，信息收集、通信、筹款和公共关系都已实现数字化和发生了根本改变。

结果，所有政治和军事冲突现在都有了网络维度，其范围和影响难以预测，网络空间发生的战斗比地面发生的任何战斗都更为重要。至于恐怖行动，黑客们已经发现采用纯媒体渲染就能获得成功。至于大规模杀伤性武器（WMD），根本无法对付非对称攻击。

网络间谍的惊人成就可以用来证明从计算机黑客行为中发现的高投资回报率。开始成本很低，人力情报等传统间谍形式更为危险。计算机黑客行为产生自由研究与发展数据，有权使用敏感通信。频繁处理世界舞台上网络间谍的国家领导者总是为此而闷闷不乐。

使用和滥用计算机、数据库以及连接它们的网络来实现军事目标早在20世纪80年代初期就以苏联军事技术革命（MTR）而知名。1991年海湾战争之后，美国国防部的军事革命几乎一夜之

间成为家喻户晓的术语。网络攻击本身不是结束，而是达到各种目的的有效手段，从宣传到间谍，从拒绝服务到破坏重要基础设施。国家安全威胁的特点没有改变，但是互联网已经提供了能够增加攻击速度、规模和力量的新投送机制。

从美国到俄罗斯，从中东到远东，数十个例证都已证明互联网的无处不在与脆弱性具有切实的政治与军事后果。随着互联网变得更加强大和我们的工作和生活越来越离不开它，网络攻击可能从现实争论的一个推论发展为将在未来冲突中发挥主要作用。

美国政治家汉斯·摩根索 1948 年写到，国家安全依靠一个国家的边界完整性及其公共机构。2011 年，军事入侵和恐怖攻击仍然是威胁敌国安全的最可靠方式。然而，因为国家重要基础设施，包括从选举到电力的每件事物，都已算机化与连通互联网，国家安全计划人员也不得不担心网络攻击。

事实是，大型和复杂的基础设施使用计算机和公共操作系统、应用软件和网络协议更便于管理。但是，这种便利必然要付出代价。联通性发生在安全之前，所以这使互联网和互联网用户更易受到攻击。现在，不仅每天都有更多的设备连通互联网，而且互联网上每个月都增加数十个共性弱点暴露（CVE）数据库。它们共同制造了黑客所谓的扩展“攻击面”。黑客们往往是创造性人员，他们能够利用这种复杂性找到没有适当授权的阅读、删除和/或修改信息的方法。

网络战场的一个似乎矛盾的论点是或大或小的参与者们都具有优势。信息技术强大的国家充分利用计算能力和带宽，弱小国家甚至独立黑客则利用不断增强的互联网力量攻击更强的传统敌国。而且，独立于互联网的国家是诱人的目标，因为它们在网络崩溃时可供选择的机会更多。

发生网络冲突时，敌国陆地之间可能互不相连，因为每个国

家在网络空间里都是邻国。硬件、软件和带宽形成地形，而非山脉、峡谷或水道。网络冲突中的最强大武器不是军事实力，而是逻辑和创新。

网络攻击确实也受到网络空间的有限地形限制。对于网络战，也不乏怀疑论者。基本上，战术胜利等于成功改组计算机内的比特：0 和 1。接着，攻击者必须停下来观察现实会变成什么样。成功没有保证。网络重新配置、软件更新和人力决策可以在毫无预警的情况下改变网络地形，甚至周密计划的攻击也可能完全失败。

事实上，互联网的动态特点给攻击者和防御者同样提供好处。许多网络作战都将是利用前沿技术占有更大优势的一方获胜。尽管攻击者拥有更多的目标可以攻击，也有更多的方式可以击中目标，但是防御者也有办法设计比以往任何时候都强大的网络冗余和抗毁能力。

2011 年，攻击者的最重要优势仍然是在一定程度上匿名。聪明的黑客们隐藏在迷宫似的国际互联网的体系结构里面。他们通过与受害国家政府外交关系较弱或没有执法合作的国家发出攻击。理论上，即使是一场大规模网络冲突，打击的也可能是一个并不确知的敌国。

执法和反情报调查每次都因为互联网是一个国际实体而受到损害，而执法和反情报调查权限每次都在电信电缆跨越国界时被迫终止。如果是某个国家赞助黑客发起网络攻击，更谈不上开展国际合作。

黑客匿名或者难以“归属”问题现在已经非常严重，严重到增大在名义和平时期没有任何传统的现实警告的情况下损害其他国家重要基础设施差别的几率。

网络防御面临着残酷的现实：传统的安全防护技能根本无法

满足计算机网络防御的需要；同时，如何保留住技术精英也成为一大难题。天才的计算机科学家们更喜欢到别处寻找更激动人心和薪水更高的职位。

结果，在技术层面甚至可能难以知晓是否已经受到网络攻击。在政治层面，网络空间的无形特点可能使计算胜利、失败和作战损害成为很主观的任务。而且，在网络法方面，还没有足够的专门知识与威胁保持同步发展。

最后，网络防御还因为对计算机黑客行为缺乏道德抑制而受到损失，这主要与使用和滥用计算机代码息息相关。到目前为止，还没怎么认识到网络给人类带来的痛苦。

综上所述，网络力量平衡的天平目前总是有利于攻击者。这与我们对历史战争的理解形成鲜明对比。在历史战争中，防御者总是享有战争发生在本国的战术优势。

因此，许多国家政府都可能得出这样的结论：在可以预见的未来，最好的网络防御是采取有效的进攻。首先，网络攻击可能是防卫本国所需；其次，它们是投送国家力量的强大方式，有时又是可否认方式。

网络攻击能对国家安全构成严重威胁吗？决策者们仍不确定。案例研究数量很少，许多信息都在公共领域之外，互联网时代还没有哪两个军事强国之间发生战争，绝大多数组织目前仍不确定其本身的网络安全状态到底如何。

进行一场具有战略重要性的“信息作战”实属不易，但也并非不可能。第二次世界大战期间，盟国充分利用破译莫名其妙的德国密码向阿道夫·希特勒发送虚假信息，发报说盟军将在加来海峡而非诺曼底发起登陆作战行动。这给盟军部队提供了十分关键的时间在欧洲大陆建立立足点，并且因此而改变了世界历史的发展进程。

随着时间的过去，军官们所谓的“作战空间”越来越难以定义和防卫。技术进步通常是渐进式的，但也可能是革命性的：火炮射程超越作战前线，火箭和飞机飞越国界，今天的网络攻击完全能在平时和战时瞄准世界任何地方的政治领导、军事系统和普通公民，无形中增大了攻击者匿名的好处。

按照狭义定义，互联网只是大批计算机连接起来组成的网络，但是“网络空间”作为一种概念的重要性正在与日俱增。现在认识到的威胁已经如此，以致美国新成立的网络司令部宣布网络空间已经成为战争的一个新领域，美国联邦调查局更是将其三个优先重点确定为防止恐怖行动、间谍行动和网络攻击行动。

网络战争不像传统的战争，但是它也具备空中轰炸、潜艇战争、特种作战甚至暗杀行动等历史上战争任务的一些特点。特别是，它能够从远距离或者利用突袭要素对敌国造成痛苦的非对称损害。

第二次世界大战后的美国战略轰炸侦察（USSBS）可给网络战计划人员提供一些经验教训。美国战略轰炸侦察得出结论，空中力量在战争期间不会永久毁灭任何敌国不可缺少的工业，所以总是需要“持续的重复攻击”。虽然如此，研究报告得出了无可置疑的最后结论：

盟军的空中力量在西欧的战争中发挥了决定性的作用：在空战中，取得了完全胜利；在海战中，帮助消除了敌军潜艇带来的最为严重的海上威胁；在地面作战中，使形势彻底转向有利于盟军的地面部队。

网络攻击不可能具有战略轰炸机攻击的毁坏性，至少在可以预见的未来是这样。但是最后，军事行动的结果总是要以效果论胜败。如果弹道导弹和计算机蠕虫都能毁灭或损坏目标，那么自然会首选蠕虫。

2009 年 5 月，美国总统奥巴马发布一项惹人注目的公告："网络入侵者已经探明我国的电网……在其他国家，网络攻击已使全部城市陷入黑暗。"那些喜好刨根问底的新闻记者们随后得出结论：这些攻击发生在巴西，在 2005 年和 2007 年都已影响到数以百万计的市民，但是攻击来源仍不确知。国家安全计划人员应该考虑到，电力没有替代品，所有其他基础设施，包括计算机网络，都得依赖它。

2010 年，Stuxnet 计算机蠕虫可能已经完成联合国安全委员会决议执行五年都做不到的事情：阻止伊朗追求核弹。如果这是真的，半个兆字节的计算机代码静静地被以色列空军的空中攻击所代替。而且，Stuxnet 病毒可能比常规军事攻击更有效，可能已经避开大规模国际危机的附带损害。从某种程度上来说，互联网易受大规模攻击。这对民族国家产生巨大诱惑，它们充分利用计算机黑客行为能够带来的高投资回报率。

如果网络攻击在未来战争中占据主导地位，胜负主要取决于是否拥有良好的信息技术基础设施，那么国际冲突持续的时间可能更短，因冲突而丧失的生命可能会更少。只有网络胜利能够促进战后外交和解与经济恢复。这种战争会取悦世界历史上最著名的军事战略家孙子，他认为，最好的领导能够不战而屈人之兵。

然而，像 Stuxnet 病毒这种例证也许不会频繁发生。现代重要基础设施提供了复杂多样的分布式目标。它们并非由一种系统、技术或程序组成，而是由许多系统、技术或程序组成，设计能够幸免于人性弱点甚至自然灾害。现场工程师可以看出攻击何时开始，并且能在攻击变成严重威胁之前使其变得无效。简而言之，计算机的脆弱性不应同整个基础设施的脆弱性混为一谈。

网络攻击可能只有在敌国已经投入大量时间和努力对国家电网、金融系统、空中交通管制塔台等重要基础设施目标开始创造

性和适时攻击时才达到国家安全威胁级别。

防空是系统在国家安全和国际关系中发挥战略作用的例证。它也可能代表相对传统军事攻击的独特网络弱点。例如，2007 年有报告说在以色列空军破坏所谓的叙利亚核反应堆之前曾经发起过网络攻击。

军事领导，按其专业，应该想到接受拒绝服务（DoS）攻击网络基础设施。早在 1999 年科索沃战争期间，就有不确知黑客试图通过互联网破坏北约的军事行动，并且声称取得了较小胜利。在未来冲突中，拒绝服务攻击可能包括公共网络“洪泛”技术、物理破坏计算机硬件、使用电磁干扰和更多。

恐怖分子没有军队满意的绝对民族国家支持。结果，他们可能仍然坚信互联网形成更多危险而非机会。

法庭检查缴获的硬盘证明恐怖分子已经研究过计算机黑客行为，而且西方经济是一个逻辑目标。例如，中东的紧张局势现在总是伴有网络攻击。在 2006 年的以色列与加沙战争期间，亲巴勒斯坦黑客成功地拒绝了向大约 700 个以色列互联网域名提供服务。

但是，网络恐怖分子形成的长期经济威胁可能不合逻辑。在全球化和互相连接的世界里，乐意合作的民族国家可能只会损害本国，恐怖组织可能渴求更大打击，而媒体关注比网络攻击更能造成打击。美国国家情报局前局长（DNI）迈克·麦康奈尔辩论说，一个可能的例外是对金融系统本身公众信心的网络攻击，特别是在货币安全和供应方面。

综上所述，网络攻击似乎能够产生战略结果，因此，国家安全领导者们必须认真对待。在国家和组织层面，良好的开端是有条不紊地进行风险管理，包括认真的目标威胁鉴定与细致的资源分配。目标不是尽善尽美，而是应用预期的勤奋和常识。

有关问题包括：

- 我国的重要基础设施有哪些？
- 它们依靠信息技术吗？
- 它们连通互联网吗？
- 损失会构成国家安全威胁吗？
- 能够保护它们吗？或者，如果不能，就使其离线吗？

客观性是关键。网络攻击受到巨大的媒体欺骗，部分是因为它们涉及使用不可思议的可能在没有计算机科学或信息技术正式教育的情况下难以理解的工具与战术。

随着越来越依赖信息技术和互联网，政府应该对网络安全、事件反应、技术训练和国际协作进行成比例投资。

然而，因为网络安全已从一个技术学科发展成一种战略概念，还因为网络攻击可能影响战略层面的国家安全，世界领导者们必须看到战术领域以外。寻求战略网络安全涉及如何配置所有的民族国家资源。

因此，这项研究的目标是评估民族国家网络攻击减轻战略。为了支持其论点和结论，作者使用决策试验与实验评估法。

一、该书的特点和范围

今天，世界领导者们担心网络恐怖行动和网络战对国家安全形成新的也许是严重的威胁：互联网是一种强有力资源，现代社会越来越依赖它，网络攻击者们已经证明其为了广泛的政治和军事目的而使用和破坏互联网的能力。

国家安全计划人员们明显需要准备战术和战略层面的网络防御。这项研究的目标是帮助决策者们实现战略层面的网络防御：选择战略层最有效的行动方案防卫其在网络空间的国家利益。

除绪论和结论外，该书有三个主要部分：第一部分，探究网络安全的不断变化特点，追踪其从一个技术学科发展成一种战略