到法律和隐私问题，论文都有涉及。

Denning, *Information Warfare and Security*

信息已经变成了战争武器，既是军事武器也是军事配合武器。参与者不仅尝试攻击对方的信息系统，而且要防卫好自己的系统。在这本吸引人的书中，作者讨论了所有能想到的关于攻击策略和防卫策略的话题，从数据欺骗到包窝探器。该书对于计算机安全有极大兴趣的读者来说是必读的。

Ford and Allen, "How Not to Be Seen"

病毒，间谍软件，rootkits和数字版权管理系统都对隐藏数据情有独钟。这篇文章对各种隐身的方法进行了简要的介绍。

Hafner and Markoff, *Cyberpunk*

书中介绍了由《纽约时报》曾经写过网络蠕虫故事（马尔可夫链）的计算机记者讲述的世界上关于年轻黑客破坏计算机的三种流传最广的故事。

Johnson and Jajodia, "Exploring Steganography: Seeing the Unseen"

隐身术具有悠久的历史，可以回到将信使的头发剃光，然后在剃光的头上纹上信息，然后在信使的头发长出来之后再将他送走的年代。尽管当前的技术很多，但是它们也是数字化的。本书对于想在这一主题彻底入门的读者来说是一个开端。

Ludwig, *The Litte Black Book of Email Viruses*

如果想编写反病毒软件并且想了解在位级别（bit level）上这些病毒是怎么工作的，那么这本书很适合。每种病毒都有详细的讨论并且也提供了绝大多数的实际代码。但是，要求读者透彻掌握 Pentium 汇编语言编程知识。

Mead, "Who is Liable for Insecure Systems?"

很多有关计算机安全的措施都是从技术角度出发的，但是这不是惟一的角度。也许软件经销商应该对由于他们的问题软件而带来的损失负起责任。如果比现在更多地关注于安全，这会是经销商的机会吗？对这个提法感兴趣吗？可以读一下这篇文章。

Milojicic, "Security and Privacy"

安全性涉及很多方面，包括操作系统、网络、私密性表示等。在这篇文章中，6位安全方面的专家给出了他们各自关于这个主题的想法和见解。

Nachenberg, "Computer Virus-Antivirus Coevolution"

当反病毒的开发人员找到一种方法能够探测某种电脑病毒并且使其失效时，病毒的编写者已经在改进和开发更强的病毒。本书探讨了这种制造病毒和反病毒之间的"猫和老鼠"游戏。作者对于反病毒编写者能否取胜这场游戏并不持乐观态度，这对电脑用户来说也许不是一个好消息。

Pfleeger, *Security in Computing, 4th ed.*

尽管已经出版了很多关于计算机安全的书籍，但大多数却只关注网络安全性。本书不仅关注网络安全性，还包含了讨论操作系统安全性、数据库安全性和分布式系统安全性的章节。

Sasse, "Red-Eye Blink, Bendy Shuffle, and the Yuck Factor: A User Experience of Biometric Airport Systems"

作者讲述了他在许多大机场所经历的瞳孔识别系统的体验。不是所有的体验都是正面的。

Thibadeau, "Trusted Computing for Disk Drives and Other Peripherals"

如果读者认为磁盘驱动器只是一个储存比特的地方，那么最好再考虑一下。现代的磁盘驱动器有非常强大的CPU，兆级的RAM，多个通信通道甚至有自己的启动ROM。简而言之，它就是一个完整的计算机系统，很容易被攻击，因此它也需要有自己的保护机制。这篇文章讨论的就是磁盘驱动器的安全问题。

14.1.10 Linux

Bovet and Cesati, *Understanding the Linux Kernel*

该书也许是对Linux内核整体知识讨论最好的一本书。它涵盖了进程、存储管理、文件系统和信号等内容。

IEEE, *Information Technology——Portable Operating System Interface (POSIX), Part 1: System*