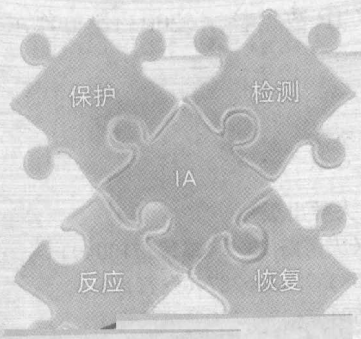
互联网安全法

马民虎 编著

西安交通大学出版社
XI'AN JIAOTONG UNIVERSITY PRESS

互联网安全法

马民虎 编著



西安交通大学出版社
XI'AN JIAOTONG UNIVERSITY PRESS

内容提要

本书综合运用信息安全保障理论、可持续发展理论、管理学、经济学的研究成果，结合我国互联网安全的实际情况，以预防、控制互联网安全风险为原则，以互联网安全文化观为核心，系统研究了网络空间权等互联网安全法的基本理论，全面阐述了我国互联网安全法的基本制度，如互联网隐私权、互联网安全监管、互联网安全紧急响应、互联网病毒防治、互联网用户安全保障、安全等级评价等法律制度，并且对互联网案件侦查以及违反互联网安全法律责任的特点进行了比较深入的研究。

本书适合于从事互联网安全监察的人民警察、国家保密人员和银行、证券、保险、电力、电信、广电、民航、海关、铁路等国家关键基础设施营运部门的信息安全人员阅读，也可以作为高等院校法学专业、信息安全专业的研究生教材。

图书在版编目(CIP)数据

互联网安全法/马民虎编著，刘正军，王伯平编 .—西安：西安交通大学出版社，2003.11
ISBN 7-5605-1770-6

Ⅰ.互… Ⅱ.①马…②刘…③王… Ⅲ.因特网-安全技术-科学技术管理-法规-研究-中国
Ⅳ.D922.174
中国版本图书馆 CIP 数据核字(2003)第 097786 号

书　　名	互联网安全法
编　　著	马民虎
出版发行	西安交通大学出版社
地　　址	西安市兴庆南路 25 号(邮编:710049)
电　　话	(029)2668357　2667874(发行部)
	(029)2668315　2669096(总编办)
印　　刷	陕西省轻工印刷厂
字　　数	670 千字
开　　本	727mm×960mm　1/16
印　　张	35.75
版　　次	2003 年 11 月第 1 版　2003 年 11 月第 1 次印刷
书　　号	ISBN 7-5605-1770-6/D·47
定　　价	68.00 元

前　言

互联网安全法是20世纪80年代以来法学研究的新领域。随着国际经济一体化的进一步发展和互联网技术的广泛应用，网络与信息系统的基础性、全局性作用日益增强，互联网安全问题已经成为人类社会发展过程中所面临的共同问题，严重影响着国家安全以及经济与社会的协调发展。网上有害信息传播、“病毒”入侵和网络攻击日趋严重，境内外敌对势力针对广播电视卫星、有线电视和网络的攻击破坏活动日益猖獗，网络恐怖组织“虎视眈眈”，严重危害着公众利益和国家安全，影响我国信息化建设的正常发展。如何正确处理“安全与发展”关系，建立以应急与预警、监控为核心的风险预防、控制制度，已经成为当前互联网安全法研究的主题。

目前，美国和欧盟在该领域的研究处于国际领先地位。如何有效协调互联网安全活动中公权益和私权益之间的冲突，始终是美国法研究的热点；“适度安全”和“社会参与”是美国法研究的最为明显的特征；建立以CIO为核心的信息安全领导体制是美国法研究的重大理论成果；重视网络信息安全的评价分析则是美国法最新的发展动态。

“电子欧盟”作为欧盟的一项重大战略，有关互联网安全的法律指令、决议和框架协议无不体现经济“一体化”的利益价值。商用密码技术与产品的适度开放、个人数据的充分流通与利用、关键基础设施运营的安全保障为欧盟法研究的主要内容；重视成员国的计算机应急响应机制，特别是对病毒等对网络和信息系统攻击的预警、预防和检测制度建设是欧盟法研究的新特点；加强共同体内、国际间的网络和信息安全事件的信息交流，强调提高全民，特别是企业，私人用户，公共管理部门的网络和信息安全意识，推广基于国际公认标准的信息安全管理措施是当前欧盟法的新发展。

加强对互联网安全法的研究，符合我国推进国民经济和社会信息化，以信息化带动工业化，实现社会生产力的跨越式发展的战略要求，是惩治国际敌对势力信息渗透、干扰、破坏活动和反独、反恐斗争的特殊需要，是应对WTO规则给我国传统信息安全监管模式提出挑战的艰巨任务。

“发展是硬道理”，我们应当强调在信息系统和网络发展中解决安全问题，应当确立积极的风险预防和风险控制的法制原则，关注信息内容安全监控，树立安全使用信息系统和互联网的新型法律文化理念。

国民经济和社会对以互联网为核心的国家信息基础设施的依赖程度，是我们研究互联网安全法的基本点。在计算机网络技术的应用初期，相对独立的信息系统还没有取得基础设施这样重要的地位。因此，财产权和隐私权、国家利益各自特

有的保护方式决定了该时期法的目的定位，“未经授权”则是该时期法的基本规范模式。当信息系统发展为国家关键基础设施后，“病毒”也随之成为人类社会的一种新型“公害”，网络恐怖活动更是肆意猖獗。信息安全与国家安全、社会公共安全的关系变得更加密切。适应信息安全保障的要求，法律十分关注信息安全与应用领域政策的统筹考虑。这在法律规范上的表现就是加强信息监控，强调信息安全策略的规划，关注信息安全风险责任有效控制原则的落实。随着人类社会对互联网空间的高度依赖，互联网空间与物理空间相互依存。保障互联网安全需要政府和全民的共同参与，强调所有参与者的责任。基于对互联网安全的新认识，立法重点发生了从对信息基础设施保护到国家关键基础设施保护的转移，强调物理空间安全与互联网安全之间的关系，要求建立应急响应、检测预警机制，重视监控和信息共享，强调推动民营资本安全技术研究的重要性。可见，“依赖性”决定着互联网安全法的目的定位及其调整范围。

本书从构思到成稿经历了比较长的时间，部分内容曾在西安、北京、上海、新疆、郑州、深圳等地的多种场合与有关专家、学者进行过广泛的交流。有些观点的形成得益于西安交通大学章德安、潘宇鹏、宋雅莼教授的教诲，有关内容曾受到国务院信息办郑静清副司长的启发。在研究和撰写过程中，陕西省公安厅郭明副厅长、公共信息网络安全监察总队苏欣总队长给予了大力支持，公安部公共信息网络安全监察局赵林、景乾元处长的诸多观点在书中尽可能地得到了反映。西安交通大学法学系李霞副教授、陕西省保密局王二鹏、电子政务办王力、信息办崔江宏、宝鸡市公安局李岩同志提出了许多有益的建议，陕西省公安厅武向阳审阅了部分章节，祁荷香、贺晓娜在校稿过程中花费了很大的精力，王宏波、张思锋教授给予了悉心指导，西安交通大学出版社李志孝编审在策划、编辑稿件中付出了艰辛的劳动，在此对他(她)们一并表示感谢。

本书大纲由马民虎拟定。采取收集体研究，分工执笔的方式，撰稿人有马民虎(第一章、第二章、第十五章)，原浩(第三章、第九章、第十章、第十一章、第十二章、第十三章、第十四章、第十六章)，张雁(第四章、第五章、第八章)，董志芳(第六章、第七章)，乔雅辉(第十八章、第十九章、第二十章、第二十一章、第二十二章)、王伯平、马玲(第十七章)。王伯平、刘正军两位副主编修改了部分章节。

技术在发展，互联网安全法的认识也在不断完善。因此，研究互联网安全法的规律，挖掘其发展趋势，需要有战略的眼光、坚实的法学基础理论功力和跟踪信息技术发展的能力。由于我们的才疏学浅，力不从心，书中不足之处，甚至错误的看法，希望读者批评指正。

马民虎

于三村寓所

目　录

中编　中国互联网安全法各论

下编　互联网安全法律责任分论

第一章 导 论

第一节 互联网及其安全问题

一、互联网安全的概念

网络空间(Cyber space)是信息社会的神经系统。网络空间由遍布在世界各地相互连接的计算机、服务器、路由器、交换机、光纤电缆和无线通信系统等组成,支撑和控制着农业、食品、水供给、公众健康、应急服务、政府办公、国防工业、信息与能源、交通、银行、证券、保险、化学与危险材料等国家关键基础设施的运行。因此,网络空间保持正常状态对社会稳定运转和国家安全,乃至国际社会安全起着至关重要的作用。

互联网是网络空间的主要形式①,其互联互通的特点改变着当今社会人们的生活方式和工作模式,维护互联网安全是保障国家安全、社会公共安全和社会成员财产安全、人格利益整体战略的重要组成部分。

何谓互联网安全,现有不同的说法。

欧共体从抵御攻击的角度认为,互联网安全可被理解为在既定的密级条件下,网络与信息系统抵御意外事件或恶意行为的能力。这些事件和行为将危及所存储或传输的数据以及经由这些网络和系统所提供的服务的可用性、真实性、完整性和秘密性。②

经合组织(OECD)"2002 年安全指南"则从互联网参与者的责任角度认为,互联网安全实质上是一种网络与信息系统的安全文化,要求互联网参与者履行互联网安全责任,强调提升互联网安全意识,及时对危害互联网安全事件做出反应,不定期地评估网络和信息系统的安全风险。这与经合组织 1992 年发布的"信息系统

① 互联网由众多的网络组成。互联网为分级的互联结构。在最顶层是 5 个全球最大的互联网骨干网 AT&T、Sprint、MCI－Uunet、Cable&Wirelesss 和 GTE,它们在一些著名的交换中心进行对等互联;第二层是全国性的骨干网;第三层是地区性的 ISP,指在某一地区范围内,通过一个或多个点提供服务的 ISP;第四层是众多为个人或中、小型企业提供 Internet 服务的 ISP;第五层是最终用户。我国目前有教育网(CERNET)、科技网(CSTNET)和金桥网(CHINAGBN)、公用计算机网(CHINANET)、中国电信 163、中国网通 169、中国联通 165 等 11 家互联网骨干网;国家先后在北京、上海和广州开通了互联网交换中心(NAP)

② Network and Information Security: Proposal for a European Policy Approach 2001

安全指南”有所不同。虽然“信息系统安全指南”已经认识到信息系统的跨国性，这些系统在社会和经济活动中发挥着日益重要和深入的作用，是国民经济、国际贸易、政府和商事业务、健康、能源、运输、通信和教育事业的关键基础设施，但该指南从信息系统安全的客体出发，认为信息系统安全是指确保信息系统的可用性、完整性和机密性，这显然忽略了利用互联网在“任何时间、任何地点”存取信息系统的特点。①

美国《网络空间安全国家战略》认为，互联网是美国经济和国家安全所依赖的最重要的信息基础设施，互联网安全是美国国土安全的应有内容。该战略号召美国人参与他们所拥有、使用、控制和交流的网络空间安全保护，实现保护美国关键基础设施免遭网络攻击、降低网络脆弱性、控制网络灾难所造成的损失和建立快速应急响应机制。

应当注意到，在美国，信息安全是互联网安全的核心内容。2002 年《联邦信息安全管理法》规定，信息安全是指确保信息和信息系统避免非授权访问、使用、披露、中断、修改或破坏，以实现完整性、机密性、可用性。

用于国家安全的信息系统被称为“国家安全系统”，它指任何类型的信息系统（包括任何类型的电信系统），可以为任何机构、机构事务承包人或其他任何代表机构的组织使用或操作。该信息系统的功能、操作或使用包括：

（1）情报活动（Intelligence Activities）；

（2）与国家安全有关的密码活动；

（3）军队命令和控制；

（4）构成武器或武器系统完整性部分的装备；

（5）从属于日常管理和商务应用系统服务的重要直接军事活动或军事任务的履行。

国家安全系统始终处于信息程序的保护，且该程序已被生效指令或国会用以确保国防或对外政策利益机密性的法案明确授权。

上述定义虽然文字表述不同，但其基本含义却是一致的。所谓互联网安全，是指为防止意外事故和恶意攻击而对互联网、应用服务和信息内容的保密性、完整性、可用性、可控性和不可否认性进行的安全保护，其中：

保密性指保证国家秘密和敏感信息仅为授权者享有；

完整性指保证信息从真实的信源发往真实的信宿，传输、存储、处理中未被删改、增添、替换；

可用性指保证信息和信息系统随时可为授权者提供服务而不被非授权者滥

① 经合组织 1992 年发布了“信息系统安全指南”。2002 年第 1037 次理事会上发布了新的“信息系统安全指南”。

用；

可控性指保证信息和信息系统的授权认证和监控管理；

不可否认性指保证信息行为人不能否认其信息行为。

二、互联网安全问题

现在，人类社会比以前任何时候都更依赖于互联网。但是，人们对网络的安全意识却远远滞后于运用互联网的商业意识。由于互联网在社会和经济发展过程中扮演着越来越重要的角色，商业利益的巨大驱动力使互联网建设与安全保障相分离，不同步，忽视对互联网安全产品开发、信息安全人员培训、网络安全管理策略和标准的研究和推广，结果给人类社会发展造成了严重的互联网安全问题。

请看以下事件：

(1)堪萨斯州(Kansas)上空的通信卫星失控，超过 35 000 000 个美国人的寻呼机停止工作。

(2)美国某一大区域内的电话服务被切断——造成一个重要地区机场内的所有联系中断，威胁到航班的最后着陆。

(3)美国两个最大城市的美国“911”救援服务瘫痪，引发了混乱，所有救援行动因此而变得迟缓，并导致了潜在的不必要死亡。

(4)1998 年 2 月中旬与伊拉克的冲突中，发现了针对美国陆、海、空三军以及国防部后勤和计算机保障系统进行的大范围入侵。美国军方并不知道入侵源于何方，也不知道入侵已持续了多长时间以及哪些信息遭到了窃取和篡改。

(5)一种新的计算机病毒在互联网上正迅速扩散，通过寄发大量的电子邮件使系统过载，导致很多公司和政府系统被迫关闭。

(6)美国国防部副部长 Dr. John Hamre 证实“这个世界正变得越来越不太平，我们已经提高了对网络活动进行监控的能力，可以观察到的探测、入侵行为和其它计算机事件的数量持续增长。目前我们每天能检测到 80 到 100 起事件，其中约有 10 起需要做进一步的调查。”

(7)1998 年，一家电信公司在其 Internet 接口处安装了一个入侵检测系统，每月约发现有 4 000 次入侵尝试。尽管大部分是无害的扫描，但其中也有数百起是攻击性的，这些攻击试图侵入他们的数据库并转移走电话卡上的金额。

(8)1998 年，一个民航公司对其计算机系统的脆弱性做了一次评估。模拟攻击中，作为攻击方的红队(red team)能够破解他们 90% 的业务，并可以访问他们的工资数据，更为危险的是，红队甚至能够侵入航班数据录入程序。

(9)为抗议美国 1999 年 3 月的军事行动，有人对 5 个联邦非国防机构的计算

机系统同时发动了攻击，攻击手法是利用 E-mail 炸弹或修改及破坏主页。

从 20 世纪初开始，摧毁或破坏为军事力量提供支持的通信、供给和经济基础设施就成了一条重要的军事原则，被认为同攻击军事力量几乎同等重要。而计算机时代的到来则为潜在的敌对势力提供了全新的选择。国家关键基础设施正处在以前看起来还遥不可及的攻击威胁之中。

如今国家依靠互联的信息系统来执行电信、能源、运输、经济和国家安全职能。但这些网络在由技术"天才"群体发起的破坏和入侵面前非常脆弱，且少有例外。作为敌对势力的主要攻击目标，网络空间正面临着越来越大的危险。商业网络所面临的危险和政府网络形势同样严峻。

（一）日益增长的网络依赖性

当代社会以信息经济为主要发展趋势。制造商、金融机构、运输商等其他商业机构、国家和地方政府都在全力建设信息网络，以提高效率、降低成本或开发新型业务。

生产商和供应商现在可以使用网络连接实现面向消费者实时需要的产品生产，从而降低生产成本。在美国，电力和通信业务提供商已把它们的控制系统进行了互联和内联，为消费者提供更加快捷而廉价的服务。计算机互联网在能源、水利、金融服务和运输服务中正在普及，信息化成为了促进工业化发展的先进生产力。各级政府也运用网络和基础设施来提供基础服务。

没有哪一种基础设施比电力更能积极地促进计算机的变革。更重要的是，电力基础设施是国家其他基础设施的血液，因而它的安全保障是国家安全和经济稳定的关键，并且，它对于紧急医疗、消防和警务服务也非常重要。

电网上的任何脆弱性都必须得到详细确认并完全改正。美国电力系统框架如图 1.1 所示。

通过信息网络，商界和政府可以获得显著效益并开拓新型服务。但是，在这场技术变革中，由于曾对技术发展的不理智决策，使公司和国家对这些系统特别依赖。国家的经济力量，众多的商业利润和生存能力以及政府的职能运作现在都极大依赖于这些复杂网络的运行可靠性。

（二）互联网的脆弱性

现在，对很多网络系统所采取的故意入侵只需要低廉的成本和很少的时间，且非常容易。信息基础设施的很多脆弱性在入侵者间广为人知，[①] 他们可以通过互联网和其他途径共享这些信息。很多强有力的攻击方法可利用设计精巧的程序自

① 以计算机操作系统为例，Windows 2000 和 Windows XP 系统的 rpc 脆弱性漏洞就被黑客利用，并在 2003 年 8 月造成了巨大灾难。

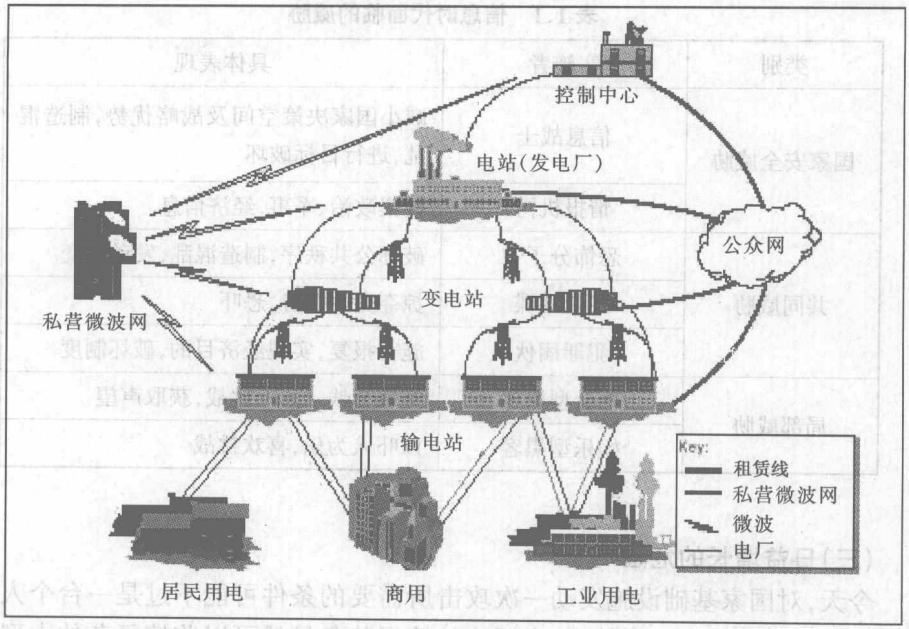


图 1.1 美国电力系统框架图

动完成,在 Internet 上很容易获得计算机盗窃的工具套件。任何意欲攻击信息基础设施的人只需要在设备上投入极少的资金、掌握中级水平的技术能力、拥有一套容易组装的工具以及了解一些可以从网上或其他开放资源处获悉的系统脆弱性和攻击技术,就可以轻松完成对这些基础设施的攻击。

计算机入侵者面临的风险极小。不同于攻击物理性基础设施,对信息网络的计算机攻击不需要物理上的接近。攻击可以来自世界上任何地方,通过互联网、其它网络和拨号线路的一种或几种的组合来施行。经由多个通信网络和计算机链发动攻击,入侵者可以有效掩盖其身份和位置,追踪这些攻击却非常困难且耗时极多。

计算机入侵者能够轻易地采取声东击西战术来隐藏其真实意图,从而达到预期的效果。入侵者可以使用病毒包括网络蠕虫、特洛伊木马等,计算机时间炸弹以及其它自动攻击方式来轻松使成千上万的组织和网络陷于瘫痪。计算机入侵者可通过这些行动将系统和网络操作员、安全事件响应小组以及事件调查组的注意力从其真实攻击目标上转移开。当"背景噪音"达到相当的程度时,对关键系统的攻击可以变得神不知鬼不觉。表 1.1 对信息时代面临的种种威胁做了总结归纳,供参考。

表 1.1 信息时代面临的威胁

类别	实施者	具体表现
国家安全威胁	信息战士	减小国家决策空间及战略优势，制造混乱，进行目标破坏
	情报机构	搜集政治、军事，经济信息
共同威胁	恐怖分子①	破坏公共秩序，制造混乱，发动政变
	工业间谍	掠夺竞争优势，恐吓
	犯罪团伙	施行报复，实现经济目的，破坏制度
局部威胁	社会型黑客	攫取金钱，恐吓，挑战，获取声望
	娱乐型黑客	以吓人为乐，喜欢挑战

（三）日益增长的危险

今天，对国家基础设施发动一次攻击所需要的条件可能不过是一台个人计算机以及相关信息技术。高精度、多用途的情报装备虽然可以监控复杂的大型军工综合设施，但敌对势力却不需要去使用这些被监控的设施。对国家攻击可以来自任何地方的一台计算机——在敌对国或是友邦，甚至就在本国境内。这些恶意甚至敌意企图的攻击，试图以电子方式阻止对关键性信息网络的访问，阴谋通过控制或改变我们的信息系统来达到欺骗的目的，或进行传统间谍及经济谍报活动。

1. 信息战威胁

发展中的信息作战能力正在成为现代战争的重要军事能力。有的国家正在开发侵略性计算机网络应用(CNE——Computer Network Exploitation)和/或计算机网络攻击(CNA——Computer Network Attack)能力。尽管很少有人公开谈论他们的这些开发工作，但是在一些国家的公开出版物上可以看到他们对 CNA 价值的讨论：

“一个想要对美国进行摧毁的敌手只需要用先进的技术扰乱银行的计算机系统，就可以损害和破坏美国的经济。如果我们忽视了这一点，只是单纯依靠建立一支耗资巨大的常备军队，那简直就如同建造可笑的马其诺防线。”

“在适当级别上保持我们核威慑潜力的同时，我们必须对全面的信息战投入更多的注意。”

——美国对 CNE、CNA 的关注

① “网络恐怖”一词最早由美国加州安全与智能研究所的资深研究员 Barry Collin 博士于 1997 年提出，用于描述网络空间与恐怖主义结合的现象。随后，又有安全专家给“网络恐怖主义”下了一个明确的定义，即：“网络恐怖主义就是由亚国家集团或秘密组织实施的有预谋、有政治动机、针对信息/计算机系统、计算机程序和数据进行的攻击行为，这些行为可能对一个国家的非战斗目标造成严重的破坏。”

2. 经济竞争者

经济间谍窃取商业情报或商业秘密的情势在互联网时代日趋严重。据美国克林顿总统的“关于外国经济情报收集和工业间谍向国会提交的1998年年度报告”，已有为数不少的国家盯上了美国的工业和经济信息。不仅仅是官方情报机构参与了谍报活动，一些外国主要的工业部门也在其国家商业情报工作中发挥了主要作用。他们瞄准美国民众、工厂、工业和美国政府，偷窃先进的关键技术、贸易秘密、财产信息以及研发成果，这种威胁长久以来就一直存在着。这一情势对我国也同样存在。

3. 犯罪分子

计算机犯罪活动给公司造成了巨大的经济损失。信用卡公司、电话公司以及金融机构都在这样一个计算机犯罪激增的大环境下进行经营。Ernst and Young “InformationWeek”的一次调查表明，在过去的五年内，超过72%的美国公司发现他们的数据正面临着不断增长的安全威胁。

有组织的犯罪集团正日益引起各国执法部门和国际社会的密切注意。这些犯罪集团借助高科技用于各类目的，不只为了获得经济利益和竞争优势，还试图获取警察计算机和网络中保存的敏感性执法信息。

据2002年4月美国FBI“Internet欺诈投诉中心”的调查，在2001年1月1日～2001年12月31日期间IFCC网站接受了49 711起投诉，欺诈总损失1 780万美元，每起平均损失435美元。发生欺诈最多的前十个国家是：美国(93.4%)，加拿大(2.2%)，英国(1.0%)，澳大利亚(0.5%)，日本(0.2%)，德国(0.2%)，新加坡(0.2%)，印尼(0.1%)，新西兰(0.1%)和南非(0.1%)。

犯罪者主要来自：美国(87.6%)，尼日利亚(2.7%)，加拿大(2.5%)，罗马尼亚(0.9%)，英国(0.9%)，南非(0.5%)，澳大利亚(0.4%)，印尼(0.3%)，多哥(0.3%)，俄罗斯(0.2%)。

很难准确估计公司受到攻击的程度。某些情况下，甚至无法对公司的损失程度进行明确地判断。而且有的单位对事件进行保密，因为他们担心由此造成的负面影响。1996年参议院少数派报告恰如其分地揭示了大多数公司的想法：

“由于害怕影响顾客或是持股人的信心，商业部门不愿意报告计算机入侵事件。一般情况下，公司内的人士可能向职员透露他们已遭受入侵的消息，但不会将事件报告给政府和其他机构，因为他们担心这些事件进入公众视野。”

4. 黑客

黑客曾经是那些十多岁的计算机天才和极度狂热的程序员，他们并不热衷于犯罪或恶意行为，他们的行为被认为是受好奇心和挑战欲望所驱使。不幸的是，新一代的黑客看起来是受贪欲或恶意所鼓动，而不再是简单的好奇心。黑客已开始