国际犯罪学丛书

网络犯罪

威胁、风险与反击

[法]达尼埃尔·马丁
[法]弗雷德里克-保罗·马丁 合著

卢建平 译

中国大百科全书出版社

网络犯罪

[illegible]

网络犯罪

——威胁、风险与反击

达尼埃尔·马丁
弗雷德里克-保罗·马丁 著
卢建平 译

中国大百科全书出版社
北京

总编辑:徐惟诚　　社长:田胜立

【京】图字:01-2001-5525 号

Cybercrime: Menaces, vulnérabilités, et ripostes par Daniel MARTIN et Frédéric Paul MARTIN/ISBN 2-13-051939-31 ISSN1275-3149

图书在版编目(CIP)数据

网络犯罪:威胁、风险与反击/(法)马丁(Martin, D.),(法)马丁(Martin, F.)著;卢建平译. -北京:中国大百科全书出版社,2002.12

ISBN 7-5000-6708-9/D·105

Ⅰ.网… Ⅱ.①马… ②马… ③卢… Ⅲ.计算机犯罪—研究 Ⅳ.①D.914.04 ②TP309.5

中国版本图书馆 CIP 数据核字(2002)第 087014 号

Ouvrage publié avec le concours du
Ministère français des Affaires Etrangères
该书由法国外交部资助出版

策 划 人:刘海英
责任编辑:刘海英
责任印制:紫玉书

中国大百科全书出版社出版发行
(北京阜成门北大街 17 号　邮政编码 100037　电话:010-68315609)
网址:http://www.ecph.com.cn
新华书店总经销
河北大厂回族自治县彩虹印刷有限公司印刷
开本:850×1168　1/32　印张 8.625　字数 210 千字
2002 年 12 月第 1 版　2002 年 12 月第 1 次印刷
印数:1~5000 册
定价:18.00 元

前 言

本书初版于1997年，当时的书名为《信息犯罪、网络犯罪：破坏、劫掠等，演化与打击》。从那时起到现在，当今世界信息与通信新技术的局面已经发生了巨大的变化。互联网铺天盖地，古老的欧洲大陆也在互联网上不断缩小着与美国的差距。这一现象如今已全然是世界性现象了，其格局也与以往明显不同。全球化正在加剧，技术进步又使其面貌焕然一新。例如，作为未来计算机核心的新生代产品芯片已经问世。它们在体积上与原子相差无几，工作速度几乎可以与人的大脑神经的反应速度媲美。它们将开启一个崭新的时代。在这个崭新的时代中，语言或语音识别将成为人机对话的正常方式：资料存储极限不复存在、辅助系统的微型化，将使人们的工作变得无忧无虑，不必再考虑什么信息的数量；通信的速度和网络的可靠性将使时间和空间的概念荡然无存。图像、声音、数据、软件、各类网络世界之间的相互沟通将成为一个全新空间的标志，这个新的空间就是“新文明空间”。

正是因为上述原因，本书的新版和初版相比就有了很大的不同。新版更加关注实际案例，重视发展变化，并对未来寄予很大的期望。

至于本书中的新网络犯罪，应该理解为是在一个不断发展演化的进程中某一特定时刻某一情景的缩影，是一张快照。

与传统的案件侦查一样，我们从具体个案的枝枝节节中得出最初的结论，然后再去考虑反击和防卫的方法。当然，我们始终强调的，而且越来越强调的，是无处不在的人的因素的重要性。

一个全新的世界格局

世界秩序的瓦解是一场名副其实的地震。各种特权，那种非敌即友、非友即敌的两分法，甚至参谋本部的各式地图，也都成了“明日黄花”。传统的军事艺术对于这个新的世界已经不再有什么影响。试想，我们怎么去侵略互联网？怎样去轰炸一个教派？又如何对一个黑社会组织实施核威慑？

无数的挫折、残酷的现实告诉我们，过去的敌人，如今已经成了合作的伙伴，但也就在同一瞬间，传统意义上的盟军，如今也变成了兵戎相见的残酷的竞争对手。

经济力量和技术因素有利于全球化，因而也呈现加速发展的态势。电信领域的创新与信息技术始终在发展，可以说是日新月异。通信和交通费用的下降极大地促进了交换。今天，得益于信息的储存和处理方法（个人计算机越来越好、软件越来越完备），得益于通信状况（卫星、光纤、网络、互联网等）的改善和进入这些现代化通信方式的民主化进程（据统计，2001 年已经有 7 亿人上了互联网），人们几乎可以删除一切时间和空间的概念。一切都是实时地以电子速度在进行着。人们甚至可以说，几乎所有的一切都是可能的。我们现在确实同时面临着三大革命的联合：其一是通信技术发展所带来的技术革命；其二是企业为拓展新的市场所引发的地理革命；最后是资本流通与储蓄管理全球化所带来的金融革命。

在这个崭新的全球化时代，竞争波及到了一切领域，如经济、政治、金融、社会、语言，而信息、知识和智力占据了最显要的位

置。也可以如此断言:我们已经进入了信息时代,或者说进入了这样一种状态,即为了占领市场、挤垮对手、欺诈客户、刺探对方的战略意图、放毒、设圈套,人们可以无所不用其极。

在这种新的环境中,我们的社会也就变得特别脆弱。这既反映在公共权力的层面(因为其脆弱的基础设施并非无懈可击),体现在企业的层面(因为信息风险已经成为企业的头号大敌),也体现在公民身上(因为公民的基本权利,尤其是其个人隐私方面或作为消费者的权利,也会受到侵犯)。而对于所有这一切的来临,也许我们仍然浑然不知,因为我们面对的是一个潜在的世界。威胁正在逼近机器设备、软件以及管理着这些信息的网络与各种计算机资源。这种威胁表现为物理破坏、非物质破坏或资料的毁损。

犯罪分子们很快就适应了这个潜在的世界,也很快利用了这个潜在的世界所提供的各种便利。实际上,以电子速度实施的交易指令执行的快速性、数字化数据编码所提供的私密性、交易的非物质性肯定会刺激有组织犯罪。在20世纪80年代,只有10%的罪犯懂得一点电子学或信息学的知识,而如今,这一比例已经高达90%。这个增长过程分成几个阶段,它与信息处理发生的变革也是密切相关的:

——20世纪70年代,是信息学普及的时期,主要犯罪行为是软件盗版和假冒信用卡;

——自1980年起,各种区域网、局域网的相互联结导致诈骗资金大案的出现,攻击美国航空航天局(NASA)或五角大楼系统的电脑黑客开始作祟;

——20世纪90年代,信息知识的扩散、信息系统的发展、互联网的普及,开创了虚拟、潜在世界的新纪元,也仿佛为一切形形色色的犯罪活动打开了地狱之门。

目 录

第二部分 反击

第三部分 未来与机遇

附 录 一

附 录 二

附 录 三

第一部分

威胁与风险

第一章

分　类

信息系统所面临的、可能导致重罪与轻罪的威胁多种多样，为了不致在这样的迷宫中迷失方向，我们有必要对这些威胁进行分类。

系统安全包括系统的完整性、持久性和私密性[①]等内容：

——完整性是指保障信息或某个过程不受篡改地存在和储存的属性；

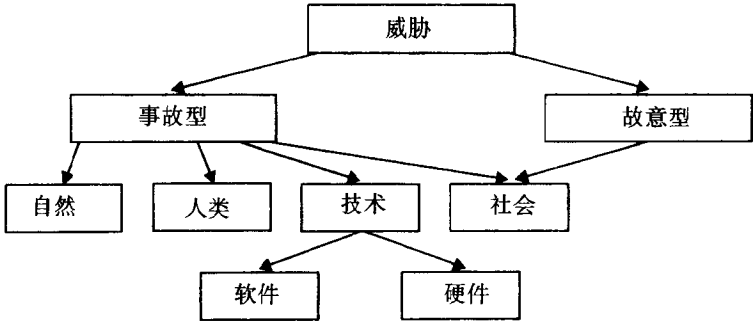
——持久性是指完整性在时间上的延续；

——私密性指的是只有在正常规定的条件下获得授权的使用者才能够访问信息(包括代码、资料、处理、关系、程序等)。

而风险则可以分成很多的类别，例如法国标准化协会(AFNOR)的分类，或者法国信息安全俱乐部(CLUSIF)的分类，这些分类所涉及的均是相同的概念。首先我们将威胁分成事故类和故意类两大类，按原因又可以分成自然原因和技术原因，而技术原因中又有软件方面和硬件方面的两种原因。最后我们也关注涉及企业的内在的或外在的人的因素，这些因素在所有情况下都是可以互相渗透的。我们这里要识别的是所有的风险，并在考虑系统的性质和边界的同时对这些风险作深入的考察。

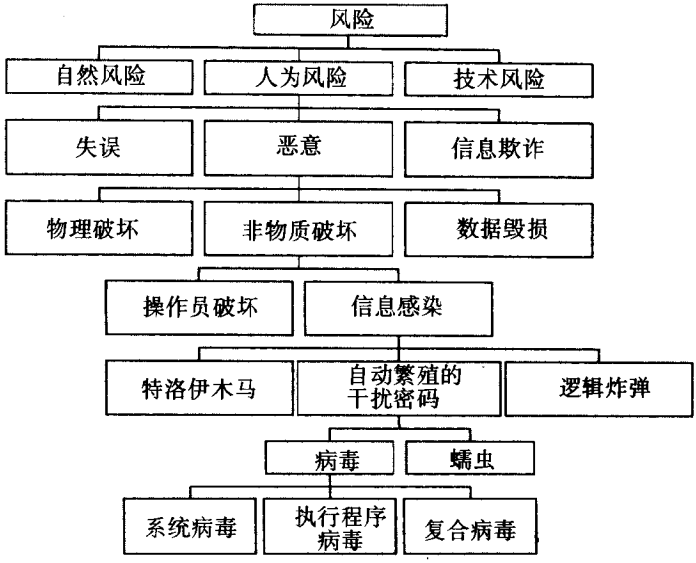
法国标准化协会对威胁所作的分类如下图：

① 见法国标准化协会编《信息安全与数据保护》。



资料来源:AFNOR

法国信息安全俱乐部的“信息风险图”如下:



资料来源:CLUSIF

4

一、自然风险

系统都是被安装在网站中的。网络也和其他任何设施一样，会因为洪水、地震或雷电的袭击而受损失，会受到液体或气体的污染，而这些自然灾害会给企业的命运带来极其严重的后果。

在选择建立信息网站地点的时候，人们很少会有兴趣去研究上述自然风险。这是一个错误。在人们作出决策之前，应该对建立网站的占地情况、环境等进行认真的研究。

雷电可能使计算机内部的集成电路熔化，并破坏机器内尚未执行完毕的运行过程。如果将网站设在临近河流或某个排水口边的地下室内，该幢楼房又没有建造防渗墙，而人们又因为疏忽没有考虑百年一遇的洪水最高水位的话，那么其结果就是不堪设想的。

最近就有一个例子。在去年夏天美国渥太华州下了一场特大暴雨，淹没了很多楼房的地下办公室，其中就有一家信息系统维护公司。该公司的直接经济损失高达几十万美元，而该公司有部分财产并没有投保，因为公司根本就忽略了这一点。由于这家公司是一家独立的计算机实验室，其拥有的设备是专门的、独一无二的，因此公司的损失不仅影响了公司自身的利益，而且也波及其客户。由于事先没有采取任何的防范措施，使该公司受到了重创，其业务直到灾害发生三个月以后才得以恢复。

二、技术风险

技术风险主要涉及设备的运行，涉及空气调节、电力供应、火灾、灾后重建所需要采取的措施以及后勤保障等。

我们所采访过的大部分网站在这方面均有缺陷，由此而带来

的惨痛教训不胜枚举：

——1999 年 7 月，某数据采集中心的大楼发生火灾，幸亏一位警惕性高的员工发现了烟雾，消防队及时赶到，火势才很快被控制住了。但是很多的机器和打印设备都在火灾中被烧毁了。由于要清理被烟熏火燎过的办公场地、整修房屋、更换损毁的设备，该中心被迫关门 5 天。

——更让人料想不到的是，啮齿目动物有时也会成为计算机故障的罪魁祸首。在 20 世纪 90 年代，日本通产省的计算机常常出故障。经过调查，发现是一群老鼠咬断了电线。电源启动时的嗡嗡声和 24 千赫兹波段的频率传送，在老鼠们听来如同是就餐的铃声。正因如此，现在的一些网站为了避免老鼠们的骚扰，专门配备了超声发电机。

——1999 年 9 月，负责向美国下曼哈顿区供电的一家电厂发生了爆炸，引发了很多计算机数据中心（其中包括纽约证券交易所数据中心）的一连串事故。纽约证券交易所被迫提前休市，使大量的难以计数的交易无法进行。

虽然从技术角度说，这些风险并不难控制，但是它们也不能因此而被忽视。

根据法国保险与赔偿公司协会（APSAD）的统计，遭受到较大信息灾难的中小企业（PME）和中小产业（PMI）有 60% 在 5 年之内都会因难以生存而销声匿迹。

所有的企业都承认，如果没有计算机和信息，它们将难以生存：

——如果没有计算机，40% 的企业只能运行不到 4 个小时；

——如果没有计算机，10% 的企业维持不了 1 天；

——如果没有计算机，20% 的企业维持不了 3 天；

——如果没有计算机，30% 的企业维持不了 1 周。

与此相反，我们发现，在 2/3 以上的情形中，人们对信息保护

的知识也仅仅达到了一般的水平。

一旦人们了解到，事故性风险和失误所造成的损失数额，在法国比公布的损失数额的40%还要多，人们就会明白还需要作多大的努力了。

三、人的因素

重罪和轻罪的概念中包含了一个主观方面的要素，也就是说，因为人的行为介入其间而使行为变成故意行为或过失行为。

与自然风险和技术风险一样，例如操作、编程或程序执行过程中的失误等过失行为也会使我们面临重重困难：

——1999年的8月间，在美国马里兰州的苏特兰，一名维修工人用手动方式打开了对该地方的人口调查局计算中心的计算机进行维护的自动洒水系统，结果造成机房进水，好几台主机受损。救援过程中又导致电源短路，造成新的财产损失。

——在工业领域，失误的事例更是屡见不鲜。例如一台安装有惯性导航系统的计算机的程序出错，使得火箭发射出现好几次故障，造成几百万美元的损失。

——银行系统也不能幸免。某银行的自动记录补贴系统的一个识别错误使系统遭受干扰达3个月之久，之后才被人们发现并加以修改。由此造成的无法回收的资金、利息损失和修复的费用十分惊人。财产扣押过程中的失误也可能让银行承担责任。例如，某银行对一笔款项进行了扣押，结果使得一名大客户眼看就要到手的1 200万法郎的贷款化为乌有，交易失败。事后银行向该客户赔偿了120万法郎。

——保险公司也会成为失误的受害人。例如某保险公司启用了一套新的灾害管理系统，运行两个月后才发现程序有错，灾害被重复计算了。此后，保险公司只回收了多赔的部分资金，其经济