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

界仍然用带有具体的、可计量的又是可替代的有形的东西来衡量国家安全。然而，信息是无形的，并没具备直接的可计量的价格，除非你失去它，但此时你要付出难以想象的代价。

进入网络空间后，我们不能忽视一个充满未知数的未来所带来的各种可能性。我们必须摘下眼罩，接受而不是否认新世界秩序里既有好人也仍有恶棍的现实。我们必须使自己对那些我们不愿考虑的意外事件有所准备，这种做法是国家福祉所必需。我们要接受这样一个事实，随着国家的财富从工厂转移到计算机网络，我国曾经清晰的边界已经变得模糊，我们至多只能看到一个隐约的轮廓。

我们将会发现，我们的工作是使自己和后代做好准备，迎接一个充满希望与可能，同时也充满危险和障碍的世界。仅是 10 年以前，我们还无法想象今天这个世界。我们的后代会对这样的世界安之若素，正如我们对流动的热水习以为常。

在探索中，我们会不幸地发觉，有决心和实力的敌人具备前所未有的能力（请注意我说的是能力）对民族国家进行挑战，争取政治或经济的势力范围。我们将发现国际冲突将在世界信息高速公路和我国的国家信息基础设施里进行。现在我们必须保护自己。

因此，我们必须提出下述问题：为什么进行信息战争？它是不是一个言之过早的结论？它是不是未来的必然组成部分？这些问题对于信息时代和国家信息基础设施的未来是及时而独特的。考虑到我们在历史中的位置，可以看到有许多原因决定了信息战争是不可避免的。

·1 高质量、高性能电子信息系统难以置信地迅速扩散，创造了全球网络——网络空间，从而改变了我们经营的方式。不仅公司和政府买进了技术，而且上亿人也在不到 10 年的时间里突然获得了以前只为少数特殊人物才能拥有的工具和能力。信息战

争所需的相对简单的技术已是唾手可得。技术无政府状态已是现实。

全球网络是史无前例的道路系统，它无视民族和边界，把通向天国、财富和数字身份的钥匙平等地交给每一个有计算机的人。与动机或意图明显不同的“能力”，是本书要经常提到的一个关键主题。

2 尽管两极军事对峙的历史已经结束，数十个有着独特历史的新民族国家出人意料地出现了，它们在竞争中确立自己的地位。共产主义的失败并不意味着民主资本主义自动获得了胜利，每个新独立的民族国家都会顺利适应这个环境。它们还可以作出其他选择，并不是所有的选择都彼此包容的。在 20 世纪 90 年代初，自我利益压倒一切。

并不是每个人都遵循同样的原则进行全球经济和政治影响的竞争。我们美国人在竞争中以古老的课本为依据，善行、母亲和苹果派构成了我们的竞争伦理。其他人不大可能信奉过时的新教伦理，虽然我们据此赢得了工业革命。某些人可能采取宁愿乞求、求借、偷窃或以任何可能的方式得到他们需要的东西，美国和美国人仍然被视作被宠坏了的、任性的孩子，习惯于得到立即的满足。这个形象会使我们成为攻击的目标。

3、只有 1/4 的人口处于发达状态，其他数十亿人则处于不令人羡慕的贫穷状态。有产者是西欧较富裕的国家、日本、太平洋沿岸的某些国家和美国，其他都是无产者。全球网络通过文字、声音特别是电影把巨量的信息传过国界，送到无产者的手中。无产者很快就会想成为有产者。穷人没有什么可失去的，因此什么也不怕。惟一的办法是起来，追赶美国这个山巅之王，这是再明显不过的了。

4 世界永远不会缺少贪婪，很少有人、公司或国家能例外。企业、国家总是相互竞争，经常采用不是那么合法的手段采取优

势。全球网络出现后，技术扩散至每个人，贪婪来到了那些可能永远也不会犯罪的人的手边。贪婪在各个层次上都起作用，而大多数信息系统存在薄弱环节则为企图利用这些弱点的人提供了攫取惊人利益的机会。信息战争会给胜利者带来巨大财富，使失败者蒙受沉重损失。

5 在冲突的记录上信息战争的效果惟一无二。信息战争可以从远处发起，主谋舒舒服服地隐身于万里之外的一个键盘之后。没必要在物理上侵入受害者的领地。全球网络提供了无数个入口。

计算机恐怖主义分子轻敲键盘，即可不加区别地伤害到上千上万人的利益，播种仇恨、嫌疑和怀疑。信息战争是低成本、高技术的大规模毁伤手段。

6 信息战争是低投入高收益的活动。被逮住的几率甚低，遭告发的几率更小，受惩罚的几率几乎为零。在国际舞台上，诸国家不能就如何处置核武器达成共识，就如何处置一个坐在键盘后的信息勇士达成一致就更困难了。

7 在本质上，我们不相信计算机。它们处理信息的速度之快超出了我们的理解，因此我们认为它们不在我们的控制之内。大多数人都不清楚计算机里面是怎么回事。然而为维系人类社会的存在，我们需要计算机。信息勇士利用我们对计算机固有的恐惧和不信任——“二进制分裂症”、“数字癖”、“近似值焦虑”——来达到他们的目的。

8 最后，也许最为重要，人将发起信息战争，因为人有能力进行信息战争。历史昭示，无论最初发明它的意愿如何，任何一项新技术很快就会成为一种武器。在本例中，计算机技术已落入信息勇士之手。

有形形色色的信息勇士。在国际上，日本人和他们的照相机相当于各司令部搜集有价值的战略情报的侦察兵。近年来，黑客

一直在对美国公司进行信息战。晚近一代的信息勇士则更嚣张，他们公然对抗整个社会的意志。

苏联人当然是出色的信息勇士。目前，数以万计的前铁幕国家情报人员试图为出价最高的客户施展手段，他们中的某些人甚至在报纸的秘密部门提供服务。

渴望权力的独裁者、激进的原教旨主义者和 20 多个国际政治集团可能会使用网络空间推行他们的计划。资金雄厚、得到技术顾问帮助的贩毒恐怖主义者已经用信息战来对付毒品管理局。

激进的环保组织已经展示了他们进行硬性对抗的意愿，而信息战争为他们提供了以新的、富有想象力并且人身危险较小的方式对付石油公司、伐木公司和其他对濒危物种漠不关心的集团的能力。

信息掮客和数据经纪人未经你的同意就向任何一个有软盘的人出售你的姓名、上一中阶层邮政编码、最近的内衣购买日期等信息。银行和信贷机构允许计算机根据包含 30% 错误数据的信息作出影响你的生活和我们的生活的决定，它们居然没有负罪感。

任何人都可以成为信息勇士。《黑客季刊》这样的出版物提供了基本的黑客技术训练。网络空间本身为信息勇士征召自己的军队、设计自己的武器并部署使用它们提供了一个安全的场所。一个不开心的工人可能突然会对老板进行信息战争，这个工人因此而受到惩罚的可能性非常小。一名政府雇员可能在夜里是一名信息勇士，一个少年可能每天在网络空间里待 20 小时，可口可乐与比萨饼是他与地球的惟一联系。 1 亿个潜在的信息勇士（有些是不友好的）在等待时机，磨刀霍霍。

信息战争是关于能力的，潜在的个人的能力和潜在的有组织集团的能力。孩子的能力、商人的能力、民族国家的能力均对我们构成威胁，它们的意图是次要的。如果一个集团或某个人决定

进行破坏，那么他们现在手头就有武器来执行这个意图。

信息战争是什么样子呢？我们怎么识别它呢？如何进行信息战争？谁是信息勇士？他们在哪儿？用什么武器打信息战争？它们能干些什么？政府与产业界采取什么措施为对付即将来临的信息战争做准备？本书就有关在全球网络里个人、公司和国家未来的某些非常简单的问题提供了令人烦恼的各种解答。

但信息战争也提供了希望，即提供了一条摆脱困扰我们的技术专家政治主义处境的道路。第一步是承认存在的问题，并有使用可得到的解决方案的意愿。如果我们认为这些问题必须解决，那么个人电子隐私可以保住，国家经济安全也是可能的。网络空间是一个新的生存环境，我们都得以这种那种方式进入其中。我们要想好怎么与它打交道，因为个人的成功与国家的强大都取决于它。

本书讨论了信息战争的如何进行？由谁来进行？本书还讨论了为什么信息战争是技术进步的一个必要组成部分，特别是在天下还不安宁的时代。同时，本书还提出了使我们能够掌握自己电子命运的方案。

国家信息政策纲要

这个解决方案是国家信息政策。目前，网络空间的生活受几条原则和共同接受的几个行为规范的影响。这些原则和行为规范把正确与错误、善与恶、合法与非法区别开来。我们真的甚至不知道信息的定义，然而我们的经济却依赖于它。我们徒劳无益地试图把现有的陈旧的、甚至是古老的指导原则拼凑起来，而它们在网络空间里根本行不通。

大多数人甚至不清楚为制定国家信息政策需要提出哪些问题，华盛顿的情况就是这个样子。在最纯粹的意义上，网络空间绝对是技术无政府主义，无政府主义的传统是拒绝政府管制，信奉自制。

不幸的是，最近 20 年的时间并不是以自制和道德责任为特点，随着技术和信息进一步与我们的存在交织在一起，我们需要规则。在规则之前需要风气和道德，在风气之前需要提出问题。

国家信息政策不是一个要提交国会辩论的特别法津提案，相反，它是一系列议题和问题。提出之、思考之并满意地解答之，这是我们能够踏实、安全、充满信心地生活在信息时代里的先决条件。

谁将拥有、运行网络空间和国家信息基础设施？在其初始和成长阶段政府和产业如何共存？它们是否或应否以符合美国经济利益的方式结成伙伴关系？这样一种看法是否带有过多的社会主义色彩而不合美国的口味？对美国实业和经济利益的攻击是否等同于对美国的攻击？在国际舞台上，我们应该在多大程度上调整自己的孤立主义立场以使自身成为全球电子村落的一部分？在美国的第三个世纪里，我们是否应该有权利保持个人电子隐私？

对这些问题和其他问题的回答将决定我们如何在未来 10—100 年里生存。这些回答将告诉世界美国是一个什么样的国家，想成为一个什么样的国家。这些回答很可能会确定美国经济体制的长远成功。实际上，这些回答将表明我们是谁。

国家信息政策提供了一个为未来打基础的框架，是网络空间的宪法。

信息战争是真实的；现在到了我们学习我们将要面对的现实的时候了。

让我们做我们未来的主人，而不是未来的奴隶。

附　文

电 子 民 防

维恩·斯瓦图

在阅读本书时，我希望读者能有一两个观念。

1991 年 6 月在国会作证时我曾说过，如果我们不开始制订政策并采取防御措施，美国就会面临潜在的电子珍珠港的危险。我描述了电子珍珠港事件可能会怎样发生。那次作证已成为本书的哲学基础。

5 年后，克林顿总统指派首席检查长珍尼特·雷诺主持制定关于网络空间安全的国家政策。在内阁领导、情报界领导和几位民间专家的协助和合作下，司法部将于 1997 年年中向总统提交政策建议。他们所关注的与本书完全相同：即美国抵御电子攻击的电子民防（其他国家已有或应有类似的关注）。1996 年 7 月 15 日，克林顿总统签署了关于设立关键基础设施保护委员会的行政命令。

现代社会由四个互依共存的关键基础设施组成，国家和个人的生存离不开它们。

●电力系统是基础。不论电是如何产生的，也无论它是怎样通过由过顶明线和地下电缆组成的巨大网络传输的，没有电一切都玩不转。

●通信基础设施需要电力，并提供了为新闻、教育、娱乐、经贸和全球联系传送信息内容的能力。

●金融基础设施需要电力和可使电子货币流通的通信。美国

的国民生产总值约 7 万亿美元，在美国国内，只有不到 3% 的国民生产总值(GNP) 以硬通货币的形式存在；其余的都是网络现金——电子贷币。我们在全球市场中的地位不仅依赖于美国系统的可靠性，而且也依赖于其他贸易伙伴金融系统的稳定性。

●运输基础设施需要电力、通信和金融基础设施才能正常运转。

在美国第三次浪潮社会和其他处于第二次浪潮末期的社会里，这些系统紧密交织在一起，如果一个系统打个喷嚏，其他系统就会感冒。所谓“阻尼系数”（衡量一个系统的减震能力的指数），指的就是系统应对意外干扰和破坏的防御能力和恢复能力。不幸的是，我们这些基础设施固有的安全和防护机制客气地说也是很薄弱的。

1996 年 6 月 5 日，我的朋友、联邦调查局计算机犯罪调查组主任赛特勒在《今日美国》报头条撰文称“让我挑选几个黑客，在 90 天内我会把美国弄得服服帖帖。”这些年来，我们一直在提请当局和公众注意网络安全问题，现在大众传媒已注意到我们的观点。

读者将从本书了解到，赛特勒并非是危言耸听，这也是为什么我和本书其他作者提出要制定国家信息政策，因为它能提供电子民防。

感谢上天，我国和其他国家都还没有遇到电子珍珠港事件。但我仍坚持认为，与 3 年前本书第一版问世时相比，当前我们面临的形势更加危险，理由是：

●网络获得了极大的发展。

●整个社会更深地依赖四大关键基础设施。

●更多的国家和更多的人通过网络联系在一起。

●人们变得更聪明，知识传播面更广。

●美国在这个世界上的朋友越来越少。

在 50 和 60 年代，美国有民防计划。尽管我们在电视上看到

了原子弹爆炸的恐怖景观，当局还是告诉我们说，如果我们闭上眼，弯下腰，躲入地铁等等，我们就能劫后余生。可是目前我们却没有民防计划来对付现已存在和在不远的将来会出现的弱点与威胁。

让我们思考一下电子民防的事。历史上，坏蛋如果想打击美国，他们首先遇到的障碍是令人生畏的美军。但现在还有多少民族国家肯用潜艇和飞机进攻洛杉矶呢？实际上，华登上校不久前所设计的传统防御模式已经过时。

以往美国的防御主要由军队来进行，军队首先保卫民众，然后是国家基础设施（敌国可对此进行常规轰炸）。只有当敌人击败军队后，才能威胁到国家的根本，而最难打击的是国家领导人。

但在今天，防御模式已发生变化。我认为应该考虑新的防御模式。

聪明的信息勇士所要打击的第一个目标，肯定是敌人最薄弱的目标——经济技术基础设施，即通过打击敌人的重心打瘫敌人，引发多米诺骨牌效应。这一打击很快就会对敌国民众产生影响。在这一过程中，没有军队什么事。信息勇士的下一个打击目标是敌国的领导人，只有那些非常渴望对敌人进行实体性破坏，并且不怕敌人作出军事上的反应的进攻者，才会继续按传统模式发起进攻。在有其他选择的情况下，为什么信息勇士不选用新的模式呢？

因此，对于新的防御模式，如果我们不改变政策就意味着没有防御。在新的防御模式中军队没有直接的用途。我们所应该做的部分工作，是让军队在传统上不属军队所负责的领域发挥适当的作用。

假如我们已认定，经济技术基础设施是值得保卫的战略资产，那么我们怎么保卫它呢？谁来保卫它呢？谁来担任保卫和防御的责任呢？（人们通常认为，在公司和国家层次上的信息袭击主要来自因特网。我希望阅读本书后读者会发现这种观点是短视的。对

第三次浪潮社会及其经济技术基础设施的进攻，可以采取许多其他更有效的方式。）

有关谁负责统筹电子民防的争论是一个非常重要的、也许是决定性的问题。在军方、司法机关和其他行政部门竞相争夺预算的情况下，这个问题变得尤为重要。

我相信电子民防应该是一个多边的计划。美国公司必须参与国家电子民防，并要尽可能发挥作用，其作用不应该比政府小。即然因利益攸关我们都得参与电子民防，那么不应该把建立共同电子防御的责任完全交给政府或任何一个政府机关。作为个人以及作为一个公司，我们都要尽自己的一份力量，而不能把我们的安全单纯地寄托在‘政府老妈’身上。

但是，从政府的角度考虑，谁来牵头呢？

联邦调查局已经不堪重负。资金不足，任务过重，积案日多，它应付日常工作已很吃力，并且不时还会有俄克拉荷马城炸弹案这样的大事出来。随着网络事件的增多，电子防御将越来越重要，也会越来越困难。联邦调查局是忙不过来的。

联邦应急事件处理局单靠自己不能担负电子民防的责任，虽然它有很好的应急事件处理计划。中央情报局是对外的，国家安全局在通信方面是权威，但它不监听国内情况。商务部、财政部也各有其局限性，不能担负这一领导责任。

我认为，军队是担当电子民防的中心协调者的适当机构。军方中有些人会赞同这一见解，也会有许多人持反对态度，赞同也好，反对也罢，都会提出很好的理由。需要克服的最主要的障碍是1878年的《非常规警戒法案》，该法案规定除在特殊情况下，不得在国内动用美军。

一般情况下，法律禁止在国内动用美军。但谁来处理危机情况呢？军方拥有大量的资源（他们自己不这么认为），并有良好的做出有组织的反应的经验。但军队的确习惯于用炸弹、子弹和刺