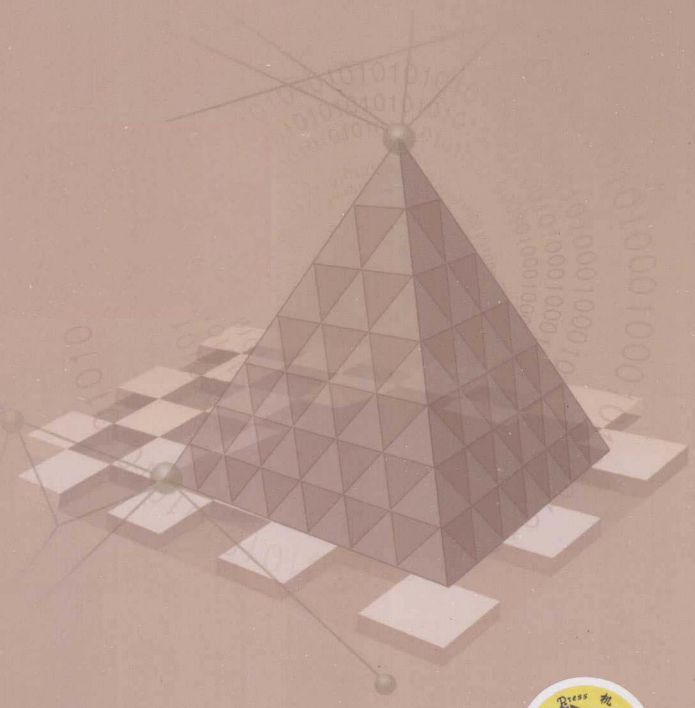
高等院校信息安全专业规划教材

信息安全案例教程：技术与应用

- 围绕构建信息安全体系结构的三个关键要素展开内容
- 以具有经典性和代表性的案例为基本教学素材
- 每章配有思考与实践题，包括材料分析、方案设计等七大类题型
- 为每章提供免费的案例分析视频，包括案例介绍和简要分析

免费提供电子教案、教学视频

陈 波 于 泠 编著



机械工业出版社
CHINA MACHINE PRESS

高等院校信息安全专业规划教材

信息安全案例教程：技术与应用

陈 波 于 泠 编著

机 械 工 业 出 版 社

本书围绕构建信息安全体系结构的人、技术和管理三个关键要素展开。其中，信息安全技术介绍7个方面：设备与环境安全、数据安全、身份与访问安全、系统软件安全、网络系统安全、应用软件安全、信息内容安全，涵盖了从硬件到软件、从主机到网络、从数据到信息内容等不同层次的安全问题及解决手段。信息安全管理介绍信息安全管理体系，涵盖法律法规和标准等管理制度、等级保护、风险评估等重要环节。对人的安全意识教育、知识介绍、技能培养贯穿全书。

本书可作为信息安全专业、计算机专业、信息工程专业或相关专业的教材，也可供科技人员、管理人员、计算机及信息技术爱好者参考和使用。本书为每一章提供案例分析视频，读者可用移动设备的相关软件扫描书中的二维码在线观看。

本书配套授课电子课件，需要的教师可登录 www. cmpedu. com 网站免费注册，审核通过后下载，或联系编辑索取（QQ：2966938356，电话：010－88379739）。

图书在版编目(CIP)数据

信息安全案例教程：技术与应用/陈波，于泠编著．—北京：机械工业出版社，2015.3
高等院校信息安全专业规划教材
ISBN 978-7-111-49615-1

Ⅰ．①信… Ⅱ．①陈… ②于… Ⅲ．①信息安全－安全技术－高等学校－教材 Ⅳ．①TP309

中国版本图书馆 CIP 数据核字(2015)第 048466 号

机械工业出版社(北京市百万庄大街 22 号 邮政编码 100037)
责任编辑：郝建伟 叶蔷薇
责任校对：张艳霞
责任印制：李 洋
北京宝昌彩色印刷有限公司印刷

2015 年 4 月第 1 版·第 1 次印刷
184mm×260mm·20 印张·495 千字
0001－3000 册
标准书号：ISBN 978-7-111-49615-1
定价：45.00 元

凡购本书，如有缺页、倒页、脱页，由本社发行部调换

电话服务
服务咨询热线：(010)88379833
读者购书热线：(010)88379649

网络服务
机 工 官 网：www. cmpbook. com
机 工 官 博：weibo. com/cmp1952
教育服务网：www. cmpedu. com
金 书 网：www. golden－book. com

封面无防伪标均为盗版

前　言

近些年来，高级持续性威胁（Advanced Persistent Threat，APT）攻击的频发、社交网络带来的中东北非社会动荡、携带自己的设备办公（Bring Your Own Device，BYOD）等问题，使得各国政府、企业和组织在关注信息化发展的同时，高度关注包括网络安全、数据安全、信息内容安全、信息基础设施安全及国家与公共信息安全在内的网络空间（Cyber Space）信息安全问题。

信息安全也关乎个人安全。美国棱镜计划（PRISM）的曝光、手机恶意软件、人肉搜索等问题，使得个人用户也必须高度关注包括网络交易安全、网络交友安全、网络隐私安全在内的信息安全问题。

当前，我国在高等教育领域大力推进信息安全的专业化教育，这是国家重视信息安全人才培养、在信息安全领域掌握自主权、占领先机的重要举措。办好信息安全本科专业的第一要素是拥有高质量的教材，为此，从国家到各个院校都大力支持开设信息安全专业，鼓励出版配套教材。为了适应信息安全教学和应用的需求，本书以信息安全案例为主线，介绍相关内容，帮助读者构建系统化的知识体系和应用体系。同时也帮助读者解决身边的安全问题，如交易安全、社交安全、隐私安全等。

本书在编写过程中力求体现如下特点。

知识体系结构完整。本书围绕构建信息安全体系结构的人、技术和管理三个关键要素展开。其中，信息安全技术介绍 7 个方面：设备与环境安全、数据安全、身份与访问安全、系统软件安全、网络系统安全、应用软件安全、信息内容安全，涵盖了从硬件到软件、从主机到网络、从数据到内容等不同层次的安全问题及解决手段。此外，信息安全管理介绍信息安全管理体系，涵盖法律法规和标准等管理制度、等级保护、风险评估等重要环节。对人的安全意识教育、知识介绍、技能培养贯穿全书。

围绕案例组织内容。本书以具有经典性和代表性的案例为基本教学素材，将学习者引入安全实践的情景中分析问题和解决问题，培养学习者的反思能力、分析及应用能力、案例教学法具有鲜明的实践性，是教育、教学中对学生能力培养的一种不可替代的重要方法，因而非常适用于信息安全这门实践性很强的课程。本书中精选了棱镜门事件、震网病毒与伊朗核设施的瘫痪等 15 个案例。在选材上，既注重经典理论素材，也追踪最新技术成果；既注重基础理论的阐述，也追求应用技能的培养。本书可帮助读者充分了解信息安全面临的问题，建立系统化的分析问题的思路，提供了实用性强的解决问题的手段。

教学设计细致独特。本书内容循序渐进，深入浅出，条理清晰，图文并茂，便于自学。每章配有思考与实践，题型包括简答、知识拓展、读书报告、操作实验、编程实验、材料分析以及方案设计七大类，内容覆盖了每章的重要知识点，对读者掌握这些知识点和使用技巧都有很大的帮助。为了便于教师教学，我们给出了本书每章中的“案例”“知识点”“技能”（即“知”“会”“行”）这 3 个能力培养层次的具体内容，并给出了教学建议。

教学资源立体丰富。本书作为江苏省教育科学十二五规划重点资助项目（泛在知识环境下的大学生信息安全素养教育：培养体系及课程化实践）、江苏省精品教材建设项目、南

京师范大学研究生课程案例库建设项目，以及南京师范大学精品资源共享课建设项目、南京师范大学精品视频公开课建设项目的建设成果，包含教学录像、教学课件、实验指导、参考资料等内容的视频、文本、图片等资源。读者可以访问南京师范大学信息化教学网主页（http://jxw.njnu.edu.cn）下载本书的配套资源。本书为每一章提供案例分析教学视频，读者可用移动设备的相关软件扫描书中的二维码在线观看。

本书可作为信息安全专业、计算机专业、信息工程专业或相关专业的教材，也可供科技人员、管理人员、计算机及信息技术爱好者参考。

本书由陈波和于泠执笔完成。另外，陈国凯、强小辉、朱汉、刘亚尚也参与了本书初稿的整理工作。

本书在编写过程中，查阅和参考了大量的文献和资料，限于篇幅，未能在书后的参考文献中一一列出，在此一并致谢。

由于编者水平有限，书中难免有疏漏之处，恳请广大读者批评指正。读者在阅读本书的过程中若有疑问，也欢迎与作者联系，电子邮箱是 SecLab@163.com。

编　者

试读结束：需要全本请在线购买：　www.ertongbook.com

本书案例分析视频二维码扫描观看方法

本书为每一章提供一个案例分析视频，每个视频包括案例介绍和案例简要分析，供读者学习参考。读者可以使用移动设备的相关软件扫描书中提供的二维码，在线观看案例分析视频。强烈建议在 WiFi 环境下观看，以避免在 3G 或 4G 通信环境下产生较大通信费用。移动设备的相关软件，请从 Android 市场或苹果 App Store 等下载安装。下面以使用“微信”软件为例，介绍扫描观看方法。

使用“微信”软件扫描二维码观看视频的方法步骤如下。

1）启动“微信”软件，如图 1 所示，单击“微信”右上角“+”按钮，再单击“扫一扫”按钮，启动二维码扫描功能，如图 2 所示。

图 1　单击“+”按钮找到“扫一扫”按钮

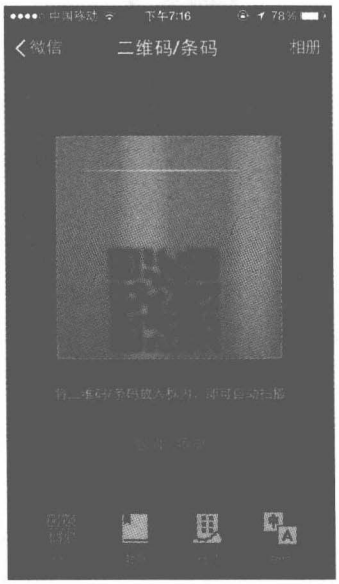


图 2　开启二维码扫描

2）扫描书中提供的二维码，如图 3 所示，即可进入视频所在页面，如图 4 所示，在“输入密码观看视频”栏中输入密码“infosec”，即可在线观看案例分析视频，如图 5 所示。

图 3　案例分析视频二维码

图 4　输入视频密码

图 5　在线观看案例分析视频

教 学 建 议

章	案例（知）	知识点（会）	技能（行）	教学建议
1	1-1：美国棱镜计划被曝光 1-2：震网病毒与伊朗核设施的瘫痪	● 信息、信息系统、网络空间的概念 ● 网络空间面临的安全威胁 ● 根据信息流动过程划分的安全威胁 ● 信息安全的需求 ● 信息安全防护的 3 个发展阶段 ● 网络空间的信息安全防护	● 躲避棱镜的方法 ● 网络空间面临的安全威胁 ● 虚拟实验环境的搭建 ● 工业控制系统信息安全防护体系设计	1. 围绕案例 1-1 介绍网络空间面临的安全威胁 2. 信息安全的概念 3. 围绕案例 1-2 介绍网络空间信息安全防护体系
2	2：电影《碟中谍 4》中迪拜哈利法塔的机房	● 计算机设备和环境安全的重要性 ● 计算机设备和运行环境面临的安全问题 ● 环境安全技术 ● 电磁安全防护技术 ● PC 物理防护 ● 网络空间的信息安全防护	● PC 物理防护 ● 移动存储设备安全防护	1. 围绕案例 2 介绍设备与环境安全的重要性、面临安全威胁及主要安全技术 2. 移动存储设备安全性分析与对策
3	3-1：第二次世界大战中的“风语者” 3-2：美国签证全球数据库崩溃事件	● 密码学术语和基本概念 ● 对称密码体制与公钥密码体制的概念及算法 ● 散列函数的概念及算法 ● 数字签名的概念及算法 ● 消息认证的概念 ● 信息隐藏的概念与方法 ● 容灾备份的概念与关键技术	● Windows 系统常用的文档安全保护 ● 密码算法的编程实现与应用 ● 信息隐藏的编程实现与应用	1. 密码基本概念 2. 围绕案例 3-1 介绍数据的保密性、完整性、不可否认性、可认证性、存在性防护 3. 围绕案例 3-2 介绍数据可用性防护
4	4：国内著名网站用户密码泄露事件	● 身份认证的概念 ● 3 种身份认证技术 ● OTP、Kerberos 及 PKI 身份认证机制 ● 访问控制的概念 ● 访问控制模型	● 基于口令的身份认证安全分析及防护 ● TNC、NAP 及 NAC 网络接入控制方案	1. 身份认证技术原理及应用 2. 访问控制技术原理及应用 3. 围绕案例 4 介绍用户口令防护
5	5：后 Windows XP 时代的系统安全	● 操作系统面临的安全问题 ● 操作系统安全机制 ● 安全操作系统的概念 ● Windows 系统安全机制 ● Linux 系统安全机制 ● 数据库系统面临的安全问题 ● 数据库系统安全需求 ● 数据库系统安全机制	● Windows XP 系统安全加固 ● Windows 系统用户账户设置、共享设置、系统修复等	1. 操作系统安全机制的分析与设置 2. 数据库系统安全机制 3. 围绕案例 5 介绍 Windows XP 系统加固

章	案例（知）	知识点（会）	技能（行）	教学建议
6	6：新型网络攻击——APT	● 认识黑客 ● APT 攻击分析 ● 防火墙、入侵检测系统等网络安全设备 ● 网络安全架构 ● 网络安全协议	● 防火墙配置与应用 ● 入侵检测系统配置与应用 ● SSL、VPN 等应用设置	1. 黑客与网络攻击剖析 2. 网络安全设备技术原理与应用 3. 网络安全架构的概念及设计 4. 网络安全协议原理与应用
7	7-1：央视 3·15 晚曝光手机吸费软件 7-2：Web 站点被攻击 7-3：苹果公司 iOS 系统越狱的安全性	● 恶意代码的概念 ● 代码安全漏洞问题 ● 软件侵权问题 ● 软件可信验证关键技术 ● 漏洞消减技术 ● 安全软件工程 ● 软件版权的技术保护与法律保护	● 反恶意代码工具的应用与分析 ● Web 漏洞分析与攻击模拟 ● 常用软件版权保护技术应用与实现	1. 围绕案例 7-1 介绍恶意代码的分类与可信验证技术 2. 围绕案例 7-2 介绍代码安全漏洞与面向漏洞消减的安全软件工程 3. 围绕案例 7-3 讨论软件侵权问题与技术和法律保护
8	8-1：脸谱和推特与伦敦骚乱 8-2：电影《搜索》中的人肉搜索与网络暴力	● 信息内容安全的重要性 ● 信息内容安全的威胁 ● 信息内容安全的概念 ● 信息内容安全保护技术 ● 信息内容安全保护设备	● 浏览器隐私保护设置 ● 社交网站隐私保护设置	1. 围绕案例 8-1 和 8-2 介绍信息内容安全问题及保护对象 2. 信息内容安全保护技术及设备
9	9-1：动画片《三只小猪》与信息安全管理 9-2：BYOD 与信息安全管理	● 信息安全管理的概念 ● 信息安全管理的制度：法律与标准 ● 信息安全等级保护的要求与实施 ● 信息安全风险评估的概念与实施 ● 信息安全意识教育的概念与方法	● 信息系统安全性测试 ● 风险评估工具应用	1. 信息安全管理的概念、制度及意识教育 2. 信息安全等级保护及风险评估的概念与实施

目　录

试读结束：需要全本请在线购买： www.ertongbook.com

第1章　信息安全概述

案例1-1：美国棱镜计划被曝光

【案例】

棱镜计划（PRISM）是一项由美国国家安全局（National Security Agency，NSA）自2007年起开始实施的绝密电子监听计划。该计划的正式名号为“US-984XN”。2013年6月，该计划因美国防务承包商博思艾伦咨询公司的雇员爱德华·斯诺登（Edward Snowden）向英国《卫报》提供绝密文件而曝光。图1-1为棱镜计划的标志。棱镜在光学中是一种透明的光学元件，抛光与平坦的表面能折射光线，一束普通白光射过棱镜，能够析出其七彩本真，这对于专门窃取信息的监视项目来说，“棱镜”是一个再合适不过的代号。

图1-1　PRISM计划的标志

斯诺登曝光棱镜项目的文件，是一份长达41页的秘密PPT文件，这是专门为国家安全局内部演示而编写的，展示了棱镜项目运作的全过程。

美国国家安全局和联邦调查局凭借棱镜项目，直接进入互联网服务商的服务器，大规模收集分析实时通信和服务器端信息，肆无忌惮地收集并监视个人智能手机使用和互联网活动信息，包括电子邮件、聊天记录、电话记录、视频、照片、存储数据、文件传输、搜索记录、视频会议、登录时间和网络社交等个人信息。可以说，棱镜项目以近乎实时备份的方式，备份了整个全球互联网的全部数据。

被曝光参与棱镜项目的互联网服务商有9个，它们为用户提供日常网络服务。

- 终端操作系统服务商有微软、谷歌和苹果。
- 电子邮件服务商有微软、雅虎、谷歌。
- 社交网站服务商有脸谱、谷歌、You Tube。
- 即时通信服务商有微软、雅虎、谷歌、脸谱、美国在线AOL、PalTalk、Skype。
- 网络接入服务提供商有美国在线AOL。

棱镜计划能够对被监控对象展开全方位、多角度的情报搜集和跟踪。在曝光的一页秘密文件中（见图1-2），显示了两种监控数据来源：Upstream（另一个监听项目的代号）和PRISM。Upstream项目在承载互联网骨干通信内容的光缆上安装分光镜，复制其通信内容；PRISM则是从上述美国服务提供商的服务器直接进行收集。“我们（斯诺登受雇公司以及美国国家安全局）主要攻击网络中枢，像大型互联网路由器，”斯诺登说，“这样我们可以接触数以十万计计算机的通信数据，而不用入侵每一台计算机。”

斯诺登在一处秘密地点接受中国香港《南华早报》记者的独家专访，2013年6月13日通过这家报纸英文版披露了美国政府更多监视细节。大约1小时的专访中，斯诺登披露，根据他向美国《华盛顿邮报》提供的机密文件，自2009年以来，美国国家安全局还一直从事

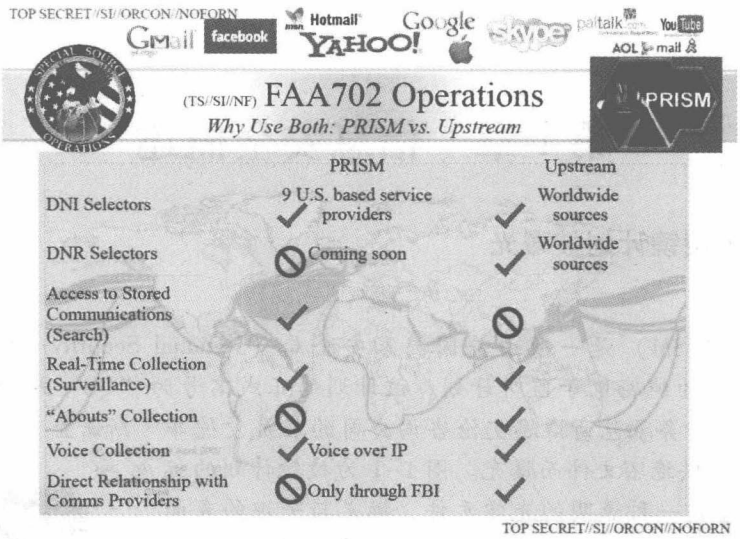


图 1-2　介绍美国国家安全局监控数据来源的一页 PPT

侵入中国内地和香港计算机系统的活动。

【案例思考】

- 如何看待棱镜计划被曝光事件对信息安全问题的影响？
- 信息为什么会有安全问题？
- 信息面临哪些安全问题？尤其是在网络空间的环境下。
- 如何定义信息安全的概念？
- 信息安全研究的内容是什么？

案例 1-2：震网病毒与伊朗核设施的瘫痪

【案例】

曝光美国棱镜计划的斯诺登证实，为了破坏伊朗的核项目，美国国家安全局和以色列合作研制了震网（Stuxnet）蠕虫病毒，以入侵伊朗核设施网络，改变其数千台离心机的运行速度。斯诺登的爆料，让世界的目光聚焦在了震网病毒这个“精确制导的网络导弹”上。

震网病毒让世人惊讶的是攻击目标精准或者说明确，即针对德国西门子公司的 SIMATIC WinCC 系统。这是一款数据采集与监视控制（Supervisory Control And Data Acquisition，SCADA）系统，被伊朗广泛使用于国防基础工业设施中。病毒并不以刺探情报为目的，而是按照设计者的设想，定向破坏离心机等要害目标。目前，这种病毒已经感染了超过 10 万台个人计算机，并且光顾了全球数万个工业控制系统，但除了伊朗设施的离心机外却没有对其他计算机和工业设备造成任何物理损害。对于那些不属于破坏目标的计算机和工业控制系统，震网病毒会在留下其“电子指纹”后离开，继续寻找其目标。病毒到达装有 WinCC 系统用于控制离心机的主机后，首先记录离心机正常运转时的数据，如某个阀门的状态或操作温度，然后将这个数据不断地发送到监控设备上，以使工作人员认为离心机工作正常。与此同时，病毒控制 WinCC 系统向合法的控制代码提供预先准备好的虚假输入信号，以控制原有程序。这时，离心

机就会得到错误的控制信息，使其运转速度失控，最后达到令离心机瘫痪乃至报废的目的。而核设施工作人员在一定时间内会被监控设备上显示的虚假数据所蒙骗，误认为离心机仍在正常工作，等到他们察觉到异常时为时已晚，很多离心机已经遭到不可挽回的损坏。

震网病毒另一个让世人惊讶的是，它的传播和渗透非常的精巧，它能够攻击我们平时认为非常安全的，在物理上与互联网隔离的内部局域网。一般来说，保密的内部网络通常都是局域网，其与互联网一般都是没有物理连接的。要想进入这样的局域网，要么想办法进行物理连接，要么通过移动存储设备，要么采用无线注入的方式。据分析，震网病毒采取的是通过移动存储设备进行传播的方式。如图 1-3 所示，该病毒首先在互联网上进行传播，大量感染的主机也就成为潜在的向内部局域网传播的“桥梁”；病毒利用被感染的主机传染给在其上面使用过的 U 盘，如果这个 U 盘在内部局域网上使用，病毒就会利用漏洞传播到内部网络；到达内部局域网后，病毒通过利用一系列的系统漏洞，实现联网主机之间的传播；最后，病毒抵达装有目标软件的主机后展开攻击。这意味着，将带有震网的 U 盘插入主机的 USB 接口后，不需要任何操作，病毒就会感染目标主机。

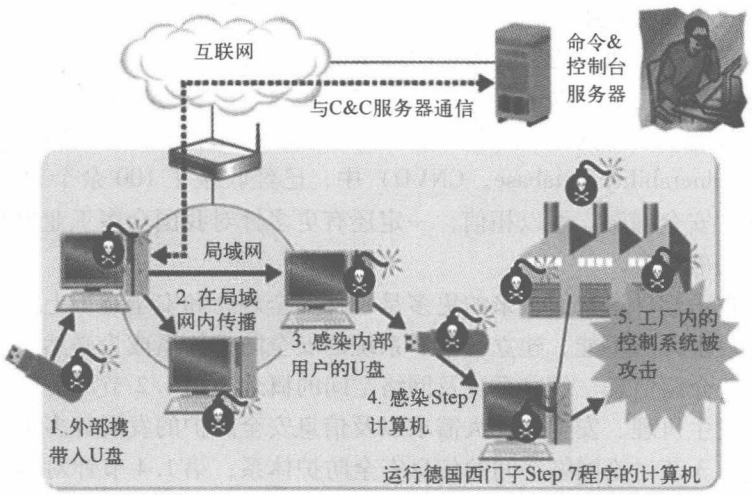


图 1-3 “震网”病毒攻击工业控制系统流程

【案例思考】

- 震网病毒这类“精确制导的网络导弹”，与传统的网络攻击相比较，有哪些新的特点？
- 面对网络空间不断出现的安全问题，我们应当建立怎样的安全防护体系？
- 建立网络空间信息安全防护体系应当确立哪些原则？

【案例分析视频】

请用移动设备扫描二维码观看案例分析视频。

案例 1 分析视频二维码

【案例分析】

案例 1-1 中的棱镜门事件，堪称是一场震惊全球的网络空间安全的核冲击波，该事件对全球各国网络空间安全与发展的影响异常深远。斯诺登所揭露的棱镜门事件使网络空间这一全新领域的发展与安全问题成为世界性的焦点论题。棱镜门事件也要求我们重新思考中国未来的网络空间安全和发展的问题。

为此，我们需要从棱镜门事件的本质——大规模网络监控入手，进一步分析目前的网络空间中存在的安全威胁，在不断发展的网络空间的全新范式下思考我国信息安全对策。

案例 1-2 中，在传统工业与信息技术融合不断加深、传统工业体系的安全核心从物理安全向信息安全转移的趋势和背景下，此次伊朗核设施遭受震网病毒攻击事件，尤其值得我们思考。这是一次极不寻常的攻击，其具体体现在以下几点。

- 传统的网络攻击追求影响范围的广泛性，而这次攻击具有极其明确的目的，是为了攻击特定工业控制系统及特定的设备。
- 传统的攻击大多利用通用软件的漏洞，而这次攻击则完全针对行业专用软件，使用了多个全新的 0 day 漏洞（新发现的漏洞，尚无补丁和防范对策）进行全方位攻击。
- 这次攻击能够精巧地渗透到内部专用网络中，从时间、技术、手段、目的、攻击行为等多方面来看，完全可以认为发起此次攻击的不是一般的攻击者或组织。

这一攻击事件绝不是偶然发生的，也不是个案。在中国国家信息安全漏洞共享平台（China National Vulnerability Database，CNVD）中，已经收录了 100 余个对我国影响广泛的工业控制系统软件安全漏洞。可以相信，一定还有更多针对我国众多工业控制系统且未被发现的漏洞和潜在的破坏者。

因此，这次攻击事件给我们带来的更多是一种安全观念和安全意识上的冲击。安全威胁无处不在，网络攻击无所不能，建立科学、系统的安全防护体系成为必然。

本章第 1.1 节介绍信息、信息系统及网络空间的概念；第 1.2 节从对信息安全的感性认识、安全事件的发生机理、安全的几大需求以及信息安全防护的发展等多个角度带领读者认识信息安全；第 1.3 节讨论网络空间的信息安全防护体系；第 1.4 节针对本章案例 1-1，介绍“粉碎棱镜”网站提供的躲避监控、保护隐私的软件及服务。

1.1 信息、信息系统与网络空间

本节首先从“信息是什么”的角度探讨信息的本质，接着讨论信息与消息、信号、数据、媒体、资料、情报、知识、智能的联系与区别，从“信息不是什么”这个角度澄清信息的面貌，进而为理解网络空间环境下的信息安全问题打下基础。

1.1.1 信息的概念

1. 信息的定义

信息依据载体的不同，通常可分为文字、图形（图像）、声音、动画、视频，其表现形式有声音、图片、温度、体积、颜色等。信息的分类方法很多，包括电子信息、财经信息、天气信息、生物信息等。在棱镜计划中，我们的通话时间、通话时长、通话内容等都是受到监控的信息。

我国国家标准 GB/T 4894—2009《信息与文献 术语》中，关于“信息”的解释是“Information 是物质存在的一种方式、形态或运动状态，也是事物的一种普遍属性，一般指数据、消息中所包含的意义，可以使消息中所描述事件的不定性减少”。

本书认同我国钟义信教授在《信息科学原理》一书中对信息的释义，书中认为，信息是事物运动的状态及其状态变化的方式。从认识论的角度来说，信息是主体所感知的事物运动的状态和状态改变的方式，包括主体所关心的这些运动状态及其变化方式的形式（语法信息）、含义（语义信息）和价值（语用信息）。这里所说的“事物”，可以是外部世界的物质客体，也可以是主观世界的精神现象；“运动”可以是物体在空间上的位移，也可以是一切意义上的变化；“运动的状态”是指事物在特定时空中的性状和态势；“状态改变的方式”是指事物运动状态随时空的变化而改变的样式。

2. 信息与消息、数据等概念的区别与联系

读者通常对于消息、数据、资料这些和信息的概念十分接近的名词感到疑惑，什么是“消息”“数据”“资料”？它们和“信息”的概念有什么区别呢？钟义信教授在其《信息科学原理》一书中对此进行了阐述。

（1）消息（Message）和信息

可以说消息是信息的俗称，信息是消息的学名。我们可以说这是一个关于什么问题的消息，也可以说这是一个长消息还是短消息，是一个重要的消息还是一个一般的消息。但是，信息就不仅有长短的区别，重要与否的区别以及价值大小的区别，信息还有信息量大小的区别。例如，同样是 140 字左右的微博，有的所包含的信息量很大，有的则很小。

（2）数据（Data）与信息

在计算机应用领域，数据的原意是指以数字形式表达的信息。人们通常把文本信息、语音信息、图形信息、图像信息等也分别叫做文本数据、语音数据、图形数据、图像数据等，实际上这是更加注重这些信息在计算机中的数字表达。例如，我们收到的一个数据文件，在计算机中的表达只是一段 0 或 1 的组合，我们可以以此作为特征码来鉴别文件是否含有恶意代码，但是作为信息，我们还需要甄别其语义（含义）和语用（价值），因为其表达的信息内容可能是有害的或违法的。本书第 3 章将讨论数据形式层面的安全，第 8 章主要讨论语义和语用层面的安全。

（3）媒体（Media）和信息

媒体的字面意义是“媒介体”或“中介物”。它的表征性作用是在不同的对象之间实现某种意义上的互相沟通。信息作为事物运动的状态和状态变化的方式，总是依附于一定的事物。如果要使这些状态和方式脱离开原来的事物，提供给相关的人们使用，就必须设法把这些状态和方式寄附在那些被称为“媒体”的事物上，这样才便于表现，便于传送，便于被人们利用。了解了这一点，我们就能够区分表示信息的“媒体”和被媒体表示的“信息”。例如，在考虑病毒等恶意代码的传播过程中，我们不能忽视对移动存储设备这种存储媒介（Storage Media）的安全控制；在研究信息内容安全的过程中，也不能忽视对传播媒体的安全管理和控制。

（4）情报（Intelligence）与信息

情报是对某人（或某集团）具有特殊意义的情况报导。最早的情报概念出现在军事斗争领域。后来，情报的概念拓展到了其他许多领域，如外交领域、技术领域、科学研究领

试读结束：需要全本请在线购买： www.ertongbook.com