信息高速公路

安全与防护

[美] Frederick. B. Cohen 著

陈安阳　　崔乃明

王步生　韩秋善　刘健辉　编译

中国人民解放军工程兵工程学院

信息高速公路

安 全 与 防 护

[美]Frederick. B. Cohen 著
陈安阳 崔乃明
王步生 韩秋善 刘健辉 编译
王 季 青 校

中国人民解放军工程兵工程学院
一九九六年八月

Protection and Security
on the Information
Superhighway
Dr. Frederick B. Cohen
John Wiley & Sons, Inc. 1995
New York. Chichester. Brisbane. Toronto

信息高速公路
安全与防护

[美]Frederick. B. Cohen 著
陈安阳 崔乃明
王步生 韩秋善 刘健辉 编译
王季青 校

中国人民解放军工程兵工程学院出版
(内部发行)

出版说明

电脑病毒已经成为未来高技术战争的秘密武器。军事专家认为“计算机中一盎司硅产生的效应，可能比一吨铀还要大”，未来战争将转向“打硅片”。当指挥员运筹于荧屏，指挥千军万马决战于高技术疆场之时，电脑病毒象“幽灵”一样威胁着计算机系统、危及军事安全、直至影响战争的进程与结局。“电脑病毒”作为一种人为编制的特殊计算机程序，对现代军事系统的干扰破坏作用主要是通过对敌各种信息化武器装备的“软杀伤”，既可实施单系统攻击，破坏敌人各种电子化作战平台，又可实施网络攻击，瘫痪敌方的指挥、控制系统。1988 年，就读于美国康奈尔大学的研究生莫里斯通过美国最大的网络系统，把自己设计的病毒程序输入五角大楼远景规划局网络，导致美军军事基地、国家航空航天局的 8500 台计算机瘫痪。海湾战争爆发前，美军利用伊拉克为防空系统购买电脑的机会，派特工将带有“病毒”的芯片装入其打印机中，通过法国卖给伊拉克，结果美军在战略轰炸前以无线摇控的方式激活隐蔽的病毒，造成伊军的预警、指挥、通信和火控系统全面崩溃，美军轻而易举地完成了轰炸任务。

如何迎接未来高技术信息战的挑战，《信息高速公路安全与防护》一书作了很好的回答。该书是 1995 年美国出版的一部信息基础设施安全与防护方面的最新专著，作者科恩博士长期从事计算机安全与防护研究工作，并取得了一系列重大成果。他首先提出了“计算机病毒”概念，今天全球一半以上的计算机系统均采用了作者研制的信息系统完整性保护机制。科恩博士作为国际公认的信

息基础设施安全方面权威，本书汇集了他在信息高速公路安全与防护方面研究的最新成果。其一系列理论与思想，对当前我国以“多金工程”为核心的NII及军事信息系统建设具有重要的借鉴与指导意义。

全书共分七章。由工程兵工程学院陈安阳同志组织翻译与出版。参加本书翻译工作的有王步生（第七章）、崔乃明（第二、三章）、陈安阳（第五、六章）、韩秋善（第一章）、刘键辉（第四章）、王季青博士担任全书的校审。

本书虽经译、校、审，编译者作了不少努力，但水平所限，时间仓促，疏漏之处，敬请广大读者批评指正。

本书的出版自始至终得到了工程兵工程学院教务部部长程宝义、科研处处长王耀华、教保处处长王者生等领导的关怀和大力支持，在此特致谢意。

编译者

一九九六年八月

此为试读，需要完整PDF请访问：www.ertongbook.com

目　录

第一章 导 论

最近你去过银行吗?当那里的计算机没有正常工作时,你是否能取到钱?在超市里,如果没有计算机核算货物,你能走出超市吗?你的汽车安装了控制燃料混合的计算机吗?在办公室,你的公司是否应用计算机给你发放薪水?你所在的供气站是否在供气泵上安装了计算机?

美国及其国民把依靠信息及信息系统作为竞争优势的重要部分,这已成为常识。但其依赖性不仅限于此,没有正常运行的信息系统,国家金融系统、电力网、运输系统、食品、水供应系统、通讯系统、医疗系统、紧急救援系统及大多数商业系统都将不能生存。

战争中信息至关重要,沙漠风暴作战是典型的一例。这场战争展示了美国有效地获取和应用信息的能力,同时也展示了美国阻止伊拉克获取和利用同等信息的能力。同样地,如果一个国家只是缓慢地依靠那些已被窃走或使用过的信息,那也将是一种教训。对掌握和控制部队所需要的通讯系统的破坏是伊拉克的最主要失败。最终导致伊拉克的经济也遭到彻底的毁灭。现在伊拉克已处于或低于大多数第三世界国家经济发展水平。

这种典型的教训已被其他国家和组织所认识和了解。在整个世界范围内,大家已经普遍认识到,在一个不重视依靠信息设施的国家,撤掉其信息设施,其结果亦是灾难性的,这种情况如果发生在高度依靠信息设施的国家,其结果又会如何呢?

美国已率先进入信息时代,但信息世界是一个危险的境地,有人经常在信息公路搞破坏,这里有一个典型的统计数字来说明我的观点:在交互网上每年就有九亿次的人为破坏。

财政损失经常作为增强信息防护的基本理论依据。例如，美国电报电话公司声称一九九二年其长途电话费被诈额增加到二亿美元。同时，美国联邦调查局统计数字表明，计算机犯罪年度损失额在 16.4 亿至 5 亿美元之间。这是一个巨大的数字，而且美国联邦调查局的统计数字似乎还不包括美国电话电报公司的数字。

财政损失仅仅是我们社会损失的一种形式。还有商业机密资料被窃、专利被竞争对手获得，因执法计算机的破坏、囚犯及其同伙被释放，国家税务计算机的失效使成千上万的小公司被逐出商界。周末假日，通过团体电话开关，经常出现价值上千元电话被人盗用，电话费单几乎无尽头。

流经信息公路的信息越多，保护人们不受侵扰的难度则越大；信息公路通往的地方越多，受伤害的人员亦越多。世界上最大信息网之一的 Internet 是一个很好的例子，目前，Internet 联接了 2 亿个计算机终端。与下滑的 1988 年比较，那时只有 60000 个终端在网上运行，之所以与之相比，是因为 Internet 病毒是在一九八八年发现的。在那次事件中，60000 个计算机终端上的人员，整整两天停止了所有的工作。1994 年 Internet 上的另一个事故发生了，至少有 100000 台计算机系统的密码被窃取，猎取者并没有被发觉，其破坏程度至少是上次的 25 倍。没有人确切地了解犯罪分子是如何对付那些密码的，但可以断定，犯罪分子至少在系统上检测或修改了估计有上亿兆字节的可利用信息。

但是我们应该正视这个问题，因为，要生活在现代时代，就必须去处理现代生活的风险。人们在刚开始使用汽车时，在公路上没有速度限制，没有交通警察及停车计时器。有些人死于早期的汽车轮下，但几乎在汽车普及 50 年以后的 1960 年，政府和制造商才采取一系列的安全措施，1994 年美国才强制性地在汽车上使用安全气囊。自二十世纪早期以来开始出现汽车抢劫；酒后驾车已经使成千上万的人丧命。现在因车祸而死已是很平常的事。

在信息时代，如果你想去哪里也许会利用信息高速公路，然而这就象交通公路上的事故与犯罪一样，计算机上没有安全带，犯罪分子很清楚如何进入计算机网络系统，正象犯罪分子知道在停车场如何进入你的汽车一样。如何才能保护好你的信息资源呢？如果这个问题能用一句话来回答，那么这本书确实应该是很短的。可喜的是，这个保护计划的基本框架已经建立起来。

·认识到你对信息的依赖性。每个人对信息的依赖程度是不同的，但在信息时代，其依赖性显得尤为突出，而且这些依赖性的相互关联作用更为广泛。信息工业生产了现代工具来处理信息，每一个依赖于信息的人，现在几乎都同样依赖于这些工具，在许多情况下，不夸张地说，没有这些工具，人们便不能生存。对信息基础设施的依赖的详细介绍，将在第二章“日益增长的依存关系”中阐述。

·认识到你所依赖的信息基础设施及对其开发程度的削弱。大多数人认为，多数计算机在大多数时间里是正常工作的，当他们偶尔出现问题时也极易修复。当然，你可能认为就是那些开发信息系统的人，一年内窃取了数十亿美元、帮助赢得军事冲突、获得谈判优势、毁坏他人名誉以至杀人。信息基础设施的弱点在第三章“破坏者就在我们中间”中讲述。这些问题的历史根源以及我们所面临的对策考量将在第四章“我们的失职”中讨论。

·认识到保护是你要做的，而不是你能买到的。这句话意味着什么呢？假如我要保护我们的住宅免受水灾破坏，我所购买的屋顶材料无关紧要，因为，我不打算永远地保护我的住宅，我只要使得我的屋顶不漏水即可，信息保护的道理也是一样的，不仅仅要购买信息保护材料，最重要的是如何来做。

今天大部分美国人认为，只要有钱便可解决一切问题。但在信息保护这个特殊领域，花费了时间和心血，效果大不一样。不管你是谁或你在做什么，都只能解决信息保护问题的一部分，而且，它影响到每个人。从周末在自动取款机提取现金的人，到世界上提供

先进信息技术的尖端技术专家，每个人都须起到他应有的保护作用，只有这样保护才能有效。要使我们自己在信息保护中有适当的作用，我们中间的每一个人都必须知道要做什么和怎么去做，常用的信息保护技术内容，将在第五章“保护信息资源”中介绍。

·信息保护优先原则。在大部分时间里，多数人完全忽视了信息保护问题，但在危机发生时人们又在短时间内把信息保护提到过高的位置，其结果只能是带来更高的成本和更大的损失。最有效的策略是，在长期的运行中使保护成本最低，即保护是一项循序渐进的工作，要使其在合理的时限用合理成本取得相应的保护水平。一些成功的案例将在第六章“保护形势案例研究”中说明。

在你阅读本书之前请注意，现实与现代技术社会所流行的认识观念差距太大，以致许多堪称专家的人，读完此书也许会认为，这里所讨论的威协可能是夸大其词。这里我至少可举一例，恰巧是多数人认为不可能的事情变为了现实。一九八八年九月，我向美国国家科学基金会提出了防治计算机病毒的研究建议，我们的技术观察员对我的回复是，像计算机病毒类的事情是根本不可能的，在现代计算机系统和网络中不可能有类似的事情发生。大约在得到这个答复三个星期后，Internet 病毒事件发生了，6 万多台网上的计算机感染上病毒长达两天时间。这也许是一个很好的机会，就在我的建议被高级研究专家否定数周之后事件便发生了。今天，成千上万的人们都知道计算机会通过世界信息系统传播感染病毒。

1.1 引　　言

本书所讨论的是计算机与通讯结合而产生的风险以及如何保证其使用环境的安全。作为政府机构首席调查员之一，我认为：此书宗旨是要发展和研究国家及政府部门的保护措施。书中的核心问题可以概括为：

此为试读，需要完整PDF请访问：www.ertongbook.com

- 我们都在依赖信息及信息系统
- 这些信息系统极易被破坏
- 许多人能够破坏这些系统
- 内部防护是最好的选择
- 保护是能做到的，而不是能买到的
- 大家都应该知道用什么方法自我防护

本书的其余部分将详尽介绍各级团体和组织，在自我防护中能够及应该做些什么和实际上已经做了些什么。

我们都依赖信息系统

在日常生活中，假如你已经理解我们都要依赖信息系统，但也许你不知道到底对信息系统的依赖性有多大。我们的电话系统、电缆系统、发电厂分压系统、许多的运输及供给系统、国家信息基础设施的每个部门等，几乎都由计算机控制。大多数国家信息基础结构的信息系统都已联网，实际上，世界上许多国家已进行内部联网。甚至美国军队都高度依赖其民防信息基础设施来实施指挥、控制、后勤供给、训练作业等。

简言之，我们的国家对信息基础设施的依赖性是相当巨大的，如果没有这些基础设施的正常运行，我们的国家乃至我们的生活将无法继续下去。

极其脆弱易损的信息系统

当你购买汽车时，通常销售人员不会告诉你，每年有多少人死于交通事故。购买计算机也一样，销售人员只会告诉你，一旦拥有

计算机你可以用它来做许多事情，它们是何等地容易使用，给我们的生活带来多么的方便，可用来储存信息、展示信息，在整个世界范围内可与其它计算机便捷联网等。

在交通事故中，有关汽车相互碰撞的报道有很多，政府部门也要求汽车必须具备一定的安全特性，以防止事故的发生或在事故发生时能减轻伤害程度。在现实生活中，人们故意开车相互碰撞的事情几乎不可能发生，如果有人这样做，那他们就会被指控犯有故意谋杀罪。而对计算机来说，则没有规定的防护要求，即必备的防护措施。部分计算机有极少的防护或根本没有防护，也没有法律规定你用计算机能或不能做什么事情，内部计算机系统（网络）通常对事故或故意破坏者是无保护能力的。

缺少必备防护措施意味着，防护对计算机硬、软件服务商是一种额外的花费，这只有通过消费者的需求来调整。这种消费者需求很大程度上取决于以下两种因素：一是市场；二是展现给人们产品销售或服务没有可察觉的安全风险。所以，此时除了节省授权的维修成本以外，提供计算机防护对供货商没有经济效益，其结果是现代计算机信息系统几乎完全失去有效的防护。

> 今天的信息系统极易遭受破坏，这本书就包含了几百个受到攻击从而导致金融财产损失，乃至系统瘫痪的实际例子，我举例的目的并不是想使这些攻击或损失由此而减少，仅仅是给出几个真实的例子而已。

信息系统正遭受许多人的破坏

世界上有许多人知道如何破坏信息系统，目前，有 30 多个国家已致力于研究有关信息系统的破坏技术及防护技术。其中许多国家已经研究开发出我们所需要的国家信息基础设施的相关技

术，但是，美国在此领域只取得小量成果。

> 整个世界范围内，已有几百个具有破坏国家大型信息基础设施能力的团体或组织。

能够破坏国家信息基础设施的组织包括：恐怖组织、经济竞争对手、雇佣组织、吸毒团体、有组织犯罪团伙及专业工作者个人。此外，国家信息基础设施中分系统损坏可导致与之相关连的其他NII部件的损坏。例如，发电厂分压系统是通过电话式通讯控制的，而电话系统的用电又取自于发电厂，如果破坏者能使发电厂某部分系统脱离线路10天，这将导致大面积电话通讯系统失效，致使电力设施无法控制发电厂的分压系统，从而使系统无法恢复。

如果注意不到全国性的系统崩馈，那么在小单位或团体内大部分人都知道怎样引起破坏的情况你应该是了解的。在几乎所有的现代机构中成千上万的人知道如何进入或破坏交互信息系统或网络。即使那些应用特殊"火墙"计算机来防护这种破坏或侵扰，都会被那些缺乏知识的攻击者轻而易举的击败。

来自这种破坏的损失是令人吃惊的。一些数字表明，由于信息系统的破坏，工业国家产品遭受其产品总额4%的损失，几份文件公布的损失已超过10亿美元，有些事故甚至造成了数十亿元的损失。

需要自我防护

实际上，国家信息基础设施包含了全美国所有内部联接的信息系统及通常用来联系工作的互联设施。当前这种互联计算机占全国的一半以上，其中包括了所有的电话系统、有线电视系统、卫星通讯系统及许多其它系统。

如果国家信息基础设施整个被破坏或破坏其中的一部分，那么，这对美国人民来说其危害是令人震惊的。

很显然，确保整个国家信息基础设施及组成部分的有效防护，是符合美国人们的最大利益的。

保护是你要做的而不是购买得到的

理解信息防护关键的问题是树立一个牢固的观念，那就是保护是你要做的事情，而不是你能购买的东西。事实表明，许多人认为，使用“火墙”计算机就可以保护联接于 Internet 上的内部网络系统，这是一种误解。

销售或经营产品的人总是声称其产品已解决了用户所有的问题，这是常见的事了，但遗憾的是，对信息保护来说，无一产品能解决用户的全部问题。

现在 Internet“火墙”保护系统已经推向市场，为一批有能力的专家队伍防止或测控来自外部的、有一定水平的攻击提供有价值的技术工具。但它并非是一种能防止各种攻击的通用产品。不夸张地说，从人事管理到欺骗性现代软件系统，有几百种方法可以避开类似这种安全防护系统。

为使“火墙”技术或其他保护技术具备有效的作用，该技术必须有正确的管理，熟练的专业人员操作，并训练用户正确地使用它，能较好地控制其发展变化。要使其切实履行保护职责，必须定期对它进行检测、审计，而这仅仅是事情的开始。

保护需要知识

保护行动的中心问题是获得正确执行保护所需要的知识。因

为信息的价值已渗透于现代生活的各个角落。因此必须对其实施保护。任何有价值的信息输送到哪里，哪里就必须有保护措施。这意味着，处理有价值信息的每个人都必须具备某种程度的保护作用。

我的女儿梅根只有十一个月，但她已经知道，在起居室不能接触录相机按扭。她的哥哥戴维年仅五岁，已经知道不能碰别人的计算机，不乱碰电线，手指不能接触磁盘发亮的部分。女儿六岁时，在操作计算机前就知道要先阅读屏幕上的操作指令，甚至还知道哪一个子目录不是属于她的，八岁时就知道，计算机如果过热会经常发生中断现象，她有一个私人信息文件以及用户 ID 口令及密码。当她离开一会儿时，她会将激光打印机临时关闭。

对整个国家来说，要使信息保护长期有效，每一个公民都有责任教育好自己的孩子，使他们知道计算机道德及信息保护的其他原则。我们都必须教育孩子使他们懂得，计算机并不总是正确的，可以信赖的，我们的孩子即需要有健康的体魄；同时也需要懂得信息技术方面的规矩，这是摆在我们所有人面前的任务。

如何进行自我保护

为了全面理解保护功能，单位各级人员都必须清楚地意识到保护问题为什么会涉及到他们每一个人以及这些问题是如何涉及到他们的。如果是有效保护的话，那么，从世界级的大公司的委员会主席，到小餐馆的盥洗室清扫工，都应该将其对信息保护的理解融入到相应的工作岗位上。

> 有效保护需要与不同领域人们之专门知识相结合，以提供一种良好的、满足要求的操作运行方法。

对夫妻店来说，提供保护功能可能意味着限制利用 NII 及其服务。对大型的商业机构来说，这可能意味着运行策略和进程的变换，长期保护义务与信息技术的长期承诺是一致的。对大型的跨国企业，这可能意味着更多的义务及投入，并且要求与世界各国人民进行合作。对军事和政府机构，这也许意味着要损失某些效率，以换取信息保护的有效性。

小　结

如果你正在购买计算机安全产品或遇到“终止”命令打算采用快速修复设施的方法时，最好能得到一位称职的专家帮助，给你制定一个合理的、响应及时的信息保护计划，然后，遵循这一计划，你将以一个较为合理的成本，获得长期的，而且有效的信息保护。

1.2 国家信息基础设施

“信息高速公路”是国家副总统戈尔在一次讨论关于应付国家信息基础结构突发事件的电话中提出的，这个有关计算机的术语，似乎遵循了汽车专业的传统。此书的剩余部分，我将应用术语 NII 或国家信息基础设施来描述这个逐渐发展起来的实体。

了解国家信息基础设施的构成，如何操作，它是怎样出现的，它将来会发展成一个什么样的模式，这对理解 NII 中出现的问题是很有帮助的。遗憾的是，没有人能在给定的时间，准确地描述 NII，因为它是在不断变化发展的，没有中央控制，而且其组成部分也是不断变化的。

在最近的一次讨论中，我利用 10 种不同的观察曲线，代表对 NII 的不同观点，从有线电视到电话系统，信息服务、卫星图像、光导纤维等等。描述完所有这些行业之后，在屏幕上我同时打出所有的幻灯片，并称这就是“NII”，当然，屏幕上这么多网络图形在一起，除了看到混乱的一堆外，其它什么东西也看不到，这就是对今

此为试读，需要完整PDF请访问：www.ertongbook.com