网络环境下信息安全若干法律问题研究

——以湖北省信息法规建设为例

黄德林 著

中国地质大学出版社

本书为湖北省社会科学基金资助项目“网络环境下的信息安全与湖北信息法规建设研究”(项目编号:2002067),华中科技大学博士后科研基金资助项目“数字条件下信息公开研究制度”的研究成果。本书出版受到中国地质大学(武汉)政法学院“211”建设项目经费资助。

网络环境下信息安全若干法律问题研究

——以湖北省信息法规建设为例

黄德林 著

中国地质大学出版社

图书在版编目(CIP)数据

网络环境下信息安全若干法律问题研究/黄德林著．—武汉：中国地质大学出版社，2005.9

ISBN 7-5625-2060-7

Ⅰ．网…
Ⅱ．黄…
Ⅲ．网络-信息安全-法律研究
Ⅳ．TP309

网络环境下信息安全若干法律问题研究 **黄德林 著**

责任编辑：王文生 责任校对：胡义珍

出版发行：中国地质大学出版社(武汉市洪山区鲁磨路388号) 邮编：430074
电话：(027)87482760 传真：87481537 E-mail：cbb@cug.edu.cn
经 销：全国新华书店 http://www.cugp.cn

开本：787毫米×960毫米 1/16 字数：258千字 印张：15.625
版次：2005年9月第1版 印次：2005年9月第1次印刷
印刷：武汉首壹印刷厂 印数：1-3 000册

ISBN 7-5625-2060-7/TP·38 定价：18.00元

前　言

当今社会是一个信息时代，计算机和互联网络的应用越来越广泛。计算机和网络的利用与普及一方面大大地促进了各国经济和科技的发展，方便了人们的学习、工作和生活，有着极大的积极作用；但另一方面，网络的存在也给个人、企业和国家带来了很大的负面影响。一些不法分子利用网络进行违法活动，例如，制造和传播计算机病毒、非法侵入他人计算机系统、网上诈骗、网上盗窃、网上侵犯个人隐私权、网上侵犯知识产权、网上非法交易、网上色情及网上窃取和泄露国家机密等。可见网络是一把双刃剑，如何正确处理网络正、负两方面的影响，充分利用好这把双刃剑是一个值得探讨的重要问题，而这个问题可以理解为网络环境下的信息安全问题。这一问题直接关系到网络能否正常运行，关系到个人、企业以及国家的切身利益能否受到有效保护。对网络环境下的信息安全问题的探讨自然涉及到对网络环境下的信息安全立法的研究。

本课题分为四个部分：

第一部分研究网络时代信息安全面临的挑战与对策，该部分首先探讨了网络时代信息安全的概念；其次讨论了网络时代信息安全面临的挑战，有计算机黑客、计算机病毒、网络犯罪和软件运行失败或硬件出现故障；然后对网络时代如何保护信息安全提出了几点对策，为加强技术防范、加快信息安全立法、规范管理体制和加强网络道德建设；最后提出了我国信息安全存在的几个比较严重的问题并对如何解决这些问题提了三点建议。这些问题是：一、基础信息基础设施的主要设备与技术严重依赖国外；二、信息与网络安全的防护能力很弱，许多应用系统处于不设防状态，具有极大的风险性和危险性；三、对引进的信息技术和设备缺乏安全检测和技术改造；四、全社会的信息安全意识淡薄。三点建议分别是：发展我国自主知识产权的信息安全产品和技术；加强信息安全的国际合作，共同维护信息安全；加强信息安全意识教育。

第二部分是对个人信息保护立法、商业秘密保护立法、电子政务信息安全立法问题的研究。第一节是有关个人信息保护立法研究。首先对个人信息和个人隐私的内涵及其法律保护作了研究，认为个人信息和个人隐私是两个内

涵不完全相同的概念。一方面二者有共同的部分，另一方面二者又有不同的部分。然后介绍了我国目前保护个人信息和个人隐私的法律法规及这些法规存在的问题。最后结合国外相关立法，对我国保护个人信息和个人隐私的立法提出了两点建议。第二节是对于商业秘密保护立法问题的研究。第三节是对于电子政务中信息安全立法的研究。

第三部分研究的是国家及湖北省信息安全法规建设的现状和存在的问题。该部分首先分析了我国和美国信息安全法规建设的现状及我国信息安全法规建设存在的问题，然后研究了湖北省和上海市信息安全法规建设的现状及湖北省信息安全法规建设存在的问题。

第四部分是对网络环境下湖北省信息法规的建设提出了建议。该部分共分为五大内容：一、网络环境下加强信息立法工作的意义；二、信息立法的基本思路和基本原则；三、信息立法的内容体系；四、信息立法的几个重点问题；五、对网络环境下湖北省信息立法的其他几点建议。

本课题的研究将有利于推进网络环境下信息安全的研究工作，为企业、政府部门以及公民个人提高网络环境下的信息安全意识以及防范能力提供借鉴，并为湖北信息法规建设提供参考性资料。

作者

2005 年 8 月

目　录

第一章　网络时代信息安全遇到的挑战与对策

20世纪后半期最典型的特征是信息化和网络化，是一个以网络为核心的信息时代。这既是一个催人奋进的时代，又是一个变幻莫测的时代。在这个时代，网络经过30多年的发展，逐渐走进千家万户，人们的学习、工作和生活已经越来越依赖网络。网络同其他事物一样，是一把双刃剑：一方面，网络的发展推动了社会的前进和人类的进步，特别是促进了经济和科技的发展；另一方面，由于网络带来的信息污染、信息侵权、信息渗透、信息破坏、信息攻击等现象比比皆是，信息安全问题日渐突出，已经成为一个亟待解决的社会问题。计算机病毒、黑客、网络犯罪等名词令人闻而生寒，而它们给网络信息带来的潜在威胁、已经造成的破坏和可能造成的毁灭性后果，更加超乎我们的想象。

1979年，一位年仅15岁的美国少年米尼克，运用破译电脑密码的特殊技能，成功地侵入了美国军方的“北美防空指挥中心电脑系统”，并将美国瞄准前苏联的核弹头绝密资料浏览无余。2000年，一位计算机黑客攻入了互联网服务供应商(ISP)英国Redhotant公司的安全系统，窃取了24000多名用户的姓名、地址、密码和信用卡的详细信息，给公司和客户都造成了极大的伤害。

2002年5月4日，一种被称为“爱虫”(I love you)的计算机病毒席卷了全球，约有100多万台计算机遭受侵袭。福特汽车、硅谷图形、忠诚投资、西门子等众多美国著名公司在爱虫的攻势面前也败下阵来，最后连微软也树起了白旗，它设在华盛顿州雷蒙德地区的总部被迫切断了与外界的电子邮件联络。2003年8月12日，“冲击波”(Worm. msBlast)病毒肆虐全球，短短三天就感染了18.8万台主机。受“冲击波”的侵袭，广州东站广九直通车电脑售票系统受到严重影响，电脑出票速度变慢，一度陷入停滞。从2004年5月1日起，很多用户反应遭到“震荡波”的攻击，截至5月5日全球已经有1800多万台电脑成为“震荡波”的俘虏。广州海关计算机网络也遭“震荡波”病毒突袭，造成电子报关频频死机。网络犯罪者不仅对个人资料和企业信息有着浓厚的兴趣，而且还将其邪恶之手伸向国防和军事领域。如果不采取措施解决这一问题，不仅个人隐私和企业的商业机密得不到保护，甚至连国家的政治、经济、军事、

国防安全都得不到保障。

那么，如何理解网络时代的信息安全？网络时代信息安全面临着哪些挑战？我们应该采取哪些措施来解决信息安全问题？我国信息安全存在哪些较为严重的问题呢？这些正是我们所要探讨的主要问题。

第一节　网络时代信息安全的概念

在引言部分中，我们已谈到了网络、计算机和信息这样三个概念。网络是由计算机组成的系统，但网络的本质在于信息。没有计算机，网络将不复存在；没有信息，网络的存在将毫无价值。总之，网络、计算机和信息三者之间有着千丝万缕的联系。信息电子化、计算机网络化、网络 Internet 化的发展趋势使我们更加难以将三者截然区分开来。为了研究信息安全问题，需要首先对网络和信息进行简单的分析和探讨。

一、网　络

一般而言，网络有广义和狭义之分。广义的网络指的是“三网”（如图 1－1），即电信网络（主要业务是电话和传真）、有线电视网络（单向电视节目的传送网络）和计算机网络。狭义的网络专指计算机网络（如图 1－2），即由地理上分散的多台独立自主的计算机遵循约定的协议，通过通信设备和线路联结起来，实现资源共享和信息传递的系统。计算机网络按其覆盖的地理范围大小，又可以分为局域网和广域网。局域网最常见的是校园网和企业内部网。

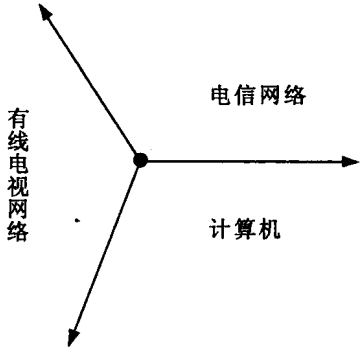

图 1－1　广义的网络

著名的 Internet(互联网或因特网)就是全球最大的广域网。本文所谈的网络指狭义上的网络,即计算机网络。

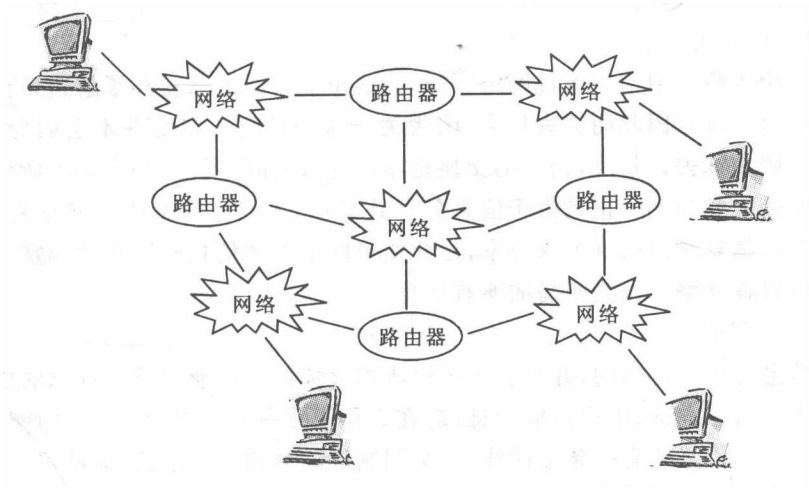

图 1-2 狭义的网络

计算机网络由资源子网、通信子网和协议三个部分组成。通信子网就是计算机网络中负责信息传递的部分;资源子网是计算机网络中负责信息处理的部分;协议是通信双方共同遵守的规则和约定。

计算机网络的功能主要表现在两个方面:一是使分散的计算机能共享网上的所有资源,包括硬件资源、软件资源和信息资源的共享;二是为用户提供强有力的通信手段,方便用户进行信息交换。

二、信 息

在日常生活中,人们常常将数据和信息混为一谈。一般而言,数据和信息是两个不同的概念。信息是经过加工和整理后的有价值的能对接收者的思想和行为产生影响的数据。如果说数据是原材料,那么信息便是成品。信息具有不同于其他事物的一些基本属性,与信息安全问题密切相关的属性是:

1. 事实性

事实性是信息的一个十分重要的属性,不符合事实的信息不仅没有价值,而且可能价值为负。破坏信息事实性的事件在网络环境下时有发生,如黑客

入侵后，有意或无意地改变信息的内容，删除其中的部分内容，用假信息代替原始信息，或者将某些额外的信息插入其中，导致信息的真实性、准确性、精确性和客观性被破坏。

2. 共享性

一个人将一条信息通过网络公开，使成千上万的人获得和了解这条信息，但他本身并没有因此而失去什么，因为关于这条信息的记忆并不会因此而从他的大脑中抹去。相反，物质的交换是零和的，即你的所得，必为我之所失，所得与所失之和为零。正是由于信息具有共享性，人们才有可能慷慨地将各自所拥有的信息拿出来供大家分享，由此使得网络上的信息资源日益丰富，人们几乎可以在网络上找到所需的所有信息。

3. 传输性

信息是可以传输的，并且它的传输成本远远低于传输物质与资源的成本。过去人们利用电话、电报传输信息，现在人们更多的通过快速、经济的网络来传输信息。你只要有一条电话线、一个调制解调器和一台电脑，你就可以将自己的信息传送到世界的每个角落。

4. 价值性

信息可以减少不确定性，可以坚定或校正对未来的估计和预测等。在网络时代，信息的价值与日俱增，关于信息的争夺也愈演愈烈。大多数黑客闯入计算机系统都是有特定的目的的，他们对系统信息进行窃取、篡改，或是获取对自己有价值的信息，或是破坏对自己的对手有价值的信息。

三、信息安全

在网络环境下，信息安全是一个与网络和信息密切相关的话题。以上讨论了网络和信息的概念，那么什么是信息安全呢？关于信息安全的定义，目前尚未形成一致的观点，几种比较典型的观点如下：

网络中的信息安全是指不因偶然或恶意的因素，使网上信息遭受非法篡改、插入、删除或显现，以保证信息的完整性、安全保密性和可用性[①]。

所谓信息安全，是指防止信息财产被故意的或偶然的非授权泄露、更改、破坏或使信息被非法系统辨识、控制[②]。

---

① 肖冬. 浅谈网络的信息安全技术. 网络，企业网络系列文章[4]

② 杨烩荣. 信息安全面临的威胁及其防范对策. 江南社会学院学报，1999(12)

信息安全，即要保障信息的私密性和可靠性[①]。

所谓信息安全是指保护信息财产，以防止偶然的或未授权者对信息的恶意泄露、修改和破坏，从而导致信息的不可靠和无法处理[②]。

我们认为，信息安全是防止信息在存储和传输过程中，不因偶然或故意的因素而被非法访问和非授权更改，以保证信息的真实性、完整性和保密性。

在网络环境下，信息是以电子文件的形式存在的，由计算机进行处理和存储的，通过网络进行传输的，因而信息安全应包括数据安全、计算机安全和通信安全三个方面。

(1)数据安全：防止信息的内容被非法篡改，以保证信息的真实性。

(2)计算机安全：防止计算机软件运行失败和硬件出现故障对数据造成破坏，以保证信息的完整性。

(3)通信安全：防止信息在网络传输的过程中被窃取或由于网络阻碍、瘫痪造成信息无法及时到达目的地。

第二节　网络时代信息安全面临的挑战

计算机网络是在“自由与开放”的思想基础上发展起来的。人们相互联网的初衷并不是为了将众多的用户排斥在网络之外，这就决定了计算机网络从硬件到软件、从协议到结构的设计都是开放式的，在某种程度上可以说是缺乏安全性的，从而导致网络极易受攻击和被破坏。在这样的网络环境下，信息安全就必然面临着诸多的挑战。

以下是网络信息安全面临的主要挑战：

一、计算机黑客

黑客的早期历史至少可以追溯到20世纪50～60年代。当时，麻省理工学院(MIT)率先研制出“分时系统”，学生们第一次拥有了自己的电脑终端。不久，MIT学生中出现了大批狂热的电脑迷，他们称自己为“黑客”(Hacker)，即“肢解者”和“捣毁者”，意味着他们要彻底“肢解”和“捣毁”大型主机的控制。

---

① 姜彦福，雷家骕，曹宁. 关于基于经济安全的信息安全问题. 清华大学学报(社会科学版)2000(1)

② 刘晓敏. 网络环境下信息安全的保护技术. 情报科学，1993(3)

可见，黑客最初指的是一批对计算机有着狂热爱好的人。但随着网络技术的发展，这一名词越来越带上了贬义的色彩，甚至被披上了“数字化时代的恐怖分子”和“最后的剑客”等神秘的外衣。关于黑客的争论现在也越来越激烈，有人说，黑客是网络时代一切罪恶的根源，也有人说这个时代不能没有黑客。争论的焦点是黑客姓什么的问题，一方认为黑客姓“善”，另一方认为黑客姓“恶”。

从攻击手段来看，“善”姓的与“恶”姓的黑客并没有什么不同。他们早期以系统作为攻击的对象，主要手段有：窃取口令、强行闯入、盗取额外特权、植入“特洛伊木马”、植入“蠕虫”病毒。随着网络的发展，黑客们转以网络攻击为主，主要手法有：以监听方式获取用户账号和密码进行攻击；利用文件传送协议(FTP)，采用匿名用户访问进行攻击；利用 UNIX 操作系统提供的缺省账户进行攻击；突破防火墙进行攻击等。

但从出发点看，不同的黑客却有着本质的不同。善意的黑客：在技术上追求精益求精，丝毫未察觉到自己的行为对他人造成的影响，属于无意识攻击行为。他们可以帮助某些内部网发现并及时堵塞漏洞，防止损失扩大，有些人还能够帮助政府部门修正网络错误。这批人是网络时代的英雄，是真正意义上的黑客(Hacker)。恶意的黑客：为了达到自己的私欲——为了成为网络的统治者或为了特定的经济利益，进入别人的计算机系统大肆破坏。我们把这批人称为骇客(Creaker)。

我们认为，不管是 Hacker，还是 Creaker，都是威胁网络信息安全的因素。Hacker 虽然动机不坏，但他们随意进入他人电脑，浏览甚至不经授权就公开个人隐私、商业信息或国家机密，使得信息的保密性得不到保障，虽然是无意识的攻击行为，但也构成事实上的攻击。Creaker 通过攻击网络，窃取、修改、删除和假造信息，破坏了信息的事实性和价值性，是对网络信息安全的严重威胁。尽管二者的轻重程度不一样，但为了表述上的方便，本文将 Hacker 和 Creaker 统称为黑客。

此处要探讨的是信息安全问题，无意给黑客带上什么帽子，划分什么类型，我们所关注的是黑客们“行黑”给信息安全带来的潜在威胁和造成的事实的破坏。1996 年 4 月 16 日，美国《金融时报》报道，全世界平均每 20 秒就发生一起黑客入侵计算机系统的事件，可见黑客的行动十分频繁，而他们的“壮举”给信息安全造成的威胁则更加超乎我们的想象。

1998 年 9 月，海南 Chinanet 系统遭到黑客非法入侵，该黑客擅自将计算

机系统的数据增加、修改和删除，并破译了700多个合法用户密码，盗用他人账号上网，给用户及社会造成重大的经济损失。

2000年2月，全世界黑客们联手发动了一场“黑客战争”，把整个网络搅了个天翻地覆。神通广大的神秘黑客，接连袭击了全世界最热门的八大网站，包括亚马逊、Yahoo和微软，造成这些网站瘫痪长达数小时，估计造成了达17亿美元的损失。

银行、金融等部门的计算机信息系统是黑客攻击的主要目标。据报道，美、英、瑞士、日本等国家的一些金融机构，为免受黑客的攻击，仅1997年一年就向侵入计算机系统的黑客支付了2亿多美元的巨额赎金。由于顾忌自己的商业信誉，许多金融机构对类似案件讳莫如深，所以这些国家的金融机构实际支持的赎金也许还要高好几倍。

综观几十年来的种种黑客事件，我们可以发现，黑客给网络信息安全造成的破坏主要体现在以下几个方面：

(1)干扰网络的正常运行。主要表现在：修改网页的全部或部分内容，使网页发挥不了传播信息的作用；通过发送大量无用的数据包加大数据流量，使网络不堪重负，甚至造成网络通信受阻；修改服务器的系统配置或对服务器发动攻击，使服务器拒绝提供服务；在网络服务软件内布下陷阱、逻辑炸弹或后门，在特定的条件下，引发连锁反应的破坏行动，导致网络完全瘫痪等。

(2)窃取秘密信息。主要表现在：利用软件的某些漏洞入侵计算机系统，获取保存在磁盘中的数据；利用高技术手段窃取在网络上传输的加密信息，使高度敏感信息泄密。更有甚者，黑客用窃取的信息威胁利诱组织的内部人员特别是高级管理人员，以便获得更多、更重要、更秘密的信息。

(3)篡改重要信息。黑客入侵系统后，随意修改和删除信息，或者将一些原本不属于系统的信息插入其中。如果信息使用者将虚假的信息信以为真，并以此信息作为决策的依据，后果将不堪设想。

随着网络的发展，黑客的攻击手段越来越“高明”，入侵的部门越来越多，造成的损失越来越大，已经成为网络信息安全的主要挑战之一。

二、计算机病毒

最初对病毒理论的构思可追溯到科幻小说。在20世纪70年代美国作家雷恩出版的《P1的青春》一书中构思了一种能够自我复制、利用通信进行传播的计算机程序，并称之为计算机病毒。这种构想，没有多久便成了现实。如

今，病毒已经泛滥，充斥着互联网的每个角落。那么究竟什么是计算机病毒呢？《中华人民共和国计算机信息系统安全保护条例》指出：计算机病毒(Computer Virus)是指编制或者在计算机程序中插入的破坏计算机功能或者破坏数据，影响计算机使用并且能够自我复制的一组计算机指令或者程序代码。可见，病毒说到底不过就是一个程序，只不过病毒具有一般程序所不具备的某些特性，这些特性包括：

(1)破坏性

病毒一旦入侵，都会对计算机系统产生程度不同的影响：轻者会降低计算机工作效率，占用系统资源，致使系统性能下降；重者可导致系统崩溃，数据无法恢复。由此特性可将病毒分为良性病毒、恶性病毒和极恶性病毒。良性病毒可能只在系统运行过程中显示一幅图像或播放一段音乐，或者根本没有任何动作，除了减少磁盘的可用空间、干扰计算机用户的正常工作外，对系统没有其他影响。恶性病毒则会锁定系统、破坏数据、删除文件、格式化磁盘，有的对数据造成不可挽回的破坏。极恶性病毒：造成死机、系统崩溃，甚至损坏主板、磁盘或其他硬件，这种破坏是灾难性的。

(2)传染性

病毒的传染性指计算机病毒能从已被感染的计算机扩散到未被感染的计算机。计算机网络的发展，为病毒的传播和扩散提供了“契机”，只要有一台计算机感染病毒，一传十，十传百，短时间内便会有成千上万台计算机被感染。

(3)隐蔽性

病毒由一行行代码组成，如果不经过代码分析，病毒程序与正常程序是不容易区别开来的；病毒通常寄生在正常程序中或隐藏在磁盘不易被人发现的地方，也有些病毒以隐藏属性的文件出现，使得病毒不易被发现；计算机受到传染后，在发作条件不成立的情况下，系统通常仍能正常运行，用户难以察觉它们的存在。这些特点使得病毒的隐蔽性极好，但隐蔽是为了攻击，病毒一旦发作，人们就可以明显地看到病毒的“杰作”了。

(4)潜伏性

大部分的病毒感染系统之后一般不会马上发作，它可长期隐藏在系统中，只有在满足其特定条件时才开始运行。如“PETER－2”病毒在每年2月27日会向用户提出三个问题，用户答错后“PETER－2”病毒就会自动将用户的硬盘加密，使用户无法使用；著名的“黑色星期五”病毒每逢每月13日又是星期五的日子发作；“上海一号”在每年3、6、9月的13日发作。当然，最令人难忘

的便是每月 26 日发作的 CIH 病毒。这些病毒在平时会隐藏得很好，只有在触发条件满足时，才会露出其庐山真面目。

正是由于病毒具有以上几个特征，才使得病毒的预防、检测和清除的难度都极大。病毒一旦发作，从个人到企业，从一个国家到全世界，凡是在使用电脑的人都可能受其困扰。那么，病毒从何而来？为什么会有人不厌其烦地编写病毒呢？病毒的产生不是自然的，也不是偶然的。病毒是人编写的，而且是人为了特定的目的而编写的。一般来说，病毒制作者编写或传播病毒主要有以下几个原因：

(1)恶作剧：某些爱好计算机并对计算机技术精通的人士，在好奇心和表现欲的驱使下，凭借对软硬件的深入了解，编写这些特殊的程序。这类人编写的病毒一般都是良性的，不会有破坏作用。

(2)报复心理：在现实生活中，总有人自认为或事实上受到不公正的待遇，于是产生对社会的不满情绪，严重者会滋生报复心理。如果这种情况发生在一个编程高手身上，那么他有可能会编制一些危险的具有破坏力的程序，借此发泄自己的不满。

(3)保护版权：计算机发展初期，由于在法律上对于软件版权保护还没有像今天这样受到人们的重视，很多商业软件被非法复制。有些软件开发商为了保护自己的利益，制作了一些特殊程序附在商业软件产品中，用以追踪那些非法拷贝他们产品的用户。

另外，因害怕拿不到开发软件的报酬而预留的陷阱，为了祝贺和求爱而制作的别出心裁的小程序也往往成为病毒的一个来源。

虽然病毒制作者编写病毒的目的各异，代码千差万别，但病毒毕竟不是一般意义上的程序。从病毒产生至今，它已经给我们上演了一幕又一幕的好戏，在此我们回忆几个“精彩”的片断。

1988 年 11 月 2 日下午 5 时 1 分 59 秒，美国康奈尔大学的研究生莫里斯(Morris)将其编写的“蠕虫”病毒输入该大学的局域网。在几小时内与该网络相连的大学、研究机关的 155 000 台计算机受到感染，造成网络通信阻塞。这件事就像是计算机界的一次大地震，震惊了全世界，引起了人们对计算机病毒的恐慌。

2003 年 8 月 12 日上午 9:30，一种名为“冲击波”(Worm. Blaster)的新型蠕虫病毒被我国江民、瑞星、趋势科技的反病毒小组分别截获。该病毒运行时会不停地利用 IP 扫描技术寻找网络上系统为 Windows 2000 或 Windows XP

的计算机，找到后就利用 DCOM RPC 缓冲区漏洞攻击该系统，一旦攻击成功，病毒体将会被传送到对方计算机中进行感染，受到感染的计算机中 Word、Excel、Power Point 等应用程序无法正常运行；弹出找不到链接文件的对话框；“粘贴”等一些功能无法正常使用；计算机出现反复重新启动等现象；在网上的其他机器即使还没有被攻击成功也会由于带宽被蠕虫严重阻塞出现网络速度变慢、应用程序异常等现象；而网络本身由于充斥了无数的攻击数据而变得非常拥挤，服务器和网关时有瘫痪。

一场戏演完了，还有下一场。一个病毒倒下了，千千万万个病毒会冒出来。近年来，计算机病毒的种类和数量越来越多，传播途径越来越广，杀伤力越来越大，如果我们不采取有力的措施来控制计算机病毒，信息安全将成为一句空话。

三、网络犯罪

网络犯罪是信息安全面临的又一大挑战。与计算机黑客相比，网络犯罪者更具破坏力，因为计算机黑客尚有 Hacker 和 Creaker 之分，在中国更有“红客”和“蓝客”之别，也就是说黑客在某种程度上存在“善”的一面，而网络犯罪者则彻头彻尾地只有“恶”的一面。

常见的网络犯罪行为有：监听他人网站内的数据流，通过清除部分或全部信息，使得公司无法得知最新资料或订单；非法进入他人网络，修改其电子邮件的内容或厂商签约日期，进而破坏甲乙双方交易，并借此方式了解双方商谈的报价价格，乘机介入其商品竞争。有些犯罪分子还利用政府上网的机会，修改公众信息，挑起社会矛盾。更有甚者，进入军事情报机关的内部网络，干扰军事指挥系统的正常工作，任意修改军方首脑的指示和下级通过网络传递到首脑机关的情报，篡改军事战略部署，达到干扰和摧毁国防军事系统的目的，严重者可以导致局部战争的失败。

与传统犯罪相比，网络犯罪具有如下几个特点：

(1)网络犯罪的工具是计算机硬件和软件。犯罪分子要想进行网络犯罪，必须首先借助计算机、调制解调器等设备建立与网络的连接，然后利用网络的缺陷和系统的漏洞，通过特定的软件侵入特定的信息系统，最后是对信息发动攻击，进行破坏。相对传统犯罪者而言，其凶器要“先进”得多。

(2)网络犯罪的直接侵害对象主要是信息。从上面所列的几种网络犯罪行为可以看出，尽管网络犯罪者的目的各异，或为了报复，或为了发泄，或为了