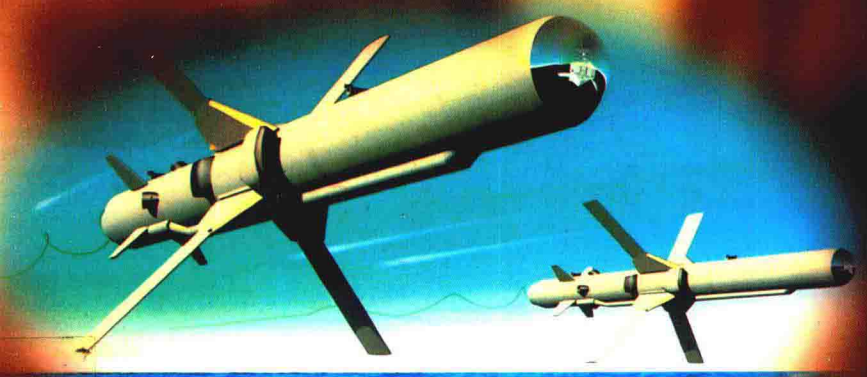
★信息时代战争新著译丛★ 陈伯江主编

信息战争

——网络恐怖主义：信息时代如何保护你的个人安全



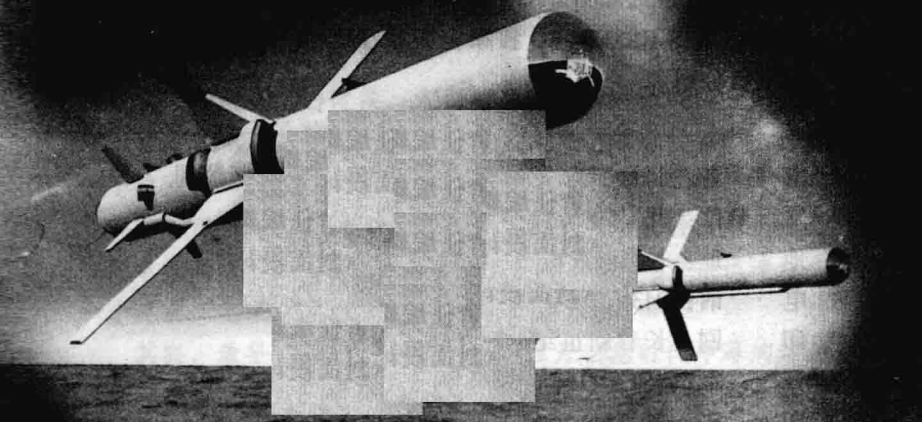
(美)维恩·斯瓦图 著
吕德宏 李力 亚日 译 李力 校

国际文化出版公司
北方妇女儿童出版社 联合出版

★信息时代战争新著译丛★ 陈伯江主编

信息战争

——网络恐怖主义：信息时代如何保护你的个人安全



(美)维[illegible]·斯瓦

吕德宏 李力[illegible]日 译[illegible]力 校

[illegible]际[illegible]公司
[illegible]出版社 联合出[illegible]

信息时代战争新著译丛（第一辑）
书名：信息战争 2.0
（美）维恩·斯瓦图　著
吕德宏　李力　亚日　译　李力　校

出 版 者：北方妇女儿童出版社　国际文化出版公司
发行单位：北方妇女儿童出版社
地　　址：长春市人民大街 124 号
电　　话：0431 - 5647211
印　　刷：长春新世纪印刷厂
开　　本：850 × 1168mm　32 开
印　　张：12.75
主　　编：陈伯江
责任编辑：安春海
封面设计：南　海

2001 年 10 月第 1 版第 1 次印刷
ISBN 7 - 5385 - 1230 - 6/E·133
定价：23.00 元

关注信息时代的战争

——《信息时代战争新著译丛》序

陈伯江

在跨入新世纪的时候，人们越来越多地感受到信息时代带来的巨大变化。其中最明显的变化，是人类社会的各个方面几乎不约而同地打上了“电子”的印记：从电子邮件到电子商务、电子银行；从电子大学到电子社区、电子政府；从电子图书到电子音乐、电子游戏……；我们所处的世界正在迅速地向一个充满“电子”的世界迈进！

其实，最早打下“电子”印记、拉开信息时代序幕的却是战争与军事领域。我没有考证“电子战”一词出现的准确时间，但这一词汇的广泛采用、甚至进入军队条令，至少也可追溯到20世纪60年代。1991年海湾战争之后，信息战、信息时代战争等新词汇、新概念，便一直是军界乃至整个社会讨论和关注的热点。

1997年6月至1998年6月，我曾有幸在美国华盛顿乔治城大学外交学院外交研究所进行客座研究。在此期间，我以“军事革命、未来战争与国防发展”为题，访谈了20多位美国军界高层人士、政府官员和著名学者，其中包括前国防部长佩

里、参联会前副主席欧文斯上将、克林顿总统第一任期的国家安全事务助理莱克博士、助理国防部长帮办米勒博士、陆军副参谋长助理加纳中将、海军少将特德等。通过访谈不仅了解到一些有关美国军事革命与国防发展的第一手材料和学术前沿信息，而且使我加深了对20世纪80年代末以来美国开展的一场持续而又不断深入的军事革命讨论的认识。美国学者认为，这场军事革命的实质是战争由工业时代向信息时代的转变。美国历经10多年进行军事革命讨论的过程，实际上也是不断认识信息时代战争新变化的过程。我从访谈美军将领与学者中得到的一个突出印象，就是他们总是从不同的角度谈到信息时代战争的新发展和新变化，并且反复强调这些新变化对未来军事发展的影响。

1998年6月回国之后，我做的第一件事是整理消化在美国客座研究的成果。做这件事的结果是先后出版了《大洋彼岸的军事革命——美国高级将领与著名学者访谈录》、《军事、外交与国际关系问题英语访谈》、《中国大校在美国》等中、英文著作，并在《解放军报》、《光明日报》、《中国国防报》、《科技日报》、《中国军事科学》、《外国军事学术》、《现代军事》、《国际展望》等报刊杂志上发表了多篇有关美国军事革命和信息时代战争发展趋势的文章。接下来我想做的第二件事，是组织翻译一套国外有关信息时代战争的新著作，以求更全面、更系统地向中国读者提供了解信息时代战争的第一手材料。《信息时代战争新著译丛》就是这第二件事的结果。

《信息时代战争新著译丛》通过有选择地翻译介绍美国等世界主要国家近年公开出版的军事理论著作，向读者全方位展示了信息时代战争的世界。该译丛力求具有以下特色：一是权威性。所选原著本身应是经典、权威名著，不仅在军事领域而

且在社会上有较大影响；原作者具有权威的身份或较高的知名度。二是新颖性。尽可能从最新的出版物中选择确有新意的原作。在内容上充分体现信息时代新的战争理论、新的战略战术思想、新的战争样式和战法，以及对官兵素质的新要求等。三是代表性。尽可能包括世界军事大国的有关著作。四是可读性。原作应为畅销书，内容雅俗共赏，引人入胜；中文翻译准确流畅，便于阅读。五是系列性。译丛陆续推出，系列配套，形成规模，从不同层面和角度反映信息时代外国军事与战争理论的发展现状。

《信息时代战争新著译丛》首批推出的10本书，可以说基本上体现了上述特色。从原著的作者来说，就有被美国誉为“军事革命之父”的参联会前副主席欧文斯上将；原苏联武装力量副总参谋长兼军事科学部部长、现俄罗斯军事科学院院长加列耶夫大将；美国著名军事预测学家亚当斯、著名信息战专家斯克图、著名海湾战争研究专家科恩；以及英国最为活跃的军事思想家等。从原著的内容来说，既有对信息战、网络战、计算机战、黑客战、太空战、精确战等信息时代战争形态的探索，也有对信息时代的战争观、威胁观、国家安全观等新变化的思考；既有对传统军事思想、作战原则在信息时代战争中面临挑战的分析，也有对信息时代军事革命、军队建设和国防发展的展望。从原著出版的时间来说，10本书全部是1995年以后的新书，其中7本为1998年以后出版，最新的一本出版于2000年10月。此外，多数书在国外许多畅销书排行榜及各类推荐、参考书目中均有其名。

江泽民主席近年多次强调，要注意跟踪世界军事发展。追踪世界军事理论的新发展就是其中一个重要方面。当前，我军建设正处在现代化建设与发展的重要时期。我军的现代化建设

与发展必须要坚持以我为主、走自己的路，这是中国特殊的国情军情实际和特有的战略文化传统所决定的。但与此同时，我们还必须看到，现在的世界已是一个日益开放的世界，信息时代也是一个正在将越来越多的资源共享的时代，在这样的大背景下，任何一个国家的军队现代化建设和发展都不可能在封闭的状态下进行。认真研究外军经验，有选择地借鉴外军经验，可以帮助我们选择正确的发展道路，加速现代化建设的步伐。知彼知己，百战不殆，打赢信息时代的战争更是如此。我衷心希望这套译丛能够在这方面发挥应有的作用。

有关信息时代战争的理论著作，涉及诸多高新技术领域和大量新词汇、新理论、新概念，翻译难度相当大。在本译丛翻译过程中，我们曾就不少难点问题请教军内外有关翻译专家，以求尽可能准确和规范。但由于我们水平有限，加之时间仓促，译文错误、疏漏之处在所难免，恳请读者不吝指正，以便再版时更正。另外特别需要指出的是，个别原著的部分内容和观点含有对我国的攻击和妄测，请读者予以分析和鉴别。

在《信息时代战争新著译丛》首批10本书面世的时候，我对热情支持本译丛出版和参与本译丛工作的所有领导、同志和朋友们表示深深的谢意！其中特别对军事科学院战略研究部部长姚有志少将等领导的热情鼓励；信息产业部军工司原司长侯印鸣等专家的积极支持；军事科学院外国军事研究部三室主任姚云竹博士、四室副主任聂送来等同事的大力帮助；北方妇女儿童出版社安春海总编助理的辛勤劳动；以及电子对抗国防科技重点实验室的慷慨资助，表示衷心的感谢！

对个人隐私的攻击　恶
意软件与计算机病毒　电磁
脉冲炸弹　数字监听　网络
空间的解决方案　国家信息
政策

目　　录

信息战争概述

“我们现有的技术、机构和政府已失去控制，各为其利而忙碌……我们把所有的一切——自然环境、我们的心灵和生命的控制权和发展方向，都交给了这个系统。”

——查尔斯·里茨：《绿化美利坚》

如果不是已经发生的话，你在某个时候将成为信息战争的牺牲品。如果不是你，那么将是你的一个家人或密友。

你的公司将成为信息战争的目标，如果不是昨天和今天，那么在未来你肯定会遭到攻击。

为什么呢？因为美国处在战争当中，一场没几个人愿意关注的战争。20世纪的信息冲突，未来全球战争的先导，已经开始。信息战争正在来临。对于某些人来说，它已经开始。

这是一本关于我们作为美国和网络空间的公民，如何掌握我们的电子命运，带领世界走向21世纪和信息时代的书。我们面临艰难的选择。信息革命不会是风平浪静，国家信息基础设施的构想展示了第三代美国梦想的复杂性。机遇与挑战都是如此之巨大，我们无法漠然置之。本书提供了一个总的概览，阐明我们现在在哪儿，我们正在向何处去，以及如果我们想决定自己的未

来，而不是被未来所吞没，我们必须直面哪些问题。

随着全球战争的幽灵归入历史书籍（关键存在哪里），人类自鸣得意的同声叹息取代了20世纪中叶在避弹所里经历过的歇斯底里。尽管在20世纪的战争和与战争有关的政治事件中有1.75亿人遇难，那种人类将会大毁灭的预言却幸运地从未成为事实。然而，随着同样危险的国际经济竞争取代大规模军事斗争成为主要的冲突样式，新的进攻目标将指向我们西方经济所依赖的信息和金融基础设施。

冷战已经结束并已为经济战所替代，竞争在正在凸现的北美、欧洲和亚洲太平洋盆地三大主要贸易板块之间进行。理查德·尼克松在20世纪70年代和80年代喜欢说第三次世界大战已经开始，并且说它是一场经济战争，也许是美国命中注定要输掉的一场战争。回想起来，也许我们应该对尼克松的预见给予更多的关注。

这三个巨大的经济力量占世界人口的1/4和世界国民生产总值的80%。利益是巨大的，每个人都想分一杯羹。

现代社会的基础是获取信息的能力，这一能力将会推动经济强大的国家走向兴盛，也会推动经济弱小的国家走向强大。在当今的电子互联的世界里，信息在以光速运动，它是无形的但却具有极大的价值。今天的信息相当于昨天的工厂，但它却比工厂脆弱得多。

现在，美国正在引导世界走向全球联网的社会，一个真正的信息时代。在这样的社会和时代里，信息与经济价值几乎是同义词。复杂的陆基和天基通信系统把1．25亿台计算机连接在一起，美国6万亿美元国内产值的主要部分都依赖于这一复杂网络连续而可靠地运转。信息战争就是一种电子冲突。在这种冲突里，信息是一种必须占有或摧毁的战略资产，计算机与通信系统以及其他信息系统成为最有吸引力的第一波打击目标。

1991 年 6 月 27 日，我曾对一个国会委员会这样说，“目前政府和商业用计算机系统的防护太差，可以认为根本不存在防御措施。我们就等着电子珍珠港事件的发生吧。政府及私人企业都没有采取适当的安全保密措施，大多数美国人的隐私已荡然无存。”

1990 年 10 月国家研究委员会提出《计算机处于风险之中》的研究报告，该报告的结果与我的观点不谋而合。报告提出，“现代盗贼用计算机偷的东西要比用枪偷的还多。未来的恐怖主义分子用一个键盘可以造成比炸弹更大的损失。”在最近的一项研究中，接受调查的 2/3 的美国人认为，如果他们的个人隐私受到侵犯，就应该减少计算机的使用。作为一个国家，我们只是刚开始认识并接受这样一个事实：我们的个人和经济利益的确与国家安全利益密不可分。

信息战争是新世界经济政治秩序的内在组成部分。经济战争正在进行并将继续下去，最终结果将影响到每一个美国人、每一家美国公司，并将影响美国的国家安全。随着恐怖主义分子向美国边界的渗透，可以预想不仅我们的客机和供水系统会受到袭击，就是我们的金融系统也会受到袭击，这是一个“点击”一下就会给成千上万美国人带来恐惧的可靠途径。

自从第二次世界大战结束以来，美国就把防御的准备放在对手的能力，而不是他们的意图上。世界军备竞赛就是这样开始的。然而，我们并没有跟上冲突之神的脚步。世界正在进入网络空间，但美国经济竞争的防御态势却仍顽固地位于陆地上。

网络空间是一个全新的世界，只有最大胆的预言家才能用心灵之眼隐约感受到它的存在，但他们也无法预断在过去 20 年里所展现出来的不确定性。

想象一下这样的世界：现金只是偶尔使用，信息成为交换的主要媒介；最通用的语言是信息而不是英语、德语、日语或俄语；知识与信息的权力超过了军事力量的威势；完全依赖于使信

息可以在任何时间同时传播到任何地点、任何一个人的高技术工具。在这个世界里，控制信息就可以控制公众。在这个世界里，电子隐私不复存在。

现在再来设想一下两个敌手之间的冲突，在这场冲突中信息是战争的目标和战争的果实。冲突中有胜利者也有失败者。计算机成为高效的进攻性武器。在这种冲突中，由于计算机和通信系统成了主要打击目标，必须对致命的却是无形的子弹和炸弹进行防御。

设想彼此竞争的经济体为扩大在电子金融领域的势力范围而不遗余力地战斗。

然后再设想由那些通过对对方的信息基础设施进行闪击战来进行竞争或解决争端的公司组成的世界。

或者再设想这样一个世界，在这个世界里一个人的爱恨和所得所失取决于对键盘的敲击。

“这是一个什么样的世界?”这是信息战争的世界。我们，作为一个国家，作为个人，还没有为我们正在创造出的未来做好准备。

在信息战争中，信息时代的武器将取代炸弹和子弹。这些武器不再是政府或中央情报局或克格勃的专利品。计算机和通信武器可以从目录、零售店和交易会上得到。许多信息武器可以由爱好者在自己的家里组装。当然，军队正在开发自己的信息武器，以进行信息战争。

信息战争与金钱有关。它可获取财富，它要剥夺对手的财富。信息勇士靠在全球网络里进行冒险、进行战斗而繁衍壮大。

信息战争与权力有关。控制信息就控制了金钱。

信息战争与恐惧有关。控制信息的人能让那些企图保住自己秘密的人感到恐惧。纽约银行就经历了这种恐惧，它在一天里丢失了 230 亿美元。

信息战争与傲慢有关。这种傲慢来源于这样一个自信，即人可以进行无懈可击的犯罪。

信息战争与政治有关。当德国政府支持情报机构对美国进行黑客活动时，盟友的含义就需要重新确定了。或者当为扰乱美国经济，伊朗政府暗中支持向美国市场投放假币时，我们应该洞察到冲突改变了它的面貌。

信息战争与挑衅和侵犯公民权有关。无论是在发达国家还是在发展中国家，从网络空间的城堡里走来了不起眼的黑客，他们一无所有而不怕失去。有些黑客会结成黑帮，他们是网络空间的有组织犯罪团伙。他们了解进行信息战争的经济收益。

信息战争与控制信息有关。随着网络空间的扩展和电子无政府状态的漫延，现实社会越来越失去控制。从80年代末和整个90年代的情况来看，信息战争不可避免。进行信息战争的条件已经成熟，仅只几年之前人们还无法预料这些条件会发展到这种程度。

当前信息战争每年给美国造成约1000—3000亿美元的损失，而且对美国经济的影响还在上升。美国国民生产总值的5%要经过全球网络，不在我们的掌握之内，这一情况影响了我们削减财政赤字、扩大出口和平衡贸易的努力。由于在商业、税收等方面损失数十亿美元，政府的财政收入受到相当大的影响。美国是信息战争的受害者这一情形，不仅仅是使我们的形象受损。我们的信用卡不再那么可信；我们的购买力和进行交易的能力受损；我们的政治和外交影响下降，因为我们的经济不再是毫无疑问的世界第一。我们不再是角斗场上惟一的硬汉。

要知道，每年超过2000亿美元的损失意味着有300到800万美国人失业。他们也是信息战争的受害者。信息战争利用了我们对自动化和现代计算机工具的依赖和沉迷。信息战争袭击的是我们的生活方式。

未来可能会发生计算机切尔诺贝利事件这一威胁并不是空穴来风。它只是一个由谁在何时发起的问题。任何有意志和有计划的人都可以进行信息战争，信息战争可以在三个不同的层次上进行，各有其目的、手段和目标。

第一类信息战争：个人信息战争

不存在电子隐私这样的事。我们存在的本质被传播到我们只能略微控制或根本无法控制的成千上万台计算机和数据库。从信贷报告到体检记录，从汽车行的档案到法庭记录，从司法机关的计算机到学校成绩单到透支购物单，从保险档案到旅行日志到个人储蓄状况，我们做过的和正在做的每一件事都记录在数字存储器的某个地方。

不幸的是能表明我们作为一个人的特点的那些记录全是没有保护的，容易遭到恶意修改、非法泄露或全部被抹掉。社会安全机关的雇员以每个姓名 25 美元的价格出卖我们的最高机密。更糟糕的是，直到今天我们还无法采取任何措施来保护我们的数字信息。我们没有获得必要的工具和机会来保护自己和家人免遭他人对隐私的电子侵犯。

如果我们的数字档案不存在了，我们的生活可能会完全乱套。网络空间的电子谋杀就是将数字记录全部删掉。人们认为计算机又不会撒谎，你怎么证明自己还活着呢！如果电子肖像被重新画过了，王子可能会在一微秒内变成一个穷光蛋。在网络空间，在你能证明自己无罪之前，你一直是有罪的。

第二类信息战争：公司信息战争

公司管理层对于公司资产已变得多么不堪一击这种情况没有什么感觉。虽然公司的财富越来越靠其信息的时效和价值来衡量，没有一个公司把信息资产开列在资产负债表上。可是没有这个条目，公司的经济稳定性就会出问题。通过攻击公司的信息系统把这家公司搞垮，或许很快就会成为受到重视的进行经济和政

治竞争与报复的方法。目前，进行信息战争所需的武器和技术就像电子制表软件和计算器一样普遍。

为防备只在概率统计上才会出现的龙卷风掀掉公司的作战指挥部，公司理事会的会议室将布设精心的防护设施。洪水摧毁丹佛市中心这种情况只有理论上微乎其微的可能性，然而为了躲过洪水的千钧一击，公司宁可在附近的山里挖掘地下掩护所。然而，公司没有考虑到如何防备其信息系统可能会遭到的组织精良的进攻。这种进攻不是大自然母亲所发起的，而是由人进行的。

我们应该意识到很难因此而责难美国的公司。近 50 年来信息处理能力的迅猛增长已成为并仍然是一场震撼世界的革命。令人眼花缭乱的技术成就和不可思议的想象力推动了这场革命。与此同时，在衡量与把我们的全部信念押在技术基础设施上这种做法相关的风险方面，投入的努力还远远不够。

正如我们理应看到的那样，对于我们当前的状况，联邦政府必须承担大部分责任。事实上，经常的情况是帮助我们保护计算机和网络并不符合政府的最大利益。政府不负责任的态度甚至妨碍了正在进行的增强个人隐私和商业性国家经济安全的努力。

然而，空洞过时的政策仍在继续，在某些情况下，政府公然采取某些措施进一步破坏每个美国公民的电子隐私。甚至克林顿总统关于个人隐私和保护美国商业的讲话也受到了近乎普遍的嘲笑、猜疑和怀疑。不论大家怎么努力，政客们就是无动于衷。

第三类信息战争：全球信息战争

总体上看，国会山和白宫还没有明智到把信息看成是至关重要的国家资产。他们还是以军事投送能力、石油储备、日本汽车和非法移民这类的术语进行思维。他们没有抓住新世界秩序之下更为根本的观念：国家信息基础设施和我们在电子技术全球网络中的地位。

除了五角大楼和情报机构内部几个有眼光的人，军方和情报