国　　际　　电　　信　　联　　盟

发展中国家网络安全指南

2007 年版

国际电信联盟

国　　际　　电　　信　　联　　盟

发展中国家
网络安全指南

2007 年版

序 言

出席信息社会世界高峰会议（WSIS）日内瓦和突尼斯阶段会议的各国际组织、政府、公司和民间团体，一致通过了对信息社会的共同展望。

然而，只有在线交易具有安全保障、重要信息基础设施受到防护以及公司、公民和政府所依赖的信息系统和数据得到保护的情况下，我们才能将这一共同展望化为现实，奉献于各国人民。

网络安全解决方案的不完善、以及未就全面解决这一问题所涉及的诸多方面及其必要性达成共识，只是我们必须共同面对的挑战之中的一部分。

肩负WSIS C.5行动方面（树立使用ICT的信心并提高安全性）协调方/推进方责任的国际电信联盟（ITU），致力于与所有利益攸关方开展合作，就上述挑战达成共识，汇集我们的共同资源，构建一个全球性的安全与信任框架。

我请诸位与我们同心协力，为实现建立全球性安全信息社会的理想而奋斗。

国际电信联盟
秘书长

哈玛德·图尔

前 言

随着技术在社会经济发展中的作用与日俱增逐渐形成的全球性跨国界的信息社会，为全球所有国家带来了新的机遇。卫生、教育、商业、金融和公共行政部门均能利用信息通信技术（ICT）应用提供服务。

然而ICT也带来了新的挑战。要想安全地开展电子卫生工作、让国民享受电子政务服务、使人们对网上商务以及公司对网上交易树立必要信心并使我们的信息技术系统和资源保持完好无损，我们就必须应对这些挑战。

因此，实施适当的安全和信任解决方案，是致力于帮助各国推广电信和ICT使用的国际电联电信发展局必须解决的重大挑战之一。

信息社会的无国界性还意味着，解决方案的制定必须以各国间达成共识为基础，即认识到安全的 ICT 应用所具有的潜力以及在树立安全信心过程中面临的挑战。因此，除了致力于缩小数字鸿沟外，我们还必须通过提高人们的基本认识并加强人员和机构的能力建设，弥合知识鸿沟。

这份指南旨在向发展中国家提供一种工具，使他们能够更好了解与信息技术安全相关的问题，并向他们介绍其它国家针对这一问题采用的解决方案的实例。本指南还参考引用了其它已发行刊物中有关网络安全问题的更多信息。它的目的不是提供一份有关这一议题的包罗万象的文件或报告，而是作为一份总结，说明希望享受信息社会实惠的国家目前面临的主要问题。

本指南选取的内容旨在满足发展中国家，尤其是最不发达国家利用信息通信技术在不同部门提供基本服务的需要，同时亦继续致力于发掘当地潜力并提高所有利益攸关方的认识。

为彻底避免对这些议题的重复论述，我们在这份出版物的内容编制过程中，考虑到了在国际电联电信标准化部门（ITU-T）第 17 研究组框架内完成的工作以及这一领域现有的其它研究成果和出版物。

电信发展局
主任

萨米·阿勒巴舍里·阿勒穆什德

内容提要

是社会、经济和公共政策问题还是人的问题？无论从哪个角度去观察它，也无论冠以它什么名称（信息技术安全、电信安全），网络安全都事关民众、机构和国家的数字和文化财富的安全，牵涉诸多复杂的棘手问题，而应对这些挑战需要靠政治意志制定和实施一项发展数字基础设施和服务的战略，其中包括一项协调有效并方便验证和管理的网络安全战略。

达到足以应对技术和信息风险的信息安全水准，与政府和机构的正常运行息息相关。随着数字技术广泛应用而来的，是对这些技术越来越大的依赖性，以及关键基础设施之间日益增长的相互依赖性。这会给机构的运行造成薄弱环节，给机构带来潜在威胁，甚至侵害到国家主权。

网络安全工作的目的在于帮助机构保护其组织、人力、财务、技术和信息资源，使机构能够履行其使命。其最终目标是确保机构不会受到持久的伤害，其中包括降低形成威胁的可能性，限制威胁导致的破坏或故障的范围，并确保在发生安全事故后，能够在可接受的时间和成本范围内恢复正常运行。

网络安全工作涉及整个社会，它的实施关系到社会的每一分子。为正确使用 ICT 制定网络行为准则，并颁布一项名副其实的安全策略，规定网络安全用户（实体、合作伙伴和提供商）应当遵守的标准，将会提高网络安全工作的效率。

确定网络安全工作流程，必须准确地确定需要保护的资产和资源，以便精确地划定需要有效安全保护的范围。这需要采取综合的安全措施，即一种涉及多个学科的全面措施。网络安全难以容忍那种崇尚宽容放纵、为所欲为的世界。它所需要的是适用的法律框架和实用的规则与规定体现出的一套有关道德行为、责任和透明度的核心原则。这些原则无疑必须在当地得到实施，但它们也必须得到整个国际社会的采用，并符合现行的国际规则。

为避免给犯罪以滋生的机会，在用的电信基础设施必须具备技术和法律性的适用安全措施。通过网络发起的攻击可表现为多种形式：秘密劫持系统、拒绝服务、破坏和盗窃敏感数据、黑客入侵网络、破解软件保护和飞客（phreaking）（包括蓄意破坏和劫持电话交换机等），而作为这些攻击受害者的机构和个人，无一例外地要承担因此而增加的成本。

作为一种系统，电信（包括基础设施和服务）面临的安全挑战与信息技术资源面临的挑战大致相同。要应对这一挑战，也必须在技术、机构和人员方面施加同样限制。对传送中的信息提供保护是必要的，但这本身还远远不够，因为一旦进入处理和存储阶段，信息反而更加不堪一击。因此必须全面地看待网络安全问题。缺少对安全需求、措施、程序和工具的统一和严格的管理，不是纯粹的技术安全解决方案所能补救的。无序地哄抢安全工具不仅会妨碍使用，

使运行不堪重负，还会降低信息技术系统的性能。严格意义上的信息技术安全是一个管理问题，有关工具和业务是与运行系统管理相联系的。例如，如果后来的数据存储方式不安全，那么为保护传输中的数据而进行数据加密就是徒劳的。同样，如果允许连接绕过系统，在该系统中安装的防火墙便起不到作用。

要想扩展基于信息处理的活动并缩小数字鸿沟，就需要：

- 可靠和安全的信息基础设施（提供有保障的可接入性、可用性、可靠性和业务连续性）
- 建立信任的政策
- 适用的法律框架
- 精通新技术并能够同其它国家同行开展合作的司法和警察机构
- 信息风险和安全管理工具
- 安全实施工具，并利用这些工具培养对提供的应用和服务（商业和金融交易、电子卫生、电子政务、电子选举等）和重点在个人数据隐私的人权保护程序的信任。

数字信息资产的良好管理、无形商品的分配、内容的使用以及弥合数字鸿沟，都说明这些是仅靠信息技术安全手段无法解决的经济和社会问题。参考数字基础设施和用户在人员、法律、经济和技术方面的安全需求而提出的对策，有助于建立信心，并实现造福于全社会的经济增长。

对阅读本指南的几点说明

网络安全指南介绍网络安全这一重要议题，重点说明数字数据的出现带来的变化，信息的虚拟化和电信网络的普遍使用，还提出了社会发展中的要点问题，以便在信息技术和电信领域推出安全要素的概念。

第一部分以网络安全的需求为重点，简要介绍解决方案的某些内容，并根据观察到的信息通信技术安全方面的弱点和整体性的缺失，对通信基础设施安全的概念进行分析。参照研究最佳做法得出的经验教训、日常的互联网安全现状以及国际社会获得的经验，指南随即提出了发展中国家的具体网络安全需求。

指南对网络安全的管理、政策、经济、社会、法律和技术内容做出分析，就电信基础设施的接入提出了具有普遍性的建议，旨在控制风险（无论是否源于犯罪）并培养人们对于电子服务这一经济发展重要推动因素的信心。

第二部分关注控制网络犯罪的问题，研究那些为说明现有的安全措施和反网络犯罪的斗争能力有限而不惜鼓励犯罪的人物，还研究了我们面临的问题的复杂性和广泛性。

指南重点从经济犯罪角度介绍网上从事的各种违法和犯罪活动，对发现的犯罪行为以及犯罪黑客的特征进行了分析，并对网络攻击和恶意软件做出总体描述，还为准备应对网络犯罪的威胁提出了一些指导原则。

第三部分阐述电信的一些基本要素，提出了一种可行的解决方式，并对各种基础设施安全工具予以概要介绍。

第四部分介绍现代技术各个法律方面的网络安全综合手段，并为实施电信基础设施安全解决方案勾画出可行的目标。

在本指南的最后，附有一份安全术语表以及一系列相关的索引和文件。

致 谢

国际电联电信发展局感谢 Solange Ghernaouti-Hélie 及其同事的支持，特别是 Mohamed Ali Sfaxi、Igli Tashi、Sarra Ben Lagha、Hend Madhour 和 Arnaud Dufour（互联网战略顾问）。

本指南是根据不同机构提供的信息和研究成果编写而成的，我们尤其要对“Clusif”（法国信息技术安全俱乐部）和“Cert”（计算机网络安全应急小组）这两家计算机安全机构表示衷心感谢。

本指南的编写离不开国际电联信息通信战略处成员，特别是 Alexander Ntoko 的出色合作。我们还要对 Renée Zbinden Mocellin（国际电联出版物排版室）和她的团队制作网络安全指南的工作致以谢意。

目 录

页码

序 言 ..... **iii**

前 言 ..... **iv**

内容提要 ..... **v**

对阅读本指南的几点说明 ..... **vii**

致 谢 ..... **viii**

第一部分 – 网络安全 – 背景，挑战，解决方案 **1**

第 I.1 节 – 网络世界与信息社会 **3**

I.1.1 数字化 3

I.1.1.1 数字信息 3

I.1.1.2 数字技术 3

I.1.1.3 基础设施和内容 4

I.1.2 信息革命 4

I.1.2.1 创新与发展 4

I.1.2.2 支持信息革命 5

第 I.2 节 – 网络安全 **6**

I.2.1 通信基础设施的安全环境 6

I.2.2 网络安全的要害何在 7

I.2.3 安全赤字 9

I.2.4 应汲取的经验教训 10

I.2.4.1 承担起安全的责任 10

I.2.4.2 确定和管理风险 10

I.2.4.3 确定安全策略 11

I.2.4.4 部署解决方案 13

I.2.5 从管理角度看问题 13

I.2.5.1 动态管理 13

I.2.5.2 外包与依赖性 14

I.2.5.3 防范和补救行动 14

页码

I.2.6 政治层面 15
I.2.6.1 国家的责任 15
I.2.6.2 国家主权 15
I.2.7 经济层面 16
I.2.8 社会层面 16
I.2.9 法律层面 17
I.2.9.1 关键的制胜因素 17
I.2.9.2 加强立法和执法 17
I.2.9.3 在尊重数字隐私的同时打击网络犯罪：微妙的折中 18
I.2.9.4 国际网络犯罪立法 19
I.2.10 网络安全的基本要素 21
I.2.10.1 可用性 21
I.2.10.2 完整性 21
I.2.10.3 机密性 22
I.2.10.4 身份确定与认证 22
I.2.10.5 不可否认性 23
I.2.10.6 物理安全 23
I.2.10.7 安全解决方案 23
第二部分 – 控制网络犯罪 25
第 II.1 节 – 网络犯罪 27
II.1.1 计算机关联犯罪和网络犯罪 27
II.1.2 互联网吸引犯罪的因素 28
II.1.2.1 虚拟化和虚拟世界 28
II.1.2.2 资源联网 28
II.1.2.3 非法闯入和薄弱环节的激增 29
II.1.2.4 过失与薄弱环节 29
II.1.2.5 掀开网络犯罪分子的面纱 30
II.1.2.6 无疆界，数字安全港 31
II.1.3 传统犯罪和网络犯罪 32
II.1.4 网络犯罪、经济犯罪和洗钱 32
II.1.5 网络犯罪 – 普通犯罪的延伸 33
II.1.6 网络犯罪和恐怖主义 33
II.1.7 黑客 34

页码

II.1.8 烦扰和恶意软件 36
II.1.8.1 垃圾邮件（Spam） 36
II.1.8.2 恶意软件 36
II.1.8.3 趋势 39
II.1.9 互联网犯罪的主要形式 39
II.1.9.1 诈骗、间谍和情报活动、敲诈和讹诈 39
II.1.9.2 危害人类罪 40
II.1.9.3 盗版 40
II.1.9.4 信息操控 40
II.1.9.5 公众机构的作用 41
II.1.10 安全事件和未报告的网络犯罪 41
II.1.11 为应对网络犯罪威胁做好准备：保护的责任 43
第 II.2 节 – 网络攻击 44
II.2.1 网络攻击类型 44
II.2.2 为进入系统盗窃用户密码 44
II.2.3 拒绝服务攻击 44
II.2.4 刷新攻击 45
II.2.5 欺骗攻击 45
II.2.6 针对关键基础设施的攻击 46
II.2.7 网络攻击的不同阶段 46
第三部分 – 技术途径 49
第 III.1 节 – 电信基础设施 51
III.1.1 特点 51
III.1.2 基本原则 51
III.1.3 网络成份 52
III.1.3.1 互连媒介 52
III.1.3.2 连接成份 53
III.1.3.3 专业设备和数据服务器 53
III.1.4 电信基础设施和信息高速公路 54
III.1.5 互联网 54
III.1.5.1 总体特点 54
III.1.5.2 IP 地址和域名 56
III.1.5.3 IPv4 协议 59

页码

第 III.2 节 – 安全工具 60
III.2.1 数据加密 60
III.2.1.1 对称加密 60
III.2.1.2 非对称或公钥加密 61
III.2.1.3 加密密钥 61
III.2.1.4 密钥管理系统 62
III.2.1.5 数字证书 62
III.2.1.6 值得信赖的第三方 63
III.2.1.7 公钥基础设施的缺点和局限性 64
III.2.1.8 签名与认证 64
III.2.1.9 数据完整性 65
III.2.1.10 不可否认性 65
III.2.1.11 以加密为基础的安全性解决方案的局限性 65
III.2.2 安全的 IP 协议 66
III.2.2.1 IPv6 协议 66
III.2.2.2 IPSec 协议 67
III.2.2.3 虚拟专用网 67
III.2.3 应用安全性 67
III.2.4 安全套接层（SSL）和安全 HTTP（S-HTTP）协议 68
III.2.5 电子邮件和域名服务器安全性 68
III.2.6 发现入侵者 70
III.2.7 环境隔离 70
III.2.8 访问控制 72
III.2.8.1 总体原则 72
III.2.8.2 生物特征的贡献和局限性 73
III.2.9 通信基础设施的保护和管理 74
III.2.9.1 保护 74
III.2.9.2 管理 75
第四部分 – 综合方式 77
第 IV.1 节 – 新技术监管法的相关内容 79
IV.1.1 个人数据保护和电子商务 79
IV.1.1.1 电子商务：“网下”的违法行为，在“网上”同样违法 79
IV.1.1.2 保护义务 79
IV.1.1.3 尊重基本权利 80
IV.1.1.4 立法的经济价值 81

页码

IV.1.2 电子商务与网络世界的契约 81
IV.1.2.1 法律选择问题 81
IV.1.2.2 以电子方式签订的合同 82
IV.1.2.3 电子签名 83
IV.1.2.4 撤消权 85
IV.1.2.5 争议的管理 85
IV.1.3 网络世界与知识产权 86
IV.1.3.1 有关保护知识产权的法律 86
IV.1.3.2 版权和邻接权 86
IV.1.3.3 商标法 87
IV.1.3.4 专利法 87
IV.1.3.5 网站的知识产权保护 88
IV.1.3.6 技术和法律保护的补充性质 88
IV.1.4 垃圾邮件（Spam）：一系列法律方面的考虑 88
IV.1.4.1 背景及烦扰行为 88
IV.1.4.2 垃圾邮件的法律补救方法 89
IV.1.4.3 垃圾邮件的规管 92
IV.1.4.4 处理垃圾邮件的技术手段 92
IV.1.4.5 技术与法律手段间的互补 93
IV.1.5 与网络世界相关的主要法律问题摘要 93
IV.1.5.1 商用互联网的法律地位 93
IV.1.5.2 网络合同 93
IV.1.5.3 电子文件和签名 94
IV.1.5.4 电子支付 94
IV.1.5.5 域名保护 94
IV.1.5.6 知识产权 94
IV.1.5.7 保护数字隐私 94
IV.1.5.8 其它法律问题 95
第 IV.2 节 – 前景 95
IV.2.1 教育 – 培训 – 提高网络安全所有利益攸关方的安全意识 95
IV.2.2 解决安全问题的新途径 95
IV.2.3 安全策略的特点 96
IV.2.4 识别敏感资源，保护敏感资源 96
IV.2.5 网络安全的目标、使命和基本原则 96
IV.2.6 成功因素 97
IV.2.6.1 战略指导原则 97
IV.2.6.2 针对互联网用户的指导原则 98

页码

IV.2.6.3 保证电子邮件系统安全的指导原则 98

IV.2.6.4 保护互联网-内联网环境的指导原则 99

第五部分 – 附件 101

附件 A – 主要安全术语词汇表 103

附件 B – 可作为安全管理参考的 ISO/IEC 17799:2005 标准目录 117

附件 C – ITU-D 在网络安全和打击垃圾邮件方面的职责 123

附件 D – 国际电联电信标准化部门 2005-2008 年研究期内正在研究的与安全有关的主要课题 139

附件 E – 参考资料 143

附件 F – 经济合作与发展组织（OECD）信息系统与网络安全指导原则：逐步培育安全文化 145

序言 145

F.1 逐步培育安全文化 145

F.2 目标 146

F.3 原则 146

第一部分

网络安全－背景，
挑战，解决方案

第 I.1 节 – 网络世界与信息社会

I.1.1 数字化

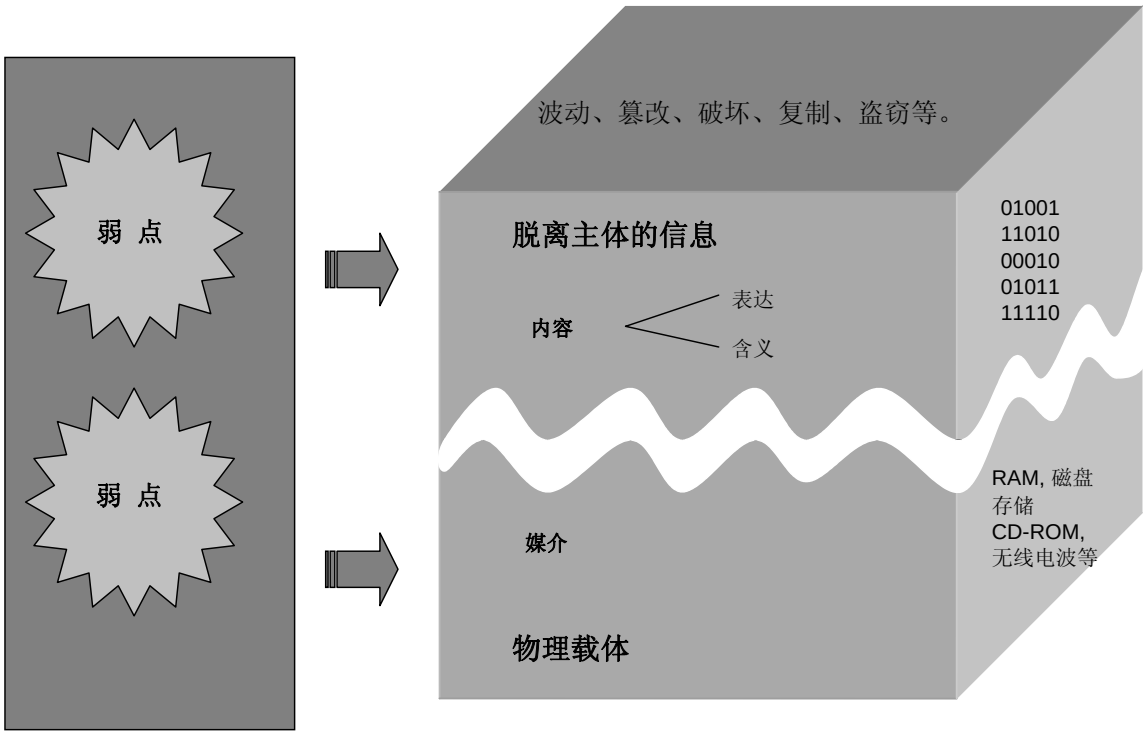
信息技术正在改变着我们生活中的几乎一切思维和行为方式。它使我们能够将形形色色的对象转化为信息形式，以便以电子方式进行操作，从而实现着重大的结构性变革。

I.1.1.1 数字信息

数字化能够生成某个实际物体的数字图像（即虚拟版的该物体）。所有信息，无论是语音、数据还是图像性质的，都可以数字化，并以某种标准化的方式得到再现。

数字化信息逐渐脱离了母体，也就是说，它不再与再现和存储它的媒介捆绑在一起。信息本身（内容）可以增值，因为与信息生成（图 I.1）相比，它的共享和存储成本要低得多。此外，数据可以局部化，同时在多个地点进行处理。无限完美复制的可能性，既掏空了“原始”数据概念的内涵，也给版权保护概念埋下了令人不安的影响。

图 I.1 – 虚拟化和数字信息



I.1.1.2 数字技术

数字技术可以通过标准化的数据制作、处理和传送，创建连续的数字信息链。如互联网现象所示，数字融合与数据压缩技术相结合，为信息技术、电信和音像媒介的结合创造了机会。信息数字化因此带来了真正的技术革命，其影响远远超出了电信的范围。

这一新层面的信息处理影响到人类活动和工作的各个方面。近年来，对于从产品设计到分销的生产价值和模式的确定方式发生了变化，导致了不同经济参与方之间的价值链重组。

I.1.1.3 基础设施和内容

对基础设施和内容等数字信息链的掌控，已成为 21 世纪的重大挑战。全面开放的新市场的特色是，在前所未有的程度上调动了全球经济中的所有参与者，即电信运营商、有线电视运营商、软硬件制造商、电视广播商等。

无节制的竞争和作用与活动的重组，是新经济给当今体制带来的挑战。

古登堡（Gutenberg）在印刷其首本书时，无从想象他的创造会在产业界造成何种反响；当时，这些反响代表着迈向产业自动化的第一步。同样的情况在上世纪 60 年代末再次发生，当时的大学和军方用户，出于各自显然相互对立的目的，着手建立尔后成为互联网的通信网络。正如其十五世纪的先辈那样，他们是在并不充分了解他们的这一创举产生的结果的情况下开展工作的。如今的网络世界预示着社会向信息时代过渡的开始。

I.1.2 信息革命

信息革命深刻地改变了信息的处理和存储方式，也改变了机构乃至整个社会的运作方式。它不仅仅是近年来出现的技术创新，其独到之处在于它对信息以至对于知识处理产生的影响。由于信息革命影响到知识的创建和共享机制，它可以被视为未来创新的源泉，而且发展中国家不应被拒之门外。

信息和电信技术的发展，彻底改变了我们对经济、社会和文化交流的看法，同时还使我们获得了一种新型的基于网络的信息技术。如要开发可进一步提高机构效率的新型应用，就必须实现信息的安全流动。没有参与者之间的交流和互动，就不可能有任何形式的经济活动；没有某种基本的安全保障，就不可能开展信息交流；不考虑服务质量，也就无法进行业务规划。然而我们还必须牢记，成功的通信取决于参与各方进行技术攻关并驾驭所有信息交流习惯势力的能力。

I.1.2.1 创新与发展

若想作为长期参与者在新的竞争环境中得以生存并有所作为，机构和国家就必须以强大和安全的信息系统为后盾，重点培养创新能力和快速适应能力。

电信多样化正在开启新的活动领域，信息技术的推广开创了多种机遇，发展中国家也应从中受益。

通过部署可靠的信息技术基础设施实现的技术和经济发展，向普通百姓展示了美好前景。然而，与之伴生的是前所未有的技术和管理上的复杂性。这种随之而来的巨大风险必须得到控制，以免使进步的概念本身受到削弱。伴随意外或恶意事故造成的信息处理和通信系统故障等技术风险而来的，是必然削弱机构信息应用能力的信息风险。

必须牢记的要点是，虽然信息技术已在广泛应用和日益发展，但仍有不容忽视的一部分人依然与这场信息革命无缘。个中原因颇为复杂，既有文化和经济因素，也在某些情况下涉及文盲等基本难点问题。为使信息技术民主化并反对信息垄断，这一领域的培训和教育较任何其它领域都更为至关重要。还必须对通信接口进行重新思考，以便更好地服务于大众，并尊重文化背景的多样化。计算机必须适应人文环境，它们必须在这种环境中得到整合，而不是强加一种新的通信秩序。

I.1.2.2 支持信息革命

信息通信技术与所有技术一样，是在具体的历史和地理环境中产生和运行的，通常反映出社会内部的平衡。相关人员的责任是利用必要的工具、程序、法律和道德准则支持信息革命，以解决安全问题并满足社会的期望和需求。

目前，国际电联、联合国教科文组织、联合国、经济合作与发展组织、欧洲理事会等机构制定了一系列局部规定，负责管理通信媒介的使用和信息的自由交流。但对它们实施管理的规定，已跟不上信息通信技术和人们使用这些技术方式的发展，因而有必要制定一个适用的法律框架，以解决诸如互联网这类跨地域性网络、责任问题以及隐私和产权保护等问题。经过这一大致盘点便可看出，随信息时代而来的挑战所具有的意义、电信在应对这些挑战时的关键作用，以及在发展受阻前解决安全问题的重要性。

向信息时代的过渡揭示了信息技术的重要性，并明确提出必须掌握信息技术。鉴于信息技术开创了技术和经济社会的新局面，显然信息技术和电信系统以及基础设施的安全已成为最基本的需求，突显出规划和实施网络安全对于国家、机构和个人都具有战略意义，利害攸关。

鉴于各国投入财力、物力和人力资源建设其信息和电信基础设施，它们必须确保这些基础设施得到安全和良好的管理与控制。

第 I.2 节 – 网络安全

I.2.1 通信基础设施的安全环境

随着新技术的日益普及、全球信息技术基础设施的建成以及新的风险的出现，人们越来越认识到控制信息技术运行风险的重要性。

新技术在每一个活动领域和每一种基础设施中的整合，使各国社会出现了向信息社会的转变，因而增加了个人、机构和国家对信息系统和网络的依赖。这是一个巨大的风险来源，必须视为一种安全风险。

发展中国家面临的问题是，在必须参与信息社会的同时，不能忽视逐渐陷入对技术和技术提供商依赖的风险，还要避免使数字鸿沟演变为安全鸿沟，或更加依赖可左右其需求和信息技术安全手段的实体的危险[1]。

电信基础设施以及通过它们开展的服务和活动，必须在其酝酿、设计、制定和管理过程中考虑到安全问题。安全是一切活动之本；应将它视为一种能够创造其它服务并生成价值（如电子政务、电子卫生和电子教学）的服务。它不仅仅是一个技术问题[2]。然而，迄今提供的基本通信工具并不具备提供或保证最低限度安全所需的足够资源。

网络化的信息技术系统是可以远程接入的资源；因此，它们也是网络攻击的潜在目标。系统面临着更多受到入侵的风险，对它们发动攻击并实施犯罪的机会也在成倍增长。虽然攻击的对象是系统，攻击者追求的目标却是处理中的信息（图 I.2）。攻击会影响到信息资本的处理、存储和共享能力，破坏无形和象征性商品、制作流程以及机构的决策过程。网络系统给拥有网络的机构的运作带来了运行风险。

因此，解决电信网络和开放系统引起的复杂和多方面的网络安全问题，具有相当的难度，而它可能造成的影响和打击会使机构和国家的运转陷入灭顶之灾。经济成功的要素可能取决于为信息、流程、系统和基础设施提供安全保障的能力。

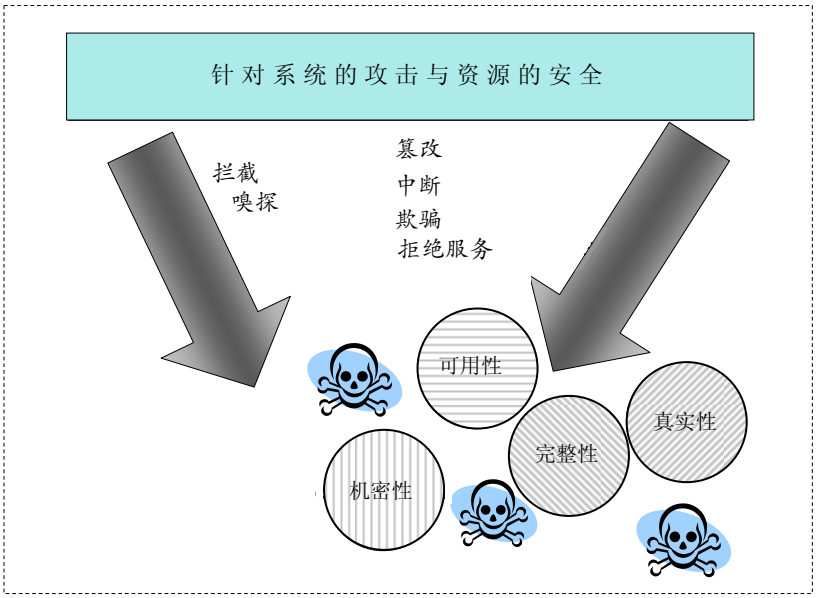
面对广泛的系统互连、基础设施之间连接的愈发紧密、对数字技术依赖的日益增长以及威胁和风险的不断增加，个人、机构和国家必须采取措施，利用程序并掌握工具，以改进技术和网络风险的管理方式。努力控制技术风险正是 21 世纪本身面临的挑战。这些挑战要求在全球范围内对安全问题采取全面措施，并需要发展中国家的参与。

---

1 S. Gheraouti-Helie：“从数字鸿沟到数字的不安全性：在多维度环境中建设和部署统一的电子安全框架的挑战”。2003年11月日内瓦发行的IUED出版物《国际合作和信息社会》有关瑞士发展政策指令部分。

2 A. Ntoko：“网络安全的职责与活动 – ITU-D”。国际电联于2005年6月28日-7月1日在日内瓦举行的WSIS网络安全专题会议。

图 I.2 – 针对系统的攻击与资源的安全



只建立电信网络接入点还不够，还需要部署可靠、便于维护、强健和安全的信息技术基础设施和网络服务，同时尊重基本的人权和国家的权利。对系统和宝贵信息必须像保护个人权利和隐私一样予以保护。

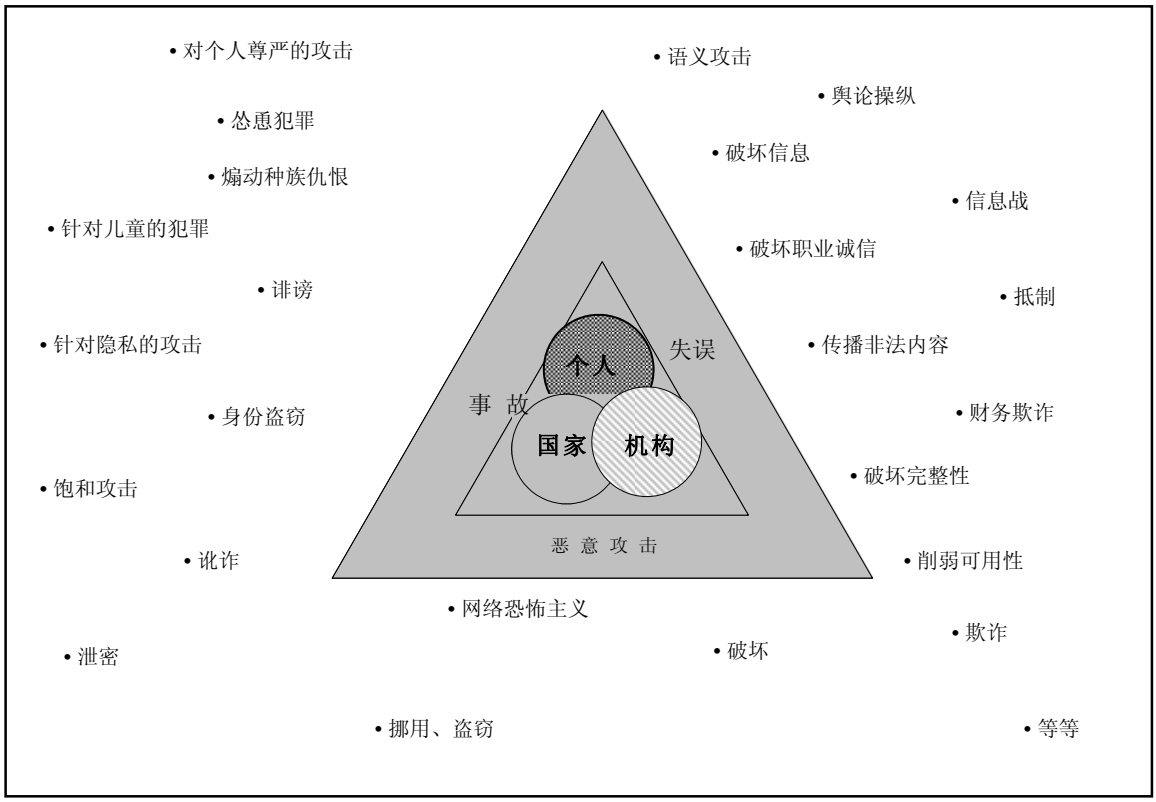
发展中国家必须在不冒过多风险的情况下进入信息社会，汲取发达国家已有的经验，并避免以网络安全形式将它们拒之门外的新生危险因素的影响。

I.2.2 网络安全的要害何在

是社会、经济和公共政策问题还是人的问题，无论人们从哪个角度去观察它，也无论人们冠以它什么名称（信息技术安全、电信安全），网络安全关系到个人、机构和国家的数字和文化财富的安全（图 I.3）。其中涉及的挑战是复杂的，应对这些挑战需要靠政治意志制定和实施一项综合战略，以发展数字基础设施和服务，其中包括一项协调有效、方便验证和管理的网络安全战略。网络安全战略必须是多学科举措的组成部分，提供教育、法律、管理和技术方面的解决方案。以有力措施在人员、法律、经济和技术方面满足数字基础设施的安全需求，既可以增强人们的信心，也可以形成为人们所期待的惠及全社会的经济增长。

掌握数字信息财富、分配无形商品、增加内容价值并弥合数字鸿沟，都是经济和社会性问题，因此对网络安全不能仅采用片面和纯技术的解决方法。

图 I.3 – 网络安全的不同层次：个人、机构和国家



要想推广基于信息处理的活动并以此推动缩小数字鸿沟的工作，就需要：

- 可靠和安全的信息基础设施（其服务具备有保障的可接入性、可用性、可靠性和连续性）；
- 促使人与人之间建立起信任的政策；
- 适用的法律框架；
- 精通新技术并能与其它国家伙伴合作的司法和公安机构；
- 信息风险和安全管理工具；
- 安全实施工具，并利用这些工具培养对提供的应用和服务（商业和金融交易、电子卫生、电子政务、电子选举等）和重点在个人数据隐私的人权保护程序的信任。

网络安全目标是帮助保护机构的组织、人员、财务、技术和信息形式的资产和资源，使机构能够履行其使命。

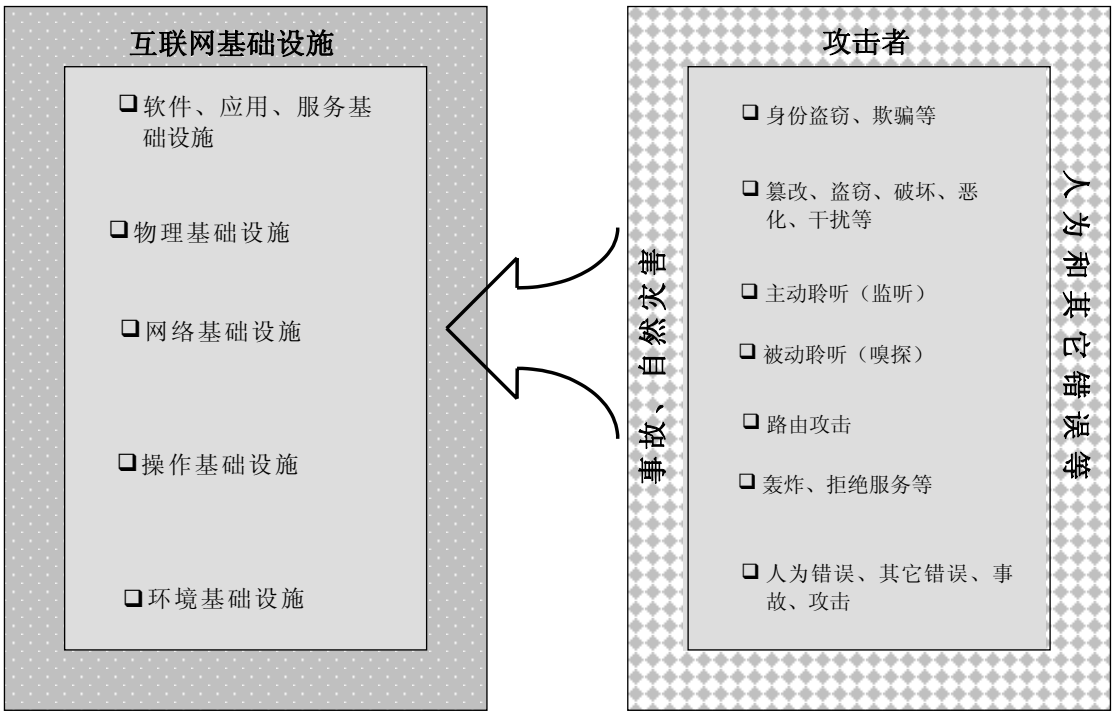
其最终目标是保证机构免受长期的损害，其中包括减少威胁降临的可能性；控制造成的破坏或故障的范围；并确保在出现安全事故后，有能力在可接受的时间和成本范围内恢复正常运行。

网络安全工作是全社会的事情，它的实施牵涉到社会中的每一个人。提高这项工作重要性的方法是，制定网络行为准则并颁布切实可行的安全策略，规定网络安全用户、实体、合作伙伴和提供商需要达到的标准。

I.2.3 安全赤字

信息通信技术的安全赤字反映出了信息技术和网络世界的性质。用户活动在虚拟空间，进行远程操作并处于相对互不了解的状态，更增加了设计、部署、管理和控制这项技术的难度。一旦在这一平衡关系中加入了停机、故障、失误、错误、不协调甚至自然灾害，其结果是信息技术基础设施因不安全的阴霾而失色也就不足为奇了（见图 I.4）。

图 I.4 – 互联网基础设施和众多问题的根源



在这种情况下，恶意攻击者可以采用多种方式利用互联网基础设施的薄弱环节[3]。

诸如身份盗窃、系统欺骗、入侵、资源劫持、病毒传播、劣化、破坏、篡改、泄密、拒绝服务、盗窃、敲诈等各种攻击的泛滥，说明了现有安全战略的局限性，而且从另一个侧面说明了基础设施具有一定的强健性。

无论个体计算机罪犯出于什么动机，他们总会造成绝对不容忽视的经济影响。网络犯罪正迅速演变为一只世界范围的多头怪兽。

安全解决方案确实存在，但是它们从来不是绝对的，而且通常只是为了应对具体条件下的具体问题。其结果是安全问题脱离了原有定位，且安全责任也出现了转移；因此更有必要在有保护的条件下获得和管理解决方案。

3 第二部分深入探讨网络犯罪、网络攻击和网络破坏问题。

安全解决方案至多只是一种初步尝试，用以应对它们面临的不断变化的现实，即变换不止的技术、游移不定的目标、日益发展的黑客技能和突变频仍的威胁和风险，因而既无法保证某一具体安全手段能够提供长久保护，而且作为必然结果，也无法确保兑现这一手段宣称的投资回报。

安全战略往往仅限于建立机制，通常以纯技术方式减少机构信息资产面临的风险。而更有效的战略要全面地考虑问题，满足个人的安全需求，尤其是对其隐私和基本权利提供保护。网络安全应该包括每一个人，将保护扩展到个人数据。

安全解决方案目前已有提供。在很多情况下，它们是纯技术性的，解决具体情况下的具体问题。但同所有技术一样，它们也会出错或掉入陷阱。在多数情况下，它们仅仅取代了安全问题的位置，并将责任转移到需要它们予以保护的系统的另一个部分。此外，它们自身也需要保护和稳妥的管理。动态环境（不断变化的需求、风险、技术、黑客技能等）使它们永远也不可能提供绝对或最终的保护，而这种环境本身又是安全环境的持续变化性造成的。存在这一问题的原因是现有的解决方案最多只是昙花一现。另一问题是异构解决方案的泛滥，可能危及整体安全战略的统一性。显然，仅有技术是不够的；必须通过管理手段对技术加以整合。

大量不同实体和个人（工程师、开发商、审计员、系统工程师、法律专家、调查人员、客户、提供商、用户等）的参与以及利益、观点、环境和语言的纷繁不一，更使安全战略的整体统一复杂化。必须对安全风险和措施有一个统一和系统的把握，并认识到所有参与方各自的责任，才有望达到利用信息通信技术放心开展活动所需的安全水平，并帮助人们增强对信息经济的信心。

I.2.4 应汲取的经验教训

I.2.4.1 承担起安全的责任

在 21 世纪之初，多数大型机构 – 以及众多小型机构 – 已普遍认识到应对信息技术安全挑战的重要性。安全战略已不再被仅仅视为安全工具的大杂烩，而被广泛地 – 也是正确地 – 看作一个持续的过程。

安全治理的目的在于保证在每一时间和地点都采用最适用的安全措施。这一概念是以下几个简单问题为依据的：

– 谁是参与者、要做哪项工作、怎样去做、何时去做？

– 谁是制定规则、确定并核准规则、落实并管理规则的参与者？

I.2.4.2 确定和管理风险

作为风险管理流程一部分的涉及信息处理、电信和网络风险的分析，必须为数字基础设施安全战略指引方向。信息技术安全风险（亦称为计算机风险、信息风险或技术风险）必须与机构面临的所有其它风险（战略、社会、环境等）一样不容忽视。

信息技术风险是必须得到控制的运行风险。安全需求分析是风险管理的核心，可用于制定安全战略和安全策略。在这一阶段需要提出以下几个问题：

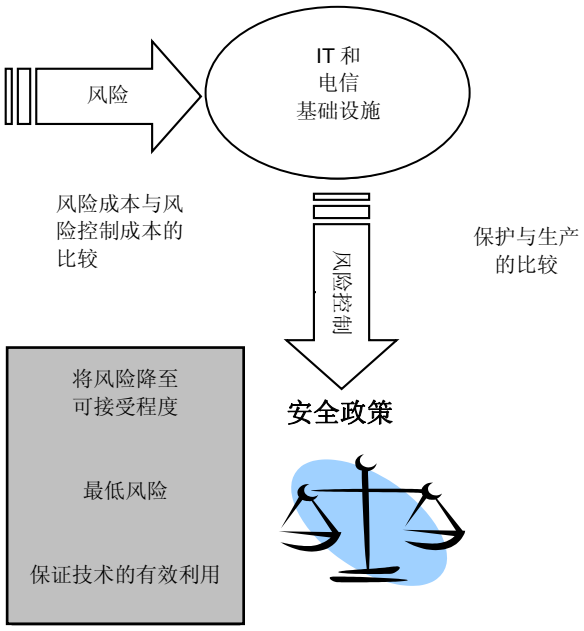
- 谁将负起风险分析和风险管理的责任？
- 什么是最佳的分析方法？
- 有哪些工具和方法可供使用？
- 这些工具和方法的可靠性如何？
- 应在多大程度上强调成果？成本有多高？
- 是否最好外包这一职能？
- 等等。

风险可以被定义为一种可在一定程度上预测的危险，可根据其可能造成的破坏及由此产生的危害加以量化。风险表示为因某些危害和危险造成的薄弱环节而丧失财产或价值的概率。

在确定部署理想程度的保护和安全措施的类型时，必须在风险规模（从财务角度看）和降低风险所需成本（见图 I.5）之间进行权衡。至少必须根据实际的局限性和可用的组织、财务、人力和技术资源，确定需要保护的资产以及保护它们的理由。采取措施必须立竿见影，也必须反映业绩与成本效益之间的平衡。

对于一个机构来说，控制信息技术风险意味着制定战略，确定安全策略，并就其策略和操作上的落实工作作出决定。

图 I.5 – 风险控制中的权衡：一项决策



I.2.4.3 确定安全策略

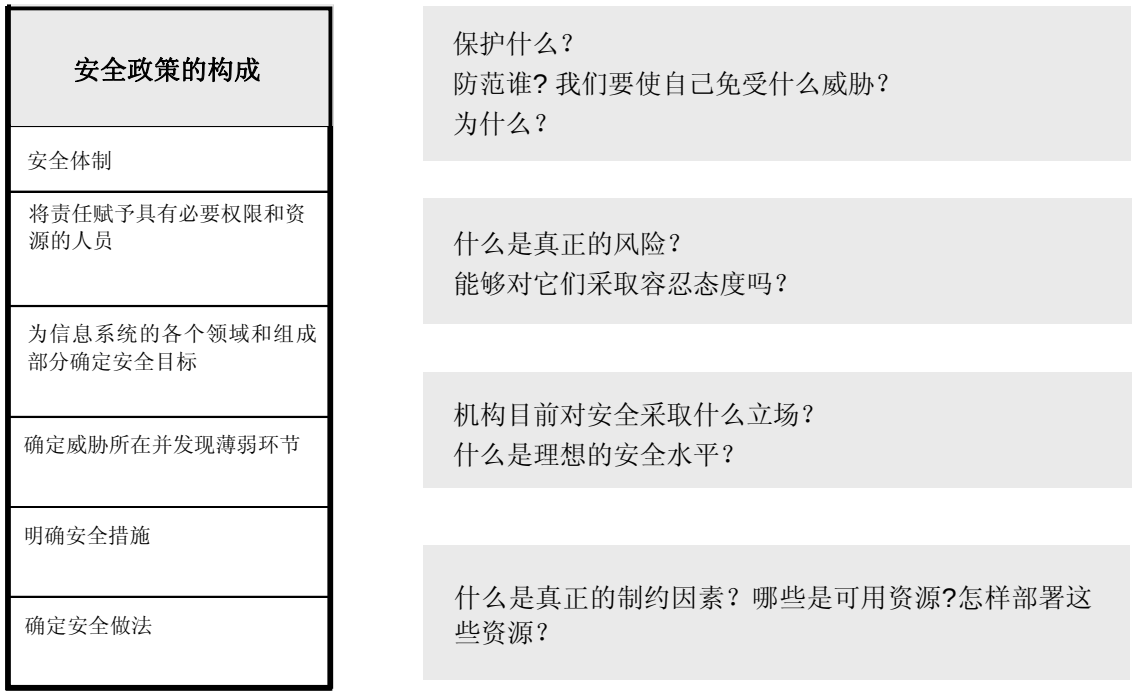
安全策略可将对于风险及其影响的认识转化为可供实施的安全措施，不仅可以推动针对安全问题采取的防护和补救行动，也有助于降低风险及其影响。

虽然不可能彻底消除风险，而且预测所有正在形成的风险也很困难，但必须减少需保护的环境和资源存在的薄弱环节，因为它无疑是众多安全问题的根源。

安全策略应在众多因素当中明确用于防范和降低风险的资源、结构、程序和计划，以确保运行、技术和信息风险得到控制。

国际标准化组织（ISO）17799 标准提出的安全管理行为准则，可以被视为制定安全策略的参考、一份风险分析列表、一种安全审计工具（无论是否用于认证）和一个用于安全目的的通信中枢。理解和实施这一标准的方式多种多样。其价值在于它能够在安全的设计、实施和维护等不同阶段解决安全涉及的机构、人员、法律和技术问题。该标准的 2005 年版（ISO/IEC 17799:2005）[4]将风险的评估与分析、财产与资源的管理和事件管理作为重点，从而说明了对安全管理方面的重视。

图 I.6 – 确定安全策略是安全管理的首要条件



一项安全策略的有效性不应以其预算的规模来衡量，因为它取决于风险管理政策和风险分析（见图 I.6）的质量。确定风险的因素包括机构的活动领域、其规模、其形象、系统的灵敏度、系统的环境和相关威胁，以及机构对其信息系统的依赖程度。

4 该标准的目录见本指南的附件B。

信息技术安全的质量主要取决于对信息资产的确定与评估、根据精心制定的安全策略在运行中采用的适当安全措施以及有效的管理。

I.2.4.4 部署解决方案

必须采取多种措施以提高信息技术和电信基础设施的安全性，其中包括：

- 提高认识；向所有利益攸关方提供有关网络安全的教学与培训；
- 建立可以发挥国家预警和危机响应中心作用的机构，有效地汇集此举所需的资源并使一区域内的多个国家共享其服务；
- 开展监测与核查（类似公路检查）；
- 加强网络公安队伍的专业技能，以推进侦办计算机犯罪的国际合作；
- 制定技术解决方案，以实现身份管理、访问控制、安全的硬软件平台的使用、备份基础设施、加密协议和运行管理。

I.2.5 从管理角度看问题

I.2.5.1 动态管理[5]

通过动态和连续的管理程序探讨安全问题，使机构能够通过不断调整和改进其解决方案，应对风险的动态特性和不断变化的需求。安全管理的质量将决定安全的提供水平。网络安全政策应由最高管理层制定。安全战略、政策、措施、程序和解决方案固然种类繁多，但在任何时间内其安全需求有待满足的机构也数量庞大。

以安全管理必须面对的动态环境为例，需要对发现和补救安全薄弱环节的程序加以考虑，并通过定期发布安全补丁程序加以解决。经过大体具有针对性的信息通报使人们能够随时了解检测出的薄弱环节，以及对它们的补救办法。如果只保持最低限度的安全，安全管理员或系统管理员则需要源源不断地安装发布的安全补丁程序。然而了解危险的系统隐患，不仅对安全管理者有益，对黑客也很有用，他们会试图赶在补丁程序被采用之前利用这些隐患。因此必须拨出足够资源实施动态管理，不断更新安全解决方案，以保持安全水准稳定不变。

发布的报警和补丁程序使管理员能够控制更新程序（即选择是否安装这些补丁程序）；自动模式不可能完成这项工作，因为这等于将定期和系统地安装补丁程序的责任下放给了软件出版商。

这就提出了一个责任的问题。例如，倘若有人利用未经补救的薄弱环节引发了问题，被拒绝的软件更新会带来怎样的法律后果？由于大量攻击正是利用了这些弱点，由谁做出决定以及系统管理员的责任便成为一个关系重大的问题。

---

5 随后的两节改编自2006年《信息与系统观察》中A. Dufour, G. Ghernaouti-Hélie所著题为“信息安全，依赖的陷阱”的文章。

安全的持续变换特性不仅对安全工具提供商和软件出版商、而且对系统管理员和安全管理员，都是一项重大挑战，因为这些管理人员缺少采纳所有可用的补丁和更新程序所需的时间。

鉴于计算机管理员、安全管理员和系统管理员享有机构全部信息技术资源的使用权，在对他们的行动采用严密的监视和控制程序（与他们可能使自己所辖系统面临的风险相对应）之外，他们还必需具备良好的职业道德。

I.2.5.2 外包与依赖性

提供反病毒和反垃圾邮件过滤器的业务提供商，实际上部分地承担了其客户的安全管理工作。这一趋势使安全任务与责任的划分开始发生变化。安全工作将逐渐向业务提供商和技术提供商转移。这一转移当然不会解决安全问题，而只是将它移交给了业务提供商，使他们不仅负责业务的提供和运行状况，也负责管理和维持一定程度的安全。

反病毒软件的出版商通常提供自动更新服务。新增的这一业务领域提高了软件租赁的吸引力，因为长期维护的责任移交给了出版商。这种做法更助长了应用外包的趋势和并行的商业模式。

全部或部分外包或下放安全工作，不是一个纯技术问题。它具有战略和法律性质，并提出了依赖于提供商这样一个带根本性的问题。

安全外包战略可包括政策制定、政策实施、接入管理、防火墙管理、远程系统和网络维护、第三方应用维护和备份管理等方面。选择承包商时，质量控制程序必需跟上，还要考虑到承包商的经验、内部专业技能、所用技术、响应时间、支持服务、合同安排（如达到某种成果目标的承诺）或法律责任的分担。

I.2.5.3 防范和补救行动[6]

网络防范，顾名思义，是主动出击，涉及人员、法律、机构、经济（实施成本/安全水平/提供的服务之间的比例）和技术方面。时至今日，信息技术环境的安全大多与技术方面相关。这种主要从技术角度理解信息系统安全的方式忽视了人的因素，从而给控制与犯罪行为相关的技术风险带来了现实问题，因为犯罪主要是人的问题，不是技术问题。因此，纯粹的技术对策不适于控制实质上的人为风险。

对信息技术犯罪的对策通常是闻风而动，进行查办，因而是事后反应，即事故发生之后采取的行动，这种方式的定义突显出保护措施方面的空白。我们不仅需要通过完善刑侦机制来防止和威慑网络攻击，还必需在安全策略中确定应对攻击和查办攻击者所需的措施。为此，必

6 本节是根据2006年 Ghernaouti-Hélie和Dunod所著《信息安全与网络》一书改编的。

须制定和落实备份及连续性计划，将涉及侦办网络犯罪的强制性规定纳入各种工作程序和目标之中，并确定具体的时间范围。

I.2.6 政治层面

I.2.6.1 国家的责任

国家承担着实现数字安全的巨大责任，在确定统一实用的相关法律框架方面尤其责无旁贷。国家不仅应该促进和提倡安全方面的研发工作，还应培育安全文化并做出遵守最低限度安全标准（安全应该嵌入产品和服务之中）的规定，同时加强针对网络犯罪的执法工作。这就提出了一个支撑国家和国际行动计划的财务模型以及公共和私营合作关系的问题。

在战略上，必须使防范、报告、信息共享和报警管理工作得到保障，同时还必须使人们更加了解风险管理和安全的最佳做法。另一项重点要求是法律系统的协调统一。还必须确定援助行动，促进执法和安全以及详细提出合作行动计划（正式/非正式、多边/双边、主动/被动、国家/国际）。

与此同时，在提出安全和威慑措施之外，还必须提供信息处理和通信技术方面的教育、信息与培训。提高对安全问题的认识不应仅限于提倡某种安全文化和网络行为准则。安全文化必须从一开始就以一种信息技术文化为基础。

各参与方必须学会管理对其使用新技术构成威胁的技术、运行和信息风险的方法。为此，国家必须鼓励报告网络犯罪案例，并保证在经济界各参与方以及法律和执法部门之间建立互信。

这些机构以及民防部门、应急服务、军队和安全部队也在打击网络犯罪中发挥着战术行动作用，负责保护、查办和修复工作。必须将针对信息技术和犯罪风险的监控、侦查和信息中心投入运行，以提供控制这些风险所需的防范措施。

每个国家都有责任为反映其具体价值的信息社会制定政策，并提供实现这一任务所需的资源，其中包括防范和打击网络犯罪的手段。

为全面、统一和协调地控制网络犯罪，需要一种政治、经济、法律和技术层面的应对措施，一种可为所有作为安全合作伙伴而参与数字链的各方采用的统一应对措施。

I.2.6.2 国家主权

人们企望的简单有效的安全与复杂的需求和环境之间的矛盾，更提高了将服务和系统及信息安全外包给专业提供商的吸引力。这一趋势派生出一种高度或全面的依赖性。

这是一大安全风险。对于依赖其鞭长莫及的外部实体从战略、策略和运行上管理其安全，国家必须提高警惕。

国家可在强制实行以下措施方面发挥作用：

– 创建用户友好、直观、透明和可核查的安全能力（安全至上）；

– 防止个人和机构陷入危险境地（避免松散配置、冒险行为、过分依赖等）；

– 遵守安全标准；

– 减少技术和安全解决方案中的薄弱环节。

I.2.7 经济层面

安全的目的不是赚钱，而是避免它的流失。虽然相比之下，安全成本（相关预算、安全产品费用、培训等）容易估算，但安全的效益却难以评估。从主观角度去看，人们可以假设安全措施固有一种防范某种潜在损失的“被动”有效形式。

然而，权衡安全成本和与事故、失误或恶意行为造成的损失相关的成本则颇有难度。安全成本是机构需求的函数，取决于需要保护的资产以及安全漏洞致损的成本。因此对以下这些问题没有现成的答案：

– 特别是在不同机构间基础设施的互连引发系列风险的情况下，怎样评估一个机构的风险暴露程度？

– 怎样评估因安全保护不足导致的形象受损或商业间谍活动造成的间接成本？

– 采取安全措施的机构能够从中得到什么？

– 安全具有何种经济价值？

– 安全的投资回报率有多高？

安全的经济价值必须从最广泛的社会意义去理解，同时考虑到新技术对个人、机构和国家的影响，不能将它仅限于安装和维护成本的范围内。

I.2.8 社会层面

要使所有互联网的参与者都认识到做好安全工作的重要性，并且在明确地计划和制定以及明智地实施了这项工作后，知道采取那些可以提高安全水平的基本步骤。

为建成一个负责任的信息社会而开展的涉及挑战、风险以及防范和威慑安全措施的信息运动和民众教育，是说服网民出资加入安全程序所必需的。

这项工作的重点应放在安全义务、个人责任、威慑措施以及不履行安全义务可能带来的刑事责任上。从更广泛的角度看，还必需进行有关信息和通信技术的教育与培训，不能只局限于安全和威慑措施。对安全问题的认识不能囿于培育某种安全文化的框框内。安全文化必须植入信息技术文化之中，或许可以 CIGREF（法国大企业计算机俱乐部）这一负责信息技术问题

的大型法国公司协会建议颁发的计算机用户许可证的形式出现[7]。

应将互联网建成一个对所有人开放的众议院，使所有网民都能享受到它所提供的基础设施和服务，并不会面临过多的安全风险。所有网络世界的参与者都需要制定、接受并遵守安全道德规范。

I.2.9 法律层面

I.2.9.1 关键的制胜因素

某些国家法律和国际工业体系使机构承担起落实安全措施的法律义务。因此，机构的经营者和得到授权的其安全管理人员，肩负着推行安全措施的义务（但不是以结果衡量的义务）。因安全废驰导致违规过失的法人机构，或许要承担刑事、民事或行政责任。这种责任能否成立无疑不会对违规过失者的刑事责任产生影响。

与数据处理相关的立法能够增强经济合作伙伴对国家基础设施的信心，从而推进国家的经济发展。因此，通过为合法的数据交换创造有利环境，合作伙伴可以成为使公众接受信息和通信服务的推动因素。立法和安全可以被视为国民经济的一对杠杆。建立在信任和质量基础上的网络安全，为服务经济的健康发展奠定了基础。

I.2.9.2 加强立法和执法

目前，网络犯罪没有得到有效控制，计算机安全协会（CSI）[8]和计算机应急响应小组（CERT）[9]的年度统计数字就说明了这一问题。因此可以看出，一些机构采取的安全措施往往可以对具体情况下的特定环境提供保护，但无力防范通过互联网的犯罪活动。造成这种情况的原因尤其与以下因素相关：

- 网络犯罪的性质（自动化、智能恶意软件、远程启动）；
- 黑客能够轻松和不受惩罚地窃得合法用户的身份，从而使法律系统无法发现犯罪者；
- 必须在侦查开始前划清职责范围；
- 负责反网络犯罪工作的部门缺少人力和物力资源；
- 网络犯罪的跨国特性经常需要请求国际援助和司法合作，由此产生的时延无法适应攻击者的行动速度和信息技术系统受到攻击后立即恢复运行的要求；

7 www.cigref.fr

8 www.gorcsi.com

9 www.cert.org

– 某些司法管辖区缺少相应的犯罪类别；

– 多数与信息技术相关的证据未加清晰界定，而且具有稍纵即逝的特性。

由于以上种种原因，法律体系依然未能在互联网环境中发挥作用。此外，正如存在合法避税手段一样，世上也有逃避法律的庇护所。计算机犯罪的泛滥并不一定说明法律不健全。现行法律已经覆盖了信息技术罪犯和黑客的许多行动。

网下的违法行为，在网上同样违法。

为满足界定适应新技术使用的相应法律框架的需要，必须形成新的立法，以充实无疑也适用于网络世界的众多现行法律。

如果没有实施立法的手段，那么只加强立法还不够。如果执法部门担负不起搜集和分析证据并查办犯罪行为人的任务，法律就起不到什么作用。如果黑客相信他们能够逃避惩罚，这就说明法律不起作用。

I.2.9.3 在尊重数字隐私的同时打击网络犯罪：微妙的折中

打击网络犯罪这一日益泛滥的国际灾难的必要手段，需要一种经过国际协调并可以有效实施的法律框架，以及在公安和司法部门层面真正开展国际合作的方式。

各国政府肩负着确保网络安全的重任。这特别体现在确定一种统一可行的适用法律框架，以培育一种尊重个人数字隐私权并加大打击网络犯罪力度的安全文化。

与网络犯罪的斗争必须将保护个人、机构和国家作为其首要目标，并铭记民主的根本原则。

打击网络犯罪所用的工具可能有损于人权，并破坏个人信息的隐私权。安全需要监控、审核与分析。为防止权利和地位的滥用、抵制专制方式的诱惑以及保证尊重网络隐私及个人信息保密等基本权利，必须实行监督制衡。

除 1995 年的欧洲指令外，还有许多历年来各国为保护个人信息而制定的其它法律：

德国： 1977 年 1 月 21 日颁布的法律

阿根廷： 1996 年的《个人信息保护法》

奥地利： 1978 年 10 月 18 日颁布的法律

澳大利亚： 1978 年的《隐私法》

比利时： 1992 年 12 月 8 日颁布的法律

加拿大： 1982 年的《私人信息保护法》

丹麦： 1978 年 6 月 8 日颁布的法律

西班牙： 1992 年 10 月 29 日颁布的法律

美国： 1974 年的《个人自由保护法》；1988 年的《私人信息数据库法》

芬兰： 1987 年 4 月 30 日颁布的法律

法国： 1978 年 1 月 6 日颁布并经 2004 年修改的《信息技术和自由法》

希腊： 1997 年 3 月 26 日颁布的法律

匈牙利： 1992 年的《个人信息保护及公共信息传播法》

爱尔兰：	1988 年 7 月 13 日颁布的法律
冰岛：	1981 年的《个人信息记录法》
以色列：	1981 年、1985 年和 1996 年的《隐私保护法》； 1986 年的《行政机构信息保护法》
意大利：	1996 年 12 月 31 日颁布的法律
日本：	1988 年的《计算机个人信息保护法》
卢森堡：	1979 年 3 月 31 日颁布的法律
挪威：	1978 年的《个人数据记录法》
新西兰：	1982 年的《官方信息法》
荷兰：	1988 年 12 月 28 日颁布的法律
波兰：	1997 年的《个人信息保护法》
葡萄牙：	1991 年 4 月 29 日颁布的法律
捷克共和国：	1995 年的《计算机系统内个人信息保护法》
英国：	1988 年 7 月 12 日颁布的法律
俄国：	《联邦信息、信息化和信息保护法》
斯洛文尼亚：	1990 年的《信息保护法》
瑞典：	1973 年 5 月 11 日颁布的法律
瑞士：	1992 年的《联邦信息保护法》
台湾：	1995 年的《信息保护法》

I.2.9.4 国际网络犯罪立法

于 2001 年 11 月 23 日在布达佩斯通过并于 2004 年 7 月生效（在五个缔约国批准之后，其中三个缔约国必须来自欧洲理事会国家）的《网络犯罪公约》[10]，是针对网络犯罪的第一个国际公约，其中包括以下内容。

- 实体刑法：
  - 针对计算机数据和系统机密性、完整性和可用性的犯罪行为；
  - 与计算机相关的犯罪行为；
  - 对版权及相关权利的侵权行为；
- 程序法：
  - 促进计算机和流量数据的保存以及迅速地向有关部门通报流量数据；
  - 在相关部门寻求数据通报所需的时段内，保存和维持计算机数据的完整性；
  - 生产通知单；
  - 搜查与扣押存储的计算机数据；
  - 实时采集计算机数据；
  - 充分保护人权和自由。
- 每个国家都应通过必要的立法及其它措施，在不损害其国内法律的情况下确定对以下犯罪行为的管辖权：
  - 有意在未经授权的情况下，全部或部分地访问计算机系统；
  - 有意在未经授权的情况下，截获进出计算机系统或计算机系统内部的非公开的数据传输；

10 http://conventions.coe.int/Treaty/ENT/Treaties/Html/185.htm

- 有意在未经授权的情况下，破坏、删除、劣化、更改或阻止计算机数据；
- 有意在未经授权的情况下严重妨碍系统运行；
- 为从事上述各类犯罪行为而生产、销售、购买使用、进口、分销或提供经设计或改装的装置；
- 有意在未经授权的情况下通过输入、修改、删除或阻止计算机数据以产生不可靠数据，达到使人误认为可靠数据并据之采取法律行动的目的；
- 有意在未经授权的情况下通过输入、修改、删除或阻止任何计算机数据或干扰任何计算机系统的运行，给他人财产造成损失，以达到未经授权地为本人或他人取得经济利益的目的；
- 将协助或怂恿任何这类违法行为以及任何从事这些违法行为的企图定为犯罪。

– 各缔约方必须对在所有下属情况下发生的犯罪行为确定管辖权：
  - 在其领土内；
  - 在悬挂其国旗的船舶上；
  - 其国民从事了犯罪活动，而这种活动在其发生地应受到刑法惩处或其发生地不在任何国家的领土管辖范围内。

– 涉及以下方面的国际合作条例：
  - 引渡；
  - 刑侦互助；
  - 对与计算机系统和数据相关的犯罪行为的惩处程序；
  - 搜集电子罪证；

– 创建互助网络；
  - 昼夜不间断的可用性；
  - 确定国家联络人；
  - 即时提供犯罪侦办援助；

世界各国都有应对网络犯罪的政治意愿。问题并不在于缺少像经济合作与发展组织（OECD）通过其《2002 年 OECD 关于信息系统和网络安全的指导原则 – 向安全文化迈进[11]》（图 I.7）颁布的法律或指导原则，而在于任务的困难和复杂程度，也在于实现打击导致互联网被恶意利用的网络犯罪，以及有组织犯罪目标所需的资源。

11 www.oecd.org/dataoecd/16/22/15582260.pdf – 见本指南附件F。

图 I.7 – OECD 关于信息安全的原则（2002 年 7 月）

认识	所有参与方都对信息系统和网络的安全负有责任
责任	所有参与方都对系统和信息网络的安全负有一份责任
应对行动	参与方应及时采取行动，共同防范、发现和应对安全事故
道德准则	参与方应尊重他方的合法利益
民主	信息系统和网络的安全应与民主社会的根本价值观相一致
风险评估	参与方应开展风险评估
安全的设计与落实	参与方应将安全作为信息系统和网络的一个关键组成部分
安全管理	参与方应采取综合的安全管理方式
再评估	参与方应对信息系统和网络安全进行复审和再评估，并对安全政策、做法、措施和程序进行相应修改

I.2.10 网络安全的基本要素

安全解决方案必须有助于满足诸如可用性、完整性和机密性（即 AIC 标准）等基本安全标准。本文经常提及的与此相关的其它标准有认证（即能够确认实体身份）、不可否认性（non-repudiation）和可归责性（imputability）（即可确认行动或事件业已发生）（见图 I.8）。

I.2.10.1 可用性

为确保业务、系统和数据的可用性，基础设施系统的构成成份必须大小适当并具有必要备份；此外，还必须提供资源和服务的运行管理。

可用性是在运行提供的业务的一个时间段内测出的。资源（如服务器或网络）的容量取决于可在服务提供期间处理的潜在工作量。资源的可用性与其可接入性密切相关。

I.2.10.2 完整性

维持数据、处理或服务的完整性意味着使它们免受意外或有意修改、篡改和破坏。这是确保其正确和可靠性所必需的。

为防止它们受到篡改，需要有一种确认它们没有在存储或传送过程中被修改的方式。

只有保护数据免受可用于修改截获信息的主动窃听技术的影响，才能保证数据的完整性。这种保护可以通过以下这些安全机制提供：

– 严格执行访问控制；
– 数据加密；
– 防范蠕虫和特洛伊木马等各种病毒。

图 I.8 – 网络安全的基本要素

系统必须	安全目标	安全工具
...可供使用	• 可用性 • 持续性 • 连续性 • 信任度	• 规模预测 • 冗余 • 运行与备份程序
...正确运行	• 运行安全 • 可靠性 • 耐久性 • 连续性 • 正确性	• 设计 • 性能 • 人体工程学（ergonomics） • 服务质量 • 运行维护
...向获得授权的实体提供接入（同时拒绝未经授权的接入）	• 机密性（保密） • 完整性（无变化）	• 访问控制 • 认证 • 差错控制 • 一致性检查 • 加密
...核实行动	• 不可否认性 • 真实性（无疑问） • 无可置疑	• 认证 • 记录、可跟踪性 • 电子签名 • 验证机制

I.2.10.3 机密性

机密性是为信息、信息流、交易、服务或在网络上从事的活动保守秘密，保证资源不会在未经授权的情况下外泄。

机密性可以通过访问控制和加密实现。

加密是通过将信息转换成一种任何不具备解密手段的人都无法识别的形式，帮助保护信息在传输和存储过程中的机密性。

I.2.10.4 身份确定与认证

认证的目的在于彻底消除资源身份的不确定因素。它预先设定所有实体（硬件、软件和人员）都得到了正确身份确定，而且某些特性可以作为它们的身份确定证明。尤其是信息技术资源的基于逻辑的访问控制系统，要求对实体的身份确定和认证进行管理。

实施身份确定与认证程序是为了促进实现以下目标：

– 数据的机密性和完整性（资源的使用仅限于被确认具有授权的用户，除获得修改授权以外的所有人都不得对资源进行修改）；

– 不可否认性和可归责性（可将行动追溯到经确定和认证的实体）、信息和交易的可跟踪性（可将传送内容追溯到经确定和认证的实体）和目的地证明（可以证明信息是发给经确定和认证的实体的）。

I.2.10.5 不可否认性

在某些情况下需要确认某个事件或交易已经发生。不可否认性关系到问责制、可归责性、可跟踪性以及在某些情况下的可审计性。

责任的确定是以存在个人认证及其行为归责机制为先决条件的。在有必要重组事件序列，特别是当进行计算机调查以查找发送数据所用的系统地址时，通过记录的信息跟踪行动执行情况的能力就变得十分重要。必须存储（信息日志）进行系统审计的后续分析所需的信息。这被称为系统的可审计性。

I.2.10.6 物理安全

工作站、服务器、信息技术区域以及服务（空调、电源配电盘等）所在空间必须受到物理保护，防止发生未经授权的使用和事故（水火等破坏）。物理保护是最为基本和普及的信息系统控制。

I.2.10.7 安全解决方案

鉴于多数基础设施的日常安全问题现状、提出的解决方案大量增长和安全市场日益繁荣，人们自然而然地提出了以下一系列问题：

– 提出的安全解决方案是否合乎要求？

– 这些方案是否得到了正确安装和管理？

– 它们能否用于或适用于急剧变化的环境？

– 它们能否解决系统管理员权力过分集中的问题？

– 能否利用它们解决因渎职、人为失误、设计缺陷、安装问题或技术和安全解决方案管理不善引起的安全问题？

– 等等。

第二部分

控制网络犯罪

第 II.1 节 – 网络犯罪

II.1.1 计算机关联犯罪和网络犯罪

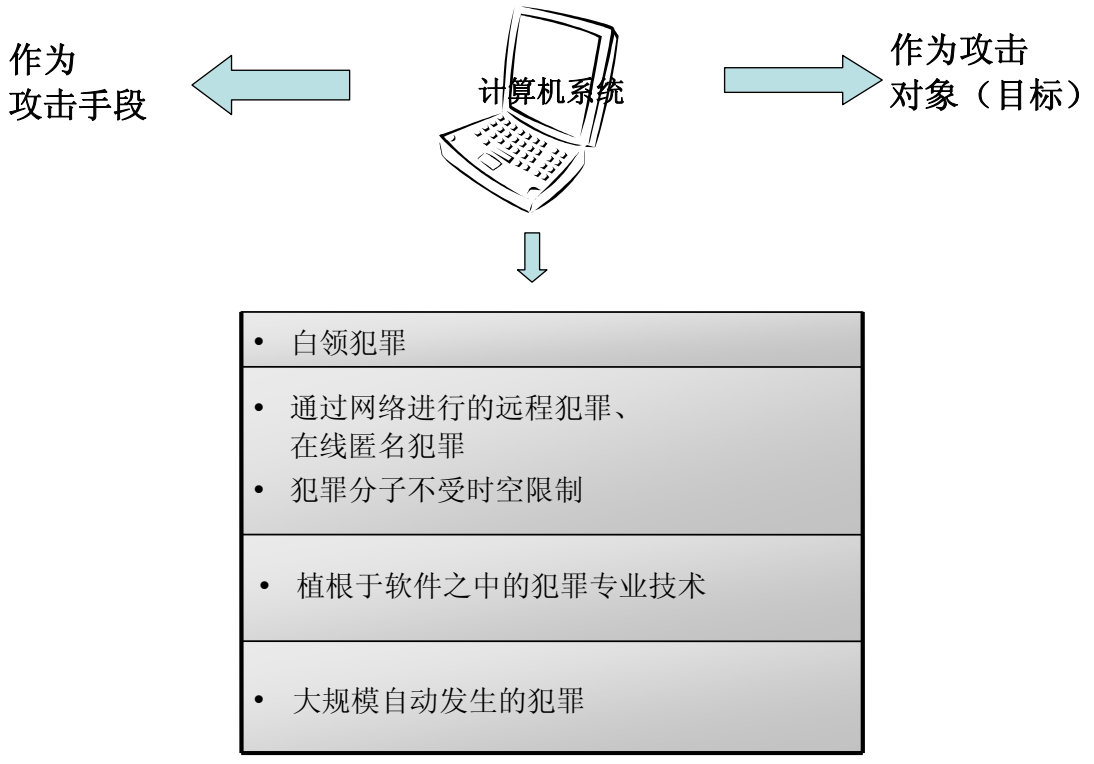
数字技术易受攻击，加之缺乏控制，因此造就了一个缺乏安全性的环境。罪犯分子自然会利用这种情况。实际上，每项技术都有可能被其用于非法目的，互联网亦不例外，网络犯罪状况已足以说明问题。

1983 年，经济合作发展组织（OECD）将计算机关联犯罪定义为在数据传送或自动处理中任何非法、不道德或未经授权的行为。

在计算机关联犯罪中，计算机系统或是罪犯攻击的对象、或是犯罪的手段，或二者兼备。这种犯罪与数字技术相关，属于白领犯罪中的一种。网络犯罪是使用互联网技术进行的一种计算机关联犯罪，它包括在网络世界发生的所有罪行。

在虚拟世界中，犯罪可以自动发生，为大面积网络流行病的爆发提供了途径，这些犯罪可以通过网络采用远程方式予以启动（犯罪分子不受时空限制），同时还能定时采取行动（见图 II.1）。

图 II.1 – 计算机关联犯罪的性质



互联网技术为多种多样的违法行为带来方便：盗窃、蓄意破坏信息、版权侵犯、违背职业诚信、数字隐私、知识产权、非法内容传播、反竞争攻击、行业间谍、商标侵权、篡改信息、拒绝服务和各种形式的欺诈等。

千年虫（Y2K）事件使人们开始关注软件的薄弱环节和整个社会对计算机的依赖。除此之外，其他众所周知的事件也帮助人们提高了对网络犯罪威胁的认识。这些事件包括：诸如针对雅虎的拒绝服务攻击（2000 年 2 月 10 日）和臭名昭著的“I love you（我爱你）”病毒攻击（2000 年 5 月 4 日）。自此之后，媒体对病毒攻击（如 2001 年 7 月的“红色代码”病毒或 2001 年 9 月的“Nimda”病毒）和拒绝服务攻击（如 2002 年 10 月 21 日针对 DNS 网络的攻击）等事件的报道已加深了人们对互联网威胁的现实性的认识。对于与计算机相关的问题，新闻媒体一直不惜笔墨加以报道。

II.1.2 互联网吸引犯罪的因素

II.1.2.1 虚拟化和虚拟世界

交易与物理媒介的分离（虚拟化）、包括加密在内的通信工具、隐写术及匿名是各国犯罪分子用来协同犯罪的手段，这些手段使他们省去了接头会面，使用起来灵活安全，完全不受任何惩罚。他们可以用传统方式或采用新技术成立团伙，谋划犯罪行为并付诸行动。互联网通达全球的特点使犯罪分子得以在全球范围内迅速地开展大规模行动。

数字世界和电信发展带来的强大功能是信息技术设计、实施、管理和控制不可避免出现问题的罪魁祸首。系统崩溃、故障、失误和人为错误，甚至自然灾害及基础设施之间的相互依赖性使数字基础设施从根本上蕴藏着一定程度的不安全性。

因此，薄弱环节被恶意利用的潜力极为可观。在现实生活中，可以导致：

身份盗窃、欺骗、未经授权的访问、对资源的欺诈性使用、感染、蓄意破坏、毁坏、篡改、泄密、盗窃数据、勒索、敲诈、骗取保护费和拒绝服务等。

这足以显示对各机构面对的计算机关联犯罪风险来源控制不足以及当前安全战略的局限性。

让用户可以通过网络远程工作的网络世界隐蔽在屏幕之后，为犯罪行为创造了理想的条件。的确，有些人可能在毫无意识到其行为犯法的情况下误入迷途，踏入犯罪的门槛。

II.1.2.2 资源联网

计算机网络和信息资源的广泛结合对利用新技术从事的经济犯罪具有极大的吸引力。今天各种形式的计算机攻击的共同之处在于，犯罪分子面临的风险较低，发动攻击所需要的资源相对于其所造成的潜在伤害和破坏微乎其微。使用电子手段的身份盗窃、方便易行的匿名及控制计算机的可能，使人们可以在没有任何重大风险的情况下轻而易举地从事非法活动。

II.1.2.3 非法闯入和薄弱环节的激增

利用系统薄弱环节的“非法闯入”（hack）普遍存在，有了建立在犯罪知识基础上的攻击库和软件，计算机攻击变得越来越容易。这种情况加之虚拟行动的可能性，纵容具有犯罪倾向的计算机专家和具有计算机技能的犯罪分子滥用其专业技能。在某些情况下，网络世界几乎不知不觉地成为方便犯罪行为的桥梁。

II.1.2.4 过失与薄弱环节

犯罪分子在充分利用互联网的组织和技术过失及薄弱环节，各国之间所缺少的统一法律框架及各国执法机构之间无效的协调。这类犯罪包括传统形式的犯罪（使用新技术从事的传统犯罪：洗钱、勒索和敲诈等）或基于数字技术的新型犯罪：系统入侵、处理器时间的盗用、源代码和数据库的窃取等。在所有上述情况中，环境格外有利于犯罪：风险最低、覆盖面广、利润丰厚。

图 II.2 概括说明互联网基础设施薄弱环节的来源。

图 II.2 – 利用互联网犯罪的主要特点

II.1.2.5 掀开网络犯罪分子的面纱

计算机关联犯罪极其复杂，还经常跨越国界，往往采用定时方式。这种犯罪在系统中留下的痕迹是无形的，难以收集和保存。它们以数字信息的形式储存在各种媒介中：工作内存、存储外围设备、硬盘、外接光盘和 USB 存储棒及电子器件等。问题是如何在数字搜查中找到多种多样的证据。从下列问题可以看出，数字证据的概念多么令人困惑：

– 如何识别相关数据？

– 如何对其进行跟踪？

– 如何对其加以存储？

– 有哪些司法证据规则？

– 如何恢复已删除的文件？

– 如何证明一条消息的来源？

– 鉴于将数字信息和实际作者准确地结合起来（虚拟化）困难重重，且身份盗窃愈演愈烈，如何仅凭数字踪迹确定一个人的身份？

– 已了解到从存储媒介中恢复的证据并非完全可靠（一台计算机系统与另一台系统对日期信息的处理方式不同，且这些信息可能被篡改），那么如何在法庭确立事实时对数字证据做出结论？

– 等等。

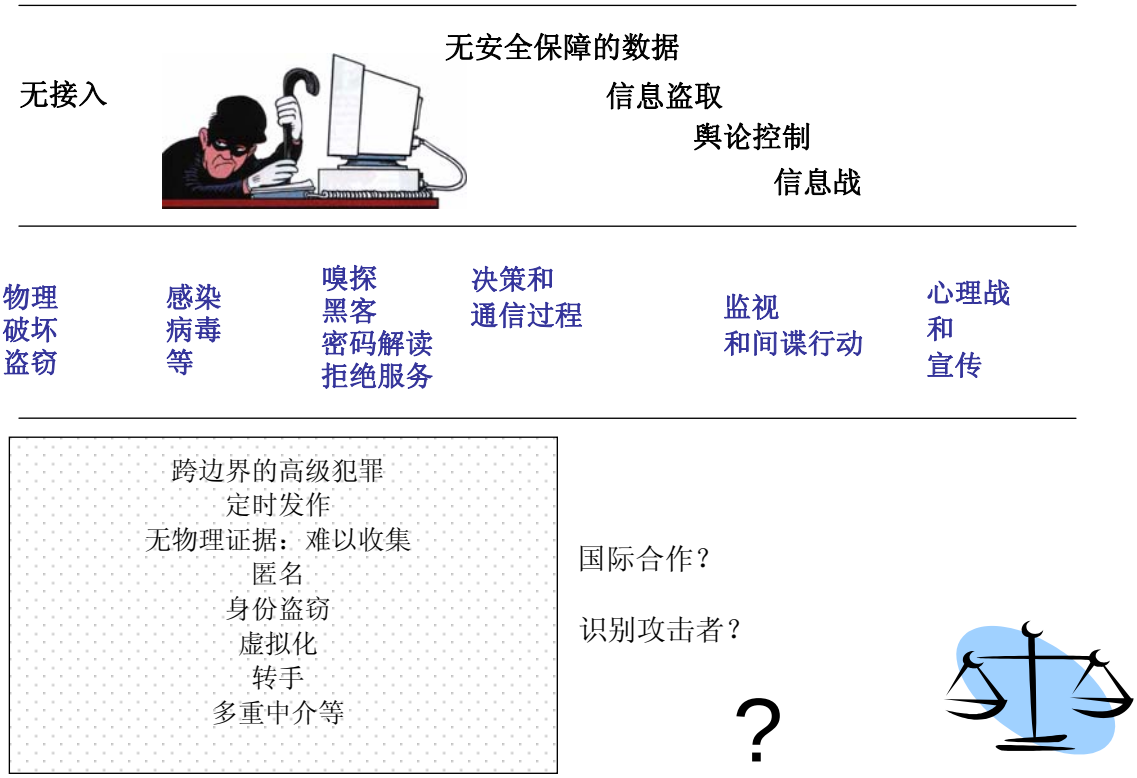
当数字证据分散在位于不同国家的多个系统时，取证更加困难。在这种情况下，能否成功完全取决于法制机构之间国际合作的成效，以及采取行动的速度。有效利用这些证据识别犯罪分子有赖于对请求进行处理的速度：如果处理速度缓慢，识别罪犯近乎不可能。

图 II.3 表明由物理破坏或盗窃设备、防止访问系统和数据、资源感染、拒绝服务攻击（或由于对系统的间谍行为或入侵）使决策或通信程序受到影响、信息盗窃和篡改（篡改意见、信息战）等恶意行为造成的不同类型的问题。该图还列举了网络犯罪的主要特点，由此看出识别罪犯是一项棘手的工作。

此外，在多数国家，利用高科技犯罪的犯罪分子的技能与执法和司法机构可用来惩治犯罪分子的资源极不匹配。无论是在国家还是在国际层面上，这些机构使用计算机技术的能力依然较弱，而且各国的情况差别很大。

在多数情况下，公安和司法机构凭借用于普通犯罪的传统调查方法对待网络犯罪分子以便将其识别并绳之以法。

图 II.3 – 识别攻击者困难重重



II.1.2.6 无疆界，数字安全港

犯罪分子对互联网无疆界的性质、一些国家在计算机关联犯罪方面立法的空缺以及互联网的多重管辖状况充分加以利用。

犹如避税港，数字安全港使犯罪分子得以托管服务器，传播非法内容或从事非法行动，毫不担心受到打击。将这些服务器安装于势单力薄的国家境内宛如为跨边界行动搭建了一个避风港。

由于缺乏国际监管和控制，司法调查和执行中开展的国际合作又徒有虚名，互联网因此充当了犯罪分子的保护伞。

目前，对于互联网上发生的以下各类犯罪行为，尚无任何有效的法律或技术手段：

- 组织严密的大规模软件、电影和音乐盗版，在网络世界中所占据的地位前所未有；
- 侵犯版权，背叛职业诚信，违背数字隐私和知识产权；
- 财产侵权、盗窃、破坏或毁灭财产，干涉他人财产（以电子手段擅自进入的概念）；
- 传播非法内容；
- 攻击竞争对手、行业间谍、商标侵权、篡改信息和针对竞争对手的拒绝服务攻击。

II.1.3 传统犯罪和网络犯罪

网络犯罪是普通犯罪活动的自然延伸。今天，犯罪分子既使用普通犯罪手段又使用非常规犯罪手段在网络世界从事犯罪活动。

互联网不仅为新的非法项目和活动提供了理想的条件，同时还为那些利用计算机进行各类欺诈并从事其他它犯罪活动的人提供了可乘之机。

互联网方便了人们发现并利用新的手段获得利益的机会。对这种强大的功能，犯罪分子自然不会视而不见。犯罪分子希望通过使用信息技术（IT）达到一本万利，同时还能将风险降至最低。

II.1.4 网络犯罪、经济犯罪和洗钱

通过互联网的经济犯罪不仅限于有组织的犯罪。现代信息通信技术使分散的个人（无论是作为个体工作者还是与各类规模机构合作的一员）为了共同的目的，卷入经济犯罪。

利用 IT，犯罪分子可以通过信息交流相互勾结。在互联网上将人与技能结合起来，从而形成虚拟的犯罪团伙。

由于经济犯罪需要高深的经济知识和高超的技能，显然是可利用现代 IT 手段予以“完善”的对象。

互联网有助于人们获得从事经济犯罪所需要的有关市场、法律和技术方面的信息和知识，同时还能用来物色受害者。

经济犯罪受到新技术的影响，这些新技术已成为犯罪分子数据库中的组成部分，同时将此信息置于其战略和决策程序的中心。

新技术为各种各样的盗窃行为、篡改、蓄意破坏信息和欺诈提供了方便，勒索、敲诈、欺骗和窃取数据均在互联网上屡屡发生。

实际上，信息资源已成为网络犯罪分子的潜在人质。勒索者也将其行为转向网络世界，任何人都可能突然发现自己沦为勒索、信息篡改或宣传炒作的受害者。此外，自 2003 年以来身份盗窃事件的激增表明犯罪分子充分把握了互联网带来的匿名优势，利用假身份逃避惩罚或承担犯罪分子应负的责任。通过互联网而轻而易举实现的身份盗用是引发非法行为的重要因素。

像所有利用现有技术基础设施的犯罪分子一样，洗钱者也越来越多地利用互联网，从种种犯罪活动（如贩毒、走私武器、腐败，嫖娼、虐童、偷税漏税等）中捞取钱财并使之合法化。

尽管通过互联网的洗钱行为很少得到报道，但这种行为日益猖獗。互联网因为其虚拟化的性质（匿名、网络、传输速度）和无领土限定的自由（跨边界、职权和管辖权互相冲突），使洗钱者有机可乘。互联网能够通过转账、投资和资本化将不法资金转移至合法的经济渠道。

在线投资、赌博和商务（如，通过销售虚幻的物品和服务挣取实实在在的金钱），使人们获得似乎名正言顺的收入。这种情况难以监控，又几乎无法予以惩治。电子银行、网上房地产交易、虚拟店面及电子现金均可用来为犯罪所谋取的收益洗钱。普通用户在使用一些虚拟服务时可能不知不觉地变成洗钱行为的帮手。商业机构也会稀里糊涂地卷入其中，由此可能造成灾难性法律和商业影响。对于企业来说，这是一个巨大的风险来源。

目前，有效控制利用 IT 洗钱的手段依然寥寥无几。

II.1.5 网络犯罪 – 普通犯罪的延伸

多数网络犯罪采用普通犯罪的形式，一般非常隐蔽，但不同的是高度依赖于网络化的资源和人力。除企业本身外，企业的 IT 和信息资产也会在犯罪组织猎取利益中成为重要目标。这是一个战略性威胁，因为放钱的地方不仅有银行，还有信息系统、公司企业和养老基金。

当企业通过网络服务器、门户网站和电子邮件系统向互联网敞开大门时，就已置身于受到犯罪分子关注的风险之中，同时为犯罪分子提供了潜在的立足之地。尽管互联网是一个能力强大的通信工具，同时也代表着一个混乱、复杂、多变和险恶的环境，成为破坏组织机构和从事犯罪的手段。应将互联网作为犯罪高发区谨慎对待。由于各组织机构非常重视各自的网上表现，因此对互联网犯罪行为的猖獗都有可能起到助纣为虐的作用。

如今，各国安全也面临着 IT 犯罪威胁的挑战。互联网技术已成为所谓信息战的核心。信息战主要针对经济目标，可以对商业运作造成巨大影响。互联网不仅可以使人们操控信息，同时还是一个理想的造谣工厂，为传播虚假信息或制造混乱煽风点火。互联网还方便了间谍行为及其他情报搜集活动，因为拦截互联网中流动的信息可谓易如反掌。

II.1.6 网络犯罪和恐怖主义

当攻击的目标系统为关键性基础设施时，网络犯罪便染上了恐怖主义的色彩。随着互联网技术的广泛使用，各国必不可少的基础设施（能源、水利、交通、食品物流、电信、银行和金融、医疗服务和政府职能等）变得愈发不堪一击。

尤其需要强调的是对于多数基础设施运行来说不可或缺的发电和配电系统。网络恐怖分子的主要目标之一就是控制关键性基础设施。针对基础设施运营机构所拥有的计算机扫描（寻找可用来在未来进入该系统的漏洞）次数的增加可以充分说明问题。

目前，对于网络恐怖主义的构成，尚无广为认可的定义。简单的定义无疑是将其看作发生在网络世界的恐怖主义。从本义来说，恐怖主义通常指系统地利用暴力以实现政治目标。

由于不良行为造成的互联网或网络部分瘫痪是否会在网民、部分经济团体和普通大众之中传播恐惧呢？提出这种质疑是完全有道理的。

其实，我们主要面对的是经济恐怖主义，其宗旨是破坏利用互联网开展工作的组织。

网络恐怖主义一词自 9 月 11 日袭击发生以来一直含糊不清，应慎重使用。不应忘记的是，首起广而受报道的分布式拒绝服务（DDOS）攻击发生在 2000 年 5 月 10 日，它出自一个昵称为“黑手党男孩”之手。几个月后，这个年轻人被发现并拘留。尽管他的行为动机依然不得而知，但是很有可能牵扯政治因素。

如果此次攻击发生在 911 之后，很可能立即被列入网络恐怖主义。

在缺少具体资料，如攻击者的声明或身份的情况下，很难将一次攻击定义为网络恐怖主义。

网络恐怖主义一词是对新型威胁极其含糊的分类。揣摩幕后攻击者或攻击者团体的动机或目标并非轻而易举。当只有攻击目标一目了然时，靠想象判断黑客、恐怖分子、唯利是图者、激进分子、普通罪犯或恶作剧者的动机是根本没有把握的。

通过一类计算机关联攻击无法确切地说明攻击者的动机或目标。这是打击计算机关联犯罪的障碍之一，因为要确定犯罪动机需要更多的信息。

不论网络恐怖主义是否通过威胁关键性基础设施，传播思想或操控信息扰乱经济，其所构成的新的威胁必须认真对待。网络恐怖主义不仅威胁信息系统和以互联网为代表的网络世界，同时可能以对生命和肌体的间接威胁危及人类安全。

II.1.7 黑客

了解黑客的动机和技能水平有助于评估攻击的严重性，同时有助于制定国家战略。要保护一个信息系统，需要了解应防范的对象。目前主要有两类黑客：以此为营生的专业黑客和渴望扬名四海的业余黑客（图 II.4）。

专业黑客一般属于以下一类或多种类型：

- 目标机构的直接竞争对手；
- 公务员；
- 受雇佣者（在私营或公共部门机构领取薪水的黑客）；
- 其他犯罪分子。

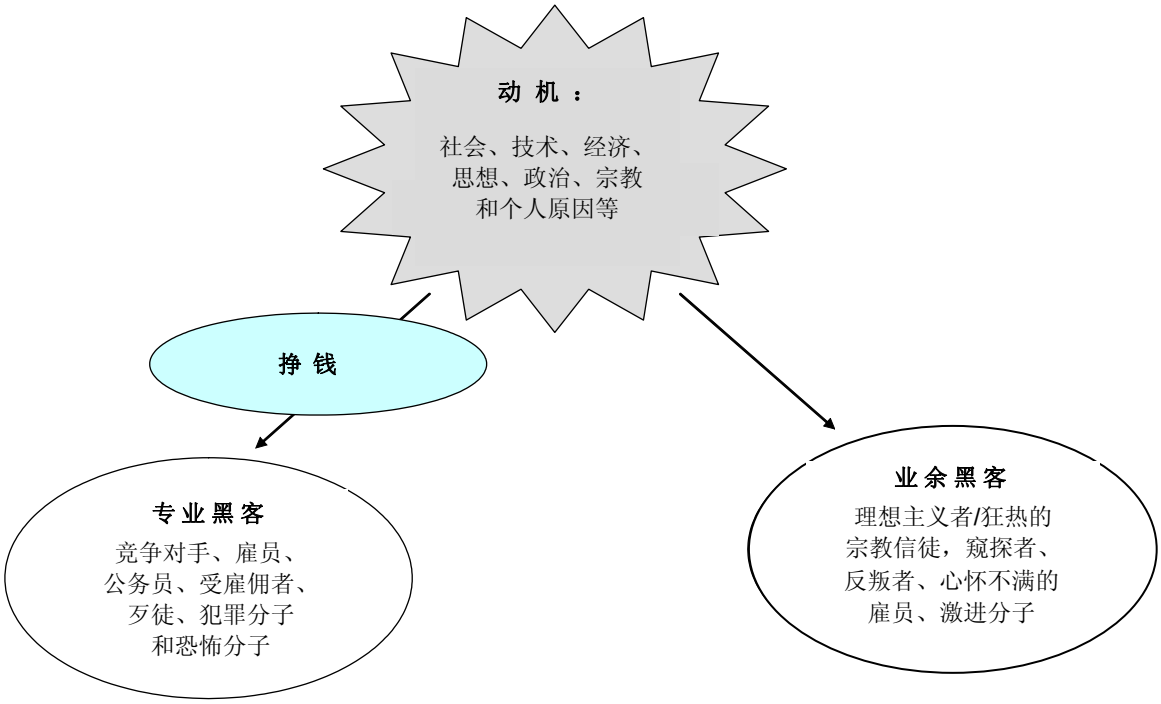
业余黑客包括：

- 技师、老“黑客”的徒弟、主要想炫耀技能的网虫；
- 窥探者；
- 亦称为“脚本小子（script-kiddies）”或“低级黑客（kidiot）”的恶作剧者，他们被擒获时，往往名噪一时，尽管他们曝光率最高，但我们不应认为他们是黑客中的唯一代表；

– 心神不安者；

– 某种思想或宗教的激进分子（专业多于业余）。

图 II.4 – 黑客的两个主要类别



这些个人行为的潜在动机中可能涉及社会、技术、政治、财务或政府因素。

所谓社会因素一般指获得同行认可的需求，往往关系到某团伙或组织的成员。这些黑客为不辜负组织期望昭显其对组织的重要性。他们的行为类似城市涂鸦者，并建立在极为简单的社会阶层观之上。这种情况在恶作剧者之中更是屡见不鲜。他们实行非法闯入是因为可以获得高人一等的感觉，从而控制那些对他们来说在日常生活中飞扬跋扈的机构。

技术动机较为罕见，其主要目的是试探技术的极限，验证这些极限及薄弱环节并掌握技术能力。

政治动机着眼于吸引媒体关注的事件，从而使人们的注意力转移到重大问题之上。通过提高公众意识促成问题的解决。政治动机与恐怖主义之间的界限极其微妙，至少从理论角度来说如此。司空见惯的是在一个人的政治目标之后通常隐藏着社会动机。

金钱刺激可以是一项重要因素，它是大量非法行为的起因。不劳而获的诱惑致使白领犯罪分子（骗子、勒索者和恶意竞争者等）在互联网上施展伎俩。

列在清单最后的一群人涉及政府。这类非法闯入行为包括信息战和间谍行为，犯罪者是为国家效劳的政府部门。

各类犯罪分子都已迅速适应了计算机的时代，将非法闯入增加到自己的作案手段之中。论到滥用技术的新招数，他们的足智多谋令人恐惧。

II.1.8 烦扰和恶意软件

II.1.8.1 垃圾邮件（Spam）

垃圾邮件是为商业或宣传目的发送的批量推介性电子邮件，其目标是诱惑网民订购产品或服务。

尽管服务提供商为寻求拦截垃圾邮件的方法投入了巨大的技术和财务资源，尽管公共主管机构打击垃圾邮件的决心众所周知，尽管一些公然制造垃圾邮件者也曾受到惩治，但垃圾邮件依然屡禁不绝。2003 年 9 月，垃圾邮件占电子邮件总流量的 54%。根据 IDC 的统计，2005 年，美国境内传送的垃圾邮件超过 120 亿件，占总流量的 38.7%。

最糟糕时，垃圾邮件构成了电子邮件的轰炸攻击，邮件服务器严重超载，用户邮箱爆满，管理人员麻烦不断。用户可能会成为所谓通讯录链接（list linking）的受害者，他们的地址未经同意即被垃圾邮件制造者编入通讯录。唯一可退出列表的方法就是更改自己的电子邮件地址。这是一项很烦琐的工作。尽管这种措施立竿见影，负面影响也相当严重，用户必须将邮箱地址的更改通知所有通信人。

像垃圾邮件（junk mail）一样，发送大量推介性、不合时宜的甚至令人震惊的信息可以被看作是对用户隐私的入侵。但是，除此之外，垃圾邮件还越来越多地作为制作恶意程序（恶意软件）的手段，其破坏性成倍增加。

II.1.8.2 恶意软件

IT 安全主要监督机构（包括计算机应急响应小组（CERT）[12]、美国联邦调查局（FBI）和法国信息安全协会（*Clusif*））在其网络犯罪年度报告中指出，运行在计算机中而其所有者却丝毫不知的恶意和垃圾程序数量持续增长。

其中包括以下各类软件：

- 下载软件（downloader）：用于远程下载和安装数据和程序；
- 按键记录软件（keylogger）：用于监测使用者输入计算机的按键、同时还有在软件层面看不到的按键记录硬件，用来记录这些数据；
- 僵尸（zombies），或“机器人”（“bot”机器人的缩写）软件是为建立一组隐形计算机使系统实现远程控制的程序。每天都可以发现 25-50 个新的机器人软件。这些软件的目的在于滥发邮件，进行网页仿冒（phishing）攻击或传播广告软件（adware）。2005 年 10 月，荷兰警方抓获三人，涉嫌运行 100 000 台机器人计算机以便发动拒绝服务攻击，目标针对受害者的 PayPal 和 eBay 账户[13]；
- 广告软件：用于定制商业交易；

---

12 www.cert.org – 见www.cert.org/stats/cert_stats.html网址上的1998-2005年统计资料。

13 来源：Clusif报告 – 《网络犯罪概览》，2005年：www.clusif.asso.fr/fr/production/ouvrages/pdf/PanoCrim2k5-fr.pdf

– 间谍软件：顾名思义，用于秘密记录信息。根据软件出版商 Webroot 的统计，互联网上有 10 万多种不同类型的间谍软件，分别载于 30 多万网址上。一般来说，一台上网的 PC 机在使用者不知情的情况下平均安装 28 个间谍软件。企业内 80%以上的计算机装有一个或多个间谍软件。这些软件参与了 70%的攻击。

除上述形式的恶意软件外，还有病毒和相关产品（蠕虫、特洛伊木马和逻辑炸弹）。

由恶意代码构成的病毒在使用者不知情的情况下安装在系统中，同时具有自我复制能力（对于多型病毒，复制品并非完全相同，而是一种突变）。病毒攻击主机并感染其它与之接触的设备。辨别病毒可以凭借其签名、行为、复制和扩散方式及其所导致的失能类型。

像生物模拟一样，计算机病毒的目的在于对自身进行复制或传播。它从一台计算机传播到另一台计算机，将自身副本附于程序。最普遍的做法是将副本作为电子邮件的附件。这种情况往往与使用者的行动相互关联。病毒对被感染的完整信息资源所造成的影响千差万别，小则使人心烦意乱，大则造成严重破坏，影响系统的可用性和机密性。

通用术语“病毒”指能够复制并传播自我的有害计算机程序（造成感染、破坏和资源分配不当等）。

据估计，2005 年运行在网络中的新病毒达 5 万多种[14]，如世界病毒跟踪中心描述的 HTML_NETSKY.P 病毒自 2004 年 4 月在全球感染了 855 244 台电脑。据计算机安全学会估计，受到影响的企业损失达 4 200 万美元。据 F-secure.com 网站估计，每天运行中的病毒总数多达 4000 多个。

蠕虫也是穿梭于网络中的计算机代码比特，往往自行其是，与使用者的行动无关。一般来说，蠕虫旨在束缚系统资源（内存和带宽），由此影响系统的可用性，或实现对受到影响的系统的远程控制。

被称为特洛伊木马的恶意软件，通常先隐藏在普通软件或帮助文件之中，然后渗入系统，对其加以控制以便盗取处理器时间，篡改或毁坏数据或程序，造成瘫痪，从事嗅探或其它形式的恶意行为，或只是保持睡眠状态并伺机发起攻击。

逻辑炸弹是由某一事件（如生日）激活的病毒，用于攻击主机系统。

所有这些均不应与计算机“缺陷”相提并论。漏洞是指程序错误，在更多情况下，表现为功能问题的设计差错。

病毒传播和执行的一般方式是等待使用者无意间造成激活，例如，启动一个受到感染的程序。过去，大多数病毒是通过电子邮件附件传播的，一般通过点击文件图标得到激活。

---

[14] 来源：IPA/ISEC计算机病毒事件报告。

很多恶意软件伪装成为用于导航、连接和定制服务的附加帮助程序。实际上，这些程序旨在进行监察（信息盗窃、密码盗窃和流量监察），利用计算机资源或发动攻击。它们还被用作发动分布式拒绝服务攻击的散发和控制工具。数千种这样的程序运行在网络之中，目的就是谋取钱财。

拒绝服务（DOS）和分布式拒绝服务（DDOS）攻击旨在损害系统资源。一般来说，通过对日常服务反复提出请求造成服务器超载，使服务器无法向固定用户提供服务（拒绝服务由此得名）。由于这些请求类似普通请求，这种攻击难以打击（致使系统瘫痪的原因是请求的数量）。为增强攻击有效性，请求同时从众多不同地点或系统发出，由此构成分布式拒绝服务攻击。

各类恶意软件的传播方式不仅包括免费软件或演示系统软件及色情网站或游戏和电子邮件，同时还包括垃圾邮件和在线讨论组。

恶意软件无论使用何种方法渗入系统（如广告软件，但间谍软件例外），都有可能包括获得用户明确许可或默许的步骤。一旦得到安装便转而用于非法用途，在多数情况下，恶意软件不经过用户同意就加以执行。这些软件偷偷地收集并转发数据（例如有关浏览习惯、对定向广告的兴趣等数据）。这些恶意软件可以像无人机一样从事诸如垃圾邮件和网络钓鱼等非法活动，为控制者谋取金钱之利尽心尽力。发现并卸载这种软件并非轻而易举。通常，用户没有控制这些风险的必要技能和手段。

“Phishing”是垂钓的代名词，指渔民利用鱼饵引鱼上钩，然后将之捕获。在这里指利用邮件程序发动攻击，吸引或诱惑网络用户披露可用于犯罪目的（如欺骗和勒索）的敏感信息。2005 年 1 月 26 日，网络日报（*Journal du net*）[15]报道，该报在一个月内（2005 年 9 月）记录下五千多个活跃在网络中的网络钓鱼网站，110 个不同品牌受到攻击。

一般来说，网络钓鱼攻击使用电子邮件信息进行。这些邮件貌似发自一个用户可能会打交道的真实机构（如邮局、银行、经销商和在线拍卖网站）。但是攻击者还可能使用电话呼叫、即时消息（IM）、或手机短信，甚至采用与受害者直接接触的方式。

15 www.journaldu net.com

II.1.8.3 趋势

如今，病毒的主要目标不再是大规模破坏免责数据。其设计初衷更加明确，即挣钱。本着这种新的务实的目标并基于这种目标自身的特点，病毒可用于欺骗。因此，对于从事经济犯罪的有组织的犯罪分子来说，病毒已成为极其有利可图的工具。

有关垃圾邮件及烦扰方面的内容，法国信息系统安全协会（*Club de la sécurité des systèmes d'information français*（Clusif））[16]有报告指出，2003 年美国在线过滤掉 5000 亿条垃圾邮件信息。打击垃圾邮件组织 Spamhaus[17] 2003 年 12 月披露，世界上最猖狂的垃圾邮件制造者在一天之内发送了 7 000 万条电子邮件信息！

Clusif 2003 年 5 月做出的又一份报告阐述了一个被称为水牛的垃圾邮件制造者是如何因发送 8.2 亿条推介性信息而在美国被判决向互联网提供商 Earthlink 缴纳 1 640 万美元的。根据 Ferris Research 公司的统计，2003 年的垃圾邮件使欧洲企业界损失达到 25 亿美元，美国 89 亿美元，加上服务提供商为阻止垃圾邮件而投入的 5 亿美元，滥用电子邮件问题之严重可见一斑。很明显，这是一个不容再忽视的问题。

除因欺诈造成的直接损失外，服务中断、停运、销售亏损、间接损失、形象和名誉的破坏以及恢复系统运行的成本亦应得到考虑。对于计算机犯罪的目标机构而言，这是一笔极其可观的开销。

通过观察可以看出，攻击数量与日俱增，计算机病毒已成为名符其实的流行病毒。盗窃身份的情况越来越多，且手段日益高明。欺诈以及各种形式的诈骗和讹诈在网络世界已成为家常便饭。它们跨越时空界限，无孔不入，影响到每个人和各个行业。

包括移动系统（笔记本电脑和手机）在内的任何系统、硬件或软件平台、或操作系统均不具有免疫性。

II.1.9 互联网犯罪的主要形式

II.1.9.1 诈骗、间谍和情报活动、敲诈和讹诈

各种常见的有组织的犯罪（勒索保护费、贩卖人口、设立骗局和盗窃等）均可利用新的信息技术，特别是互联网。互联网便于沟通，为那些从事任何形式的走私（无论是军火还是人口）和诈骗行为（针对财产、计算机系统和基础设施的攻击；数据盗窃；版权侵犯）的犯罪分子大开方便之门。

犯罪分子以各种形式利用互联网。一些人使用他人身份以便利用他人帐号购买物品。常见的方式是信用卡欺诈，即创建一个与任何实际帐户没有关联的有效卡号。犯罪分子使用该信息在线购物，利用“可用”地址完成一次性交付。损失落在银行或商家头上。当持卡人的信用卡号被扒手或无信用的商家泄露给一个专业团伙时，他们也会成为受害者。

---

16 www.clusif.asso.fr

17 www.spamhaus.org

另一种诈骗行为涉及虚构服务的销售（大学文凭、制造子虚乌有国家的外交护照、虚构产品的拍卖等）。

网络也方便了间谍和情报工作，网上传送的信息很容易受到非法劫持。

还应指出的是，加密等安全通信手段的系统化使用，帮助专业恐怖分子获得了更大的安全性，减少了易于被执法机构拦截的信息量。

互联网成为传播犯罪和非法行为方式的有利媒介，使潜在的犯罪分子勇气倍增。

II.1.9.2 危害人类罪

通过互联网可以为从事应受到法律严厉制裁的行动构成秘密虚拟社团。这些行为可能涉及色情、恋童癖或所谓暴力影片（具有因暴力和折磨导致真人死亡的镜头的影片）。这类犯罪通常与贩卖人口（主要是妇女和儿童）有关。影片和照片可以共享，很难被警察发现。由于服务器经常置于缺少执法或执法能力薄弱的国家，在很短时间内使用专用互联网中继聊天（IRC）和对等交流（P2P）手段，犯罪分子获得了更大的行动自由。

所有这些非法活动均属于普通法的范畴。问题是通过互联网和物品与人的自由流动所实现的专业化大规模行为，是否已转化成为危害人类罪。

在危害人类罪中还包括对隐私、个人形象、专业机密和数据隐私权的侵犯。针对儿童的犯罪包括传播可能被儿童看到的色情信息。

II.1.9.3 盗版

数字信息方便复制，为非法复制培育了市场。软件、音乐和视频影片发行商为此损失了数百亿美元。

人们还发现，通过复制网络上的现有文件剽窃的学术作品数量巨幅增长。

知识产权的侵权形式多种多样：伪造作家作品（包括软件）、设计、模型和商标等。

II.1.9.4 信息操控

信息操控的形式五花八门，例如泄露内部文件以便使一家企业陷入瘫痪，通过假冒网站发送电子邮件，请求慈善捐助等。

互联网本身特别适合传播谣言和错误信息。同时，互联网对违反媒体法律、犯罪煽动行为、为危害人类罪进行辩解、对恐怖主义的辩解和煽动恐怖主义、煽动民族仇恨、历史修正论（否定论）、人格毁谤和侮辱起到推波助澜的作用。

图 II.5 列出了一些由互联网推动的犯罪类型示例。

图 II.5 – 由互联网推动的犯罪类型示例

危害人类罪 – 个人伤害 – 隐私 – 个人形象 – 诽谤 – 专业机密 – 数字隐私 – 儿童
侵犯财产罪 – 诈骗 – 对信息系统的攻击 – 违反媒体法律
煽动犯罪 – 对危害人类罪进行辩解 – 对恐怖主义进行辩解和煽动恐怖主义 – 煽动民族仇恨 – 否认毁灭行为 – 诽谤 – 侮辱
违背知识产权 – 伪造作家作品（包括软件）– 设计或模型造假 – 伪造商标 – 非法在线博弈

II.1.9.5 公众机构的作用

人们从未象今天这样希望公共主管机构发挥其一贯的执法及防范欺诈和犯罪的作用。公共主管机构亦应积极向大众开展教育，提高其对问题的认识。尤其有益的是，要向公众提供有关在使用互联网时如何保护人和财产的参考资料。

执法机构在技术方面落伍是非常危险的。几年后再为追赶新技术付出的代价将大大超过购买新系统的直接投入。与此同时，影响日益深重的有组织的犯罪对社会亦将造成相关的社会成本，招致社会动荡的风险。

同时，对互联网进行过度监管也是不适宜的，并有可能与保护交流机密性和尊重个人隐私的需要背道而驰。

II.1.10 安全事件和未报告的网络犯罪

应指出的是，有关网络犯罪的统计数据寥寥无几。这是一种新的犯罪形式。多数事件未曾报告给公安部门。此外，这些违规行为跨越国界，而刑法却限于国家范畴，因此很难就各国定义不同的罪行编制统计数据，例如，当一个计算机系统使用盗窃用户身份进行欺诈性财务交易时，既可以归类为与计算机关联的犯罪，亦可以归类为财务罪。

尽管如此，由国家基础设施保护中心（NIPC）协调的美国机构 – 分散式计算机调查和基础设施威胁评估（CITA）团队 – 就网络犯罪的猖獗状况做出了一些说明。

自本世纪初以来，向 CERT[18]报告的安全事件数量以及向法制机构报告的攻击数量持续增长，使人们对计算机犯罪有了更为深入的了解。2003 年，垃圾邮件量迅猛增长，并从互联网发展到手机短信。为数众多的垃圾邮件制造者被抓获和判刑。美国和欧洲（西班牙、意大利、法国和英国等）均开展了大规模公安行动（美国 2003 年 5 月的 E-Con 行动和 2003 年 10 月的网络排查行动），这说明各国当局正在对新的犯罪环境做出反应并采取相应手段。对一些病毒写手和垃圾邮件制造者的拘捕和判刑显示出当局处理这些新型问题的决心。但是，考虑到日常的垃圾邮件和流行病毒的实际数量[19]，定罪比例依然很低。

未报告的网络犯罪比例难以估量。法制机构、公安和大众了解的网络犯罪可能仅有 12%[20]。要想获得计算机关联犯罪的实际数据困难重重，这正是分析计算机关联犯罪现象并确定其严重性的巨大障碍。

缺乏官方统计数据的部分原因在于各机构：

- 希望避免对攻击进行宣传；
- 可能尚不知自己已成为网络犯罪的受害者，尤其是在被动攻击的情况下（对数据和流量的公然劫持、被动监听、未发现的入侵等）；它们还可能在攻击后很久才发现问题，此时做出任何反应已无意义；
- 不知如何面对危机状况；
- 对法制机构和公安以及自身应对此类问题的能力缺乏必要的信心；
- 希望自己处理问题。

黑客的技能、攻击的深度和力度以及攻击者的工具套件日新月异，攻击的实际数量也在持续增长。这种多变的趋势所带来的前所未有的复杂状况难以应对。如果在国际层面上没有一个强大的政治意愿和所有参与方的责任感，以及私营和公共部门之间的有效合作，任何安全措施，无论是技术措施，还是法律措施，均无法全面解决安全问题，只能头痛医头，脚痛医脚，从而无法有效应对计算机关联犯罪。

---

18 CERT协调中心，卡内基梅隆大学（http://www.cert.org）

19 日本的信息技术促进机构信息安全中心（IPA/ISEC）在其2004年的计算机病毒事件报告中指出，在2003年12月，该中心发现了85 059个已知病毒：www.ipa.go.jp/security/english/virus/press/200401/virus200401-e.html

20 计算机犯罪研究中心于2004年1月9日发表的Vladimir Gobulev的“计算机犯罪结构”：www.crime-research.org/articles/Golubev1203/

II.1.11 为应对网络犯罪威胁做好准备：保护的责任

对于随时可能产生的网络犯罪的威胁，人们必须做好准备。

保护和守卫各机构的资产需要按部就班，严密组织。在确定安全战略时应考虑到犯罪的风险。尽管辨别网络犯罪分子困难重重，对其行动方式和动机又不甚了解，但人们已认识到，犯罪组织通常随机行事，总是将目标对准最薄弱环节。各机构可以采取措施避免成为网络犯罪的目标，确保自己的计算机系统得到更好的保护，而不是自满于在不安全性方面与竞争对手旗鼓相当。因此，网络犯罪风险已成为能否保证高水平安全性的杠杆。

相反，被犯罪分子视为有利可图的潜在受害者或重要摧毁目标的机构无疑将成为攻击的靶子。在第二种情况中，恐怖分子行为造成的破坏威胁已经变为现实。因此有必要制定适当的保护和防御战略。然而，传统的保险和风险管理手段在处理犯罪风险上不够有效，因为唯一可避免一些风险的手段就是避免上网。

犯罪风险具有全球性并影响到各个层面的组织机构（股东、企业管理者、员工和生产设施等）。因此，面对犯罪风险，他们应像面对腐败一样，学习如何保持自身的廉洁正直。企业必须保持盈利，由此补偿由网络犯罪风险和为管理这些风险而采取措施所造成的机会成本。必须设计一个经济模型，在那些与企业分享财富者的帮助下，寻求保证保护基础设施并为系统、网络、数据和业务提供安全的资金来源的最佳途径。

数字世界的脆弱以及无法实现的全面控制（不仅是 IT 和电信技术及基础设施，同时包括商业安全解决方案）无疑使人们对人类无法控制的技术的依赖性提出根本质疑。

我们在多大程度上愿意依赖于一个提供商、一个国家或一个管理人员？

控制网络犯罪风险的首要步骤是：

- 审查与新技术及提供商之间的关系；
- 要求安全保障；
- 将所有参与方的责任制度化。

在防范－保护－防御的基础上落实常规安全措施之前，我们必须首先通过研究有关机构的敏感和关键资源与新技术之间的关系，来寻求保护方式。

我们必须要求：

- 具有可管理和可核实安全水平的高品质产品；
- 安全性应透明，而不是像过去一样隐藏于背后；
- 安全不仅是用户的责任，也是技术利益攸关方的责任（软件设计者、接入提供者等专业人员的法律责任）；
- 技术解决方案中应内置最低水平的安全性（安全产品）。

除在组织层面上的关注外，面对有组织的犯罪、经济犯罪和网络犯罪的结合和融合，必须在多边和国际层面上做出全面响应，以便加强经济领域各参与方对信息技术的信心，从而降低犯罪机率。

这种响应必须符合国家安全和组织机构及个人安全的需要。它应有助于将网络犯罪控制在可接受的水平内，增强人们对数字世界的信心，并在最大程度上降低腐败风险以及对公共管理机构的威胁。

第 II.2 节 – 网络攻击

II.2.1 网络攻击类型

互联网技术提供的可能性可被广为利用。通常，利用的方式包括获取合法用户的连接方式和密码，采用骗取手段并利用技术的缺陷和薄弱环节。

II.2.2 为进入系统盗窃用户密码

为接入系统而获取合法用户连接参数的主要方式包括：

- 猜测：密码显而易见（用户、配偶或子女的姓名和生日等），使账户无法受到根本保护。
- 骗取（社交工程）：攻击者以处理技术问题为幌子，冒充管理人员询问密码。令人惊奇的是，多数用户会披露其数据。
- 监听流量：攻击者对采用通信协议在网上传送的未加密数据进行截取或监听（嗅探和监测）。
- 软件：将“特洛伊木马”渗入用户工作站，秘密记录用来连接远端系统的参数。
- 访问密码存储文件。
- 破解用加密形式传送的密码。
- 通过激活多媒体外围设备对用户进行暗中监视，以便记录其连接参数。

一旦掌握进入系统所必须的接入密钥（用户名加密码），潜入系统并进行各类读写操作则易如反掌。黑客面临的挑战是不被发现，同时不在访问过的系统中留下任何蛛丝马迹。

II.2.3 拒绝服务攻击

拒绝服务攻击的典型做法是使系统容量超载。目标系统在远远超过其可应对的大量请求冲击下陷于瘫痪，无法继续工作。利用操作系统的缺陷以及一些系统功能，例如，缓冲管理（缓冲超流量攻击）可以进行这些攻击，造成严重功能障碍，致使系统关闭。

电子邮件轰炸，即用洪水般的信息冲击用户收件箱，就是一种拒绝服务攻击。

II.2.4 刷新攻击

刷新攻击是使用一个网页替换受害者的网页。新网页的内容（如色情和政治性）取决于黑客的动机。这类攻击的一种形式是将用户引向看似与其正在访问的网站完全相同的假网站。在此网站中，用户被要求披露其信用卡等信息。网络钓鱼攻击就是这种作法。

网站内容也可能为了篡改信息而被刷新（以便影响事件，增加不确定因素，控制公众舆论等）。这些语义上的攻击目的在于篡改信息内容的含义。这类攻击属于信息战。

II.2.5 欺骗攻击

所有 TCP/IP（传输控制协议/互联网协议）协议均可受到破坏并用来危及系统安全。通过网络传输数据的协议和机制同样面临风险。因此，在客户机到服务器的工作过程中可以截获 TCP 会话。

TCP 的作用在于，在两个通信者之间建立逻辑连接，并对二者之间的应用数据交流予以支持。为连接分布式应用，TCP 使用端口编号（应用的逻辑标识）。一些为某些程序预留的编号是固定的，用户非常熟悉；而其它编号是根据具体算法在连接过程中动态分配的。TCP 端口编号攻击是对数据交流分配到的下一个端口编号进行猜测或预测，以便在合法用户所在地加以使用，从而有效予以截持。这样就可以通过防火墙并在两个实体（黑客和目标）之间建立一个“安全的”连接。与此同时，远端合法用户访问设施自然会受到阻挠。但是向其发送一条信息，说明被申请的系统处于未激活状态就可轻而易举地蒙混过关。

用户数据报协议（UDP）是一个 4 层（传输）无连接协议。它替代 TCP 用于少量数据的高速传送。UDP 通信不受任何机制控制，因而未经过身份、流向或差错检查。因此，为潜入系统，任何人均可以使用授权系统用户的 IP 地址。UDP 会话盗窃可以在不引起应用服务器警觉的情况下发生。

由于各种协议的运行均为公共信息，因此比较容易被滥用来生成虚假数据包，从而在拒绝服务攻击中冲击网络。由此可以看出，为确保网络和服务的可用性，安全性必不可少。

黑客利用协议及其局限性：

- 致使网络瘫痪；
- 将 IP 数据包引向错误目的地（例如黑客的目的地）；
- 用洪水般垃圾邮件致使系统超载；
- 阻止发送者传送数据；
- 控制数据包传输过程，阻止网络流量的流通并降低网络性能（可靠性和可依赖性等）。

一般来说，路由攻击是通过提供错误地址信息误导数据造成路由、网关和地址的混淆。

通过使用一些可选择的用来规定路由的 IP 功能，即确定数据包必须经过的中介系统的地址并篡改这些地址，攻击者可以轻轻松松地将数据包引向他们选择的目的地。

攻击者不仅知道如何利用通信协议的操作功能，而且还会利用各种操作系统的特性及运行方式。因此，让一些缓冲器（缓冲超载攻击）超载，可以致使功能受到严重破坏或造成系统瘫痪。这类攻击的目标当然是那些在数据传送或在姓名及地址的管理中提供重要服务的系统（例如路由器或域名服务器）。网站上多数攻击旨在利用操作系统的缺陷致使系统关闭。

II.2.6 针对关键基础设施的攻击

随着互联网技术的深入使用，社会中必不可少的基础设施（供电、供水、交通、食品物流、电信、银行和金融、医疗服务和政府职能等）变得愈发不堪一击，通过“网中网”便可潜入其中。

尤其需要强调的是，发电和配电系统非常容易受到攻击。这些系统关乎国家多数基础设施的运行，因而至关重要。各类关键性基础设施之间关系的复杂性和分布特征既能使其保持强大，同时也是薄弱环节的发源地。

保证用来操作这些基础设施的网络之间的网关及互联网的安全至关重要。应建立区域性或国家机构，监督对关键性基础设施的保护。这些机构的首要任务应是为保护各项基础设施而协调规划制定以及规划的更新和充实工作。在若干基础设施同时受到攻击的紧急情况下，协调一致的计划和安全解决方案必不可少。

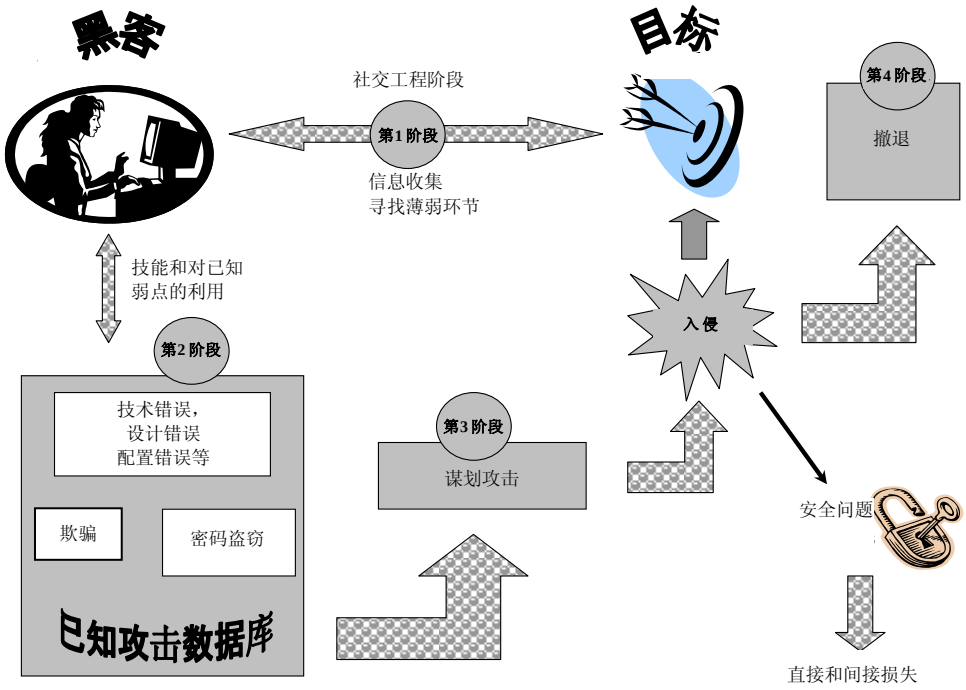
II.2.7 网络攻击的不同阶段

图 II.6 所示为网络攻击[21]的不同阶段。

第一阶段的目的在于收集目标系统的信息并探究潜在的薄弱环节，以便为日后加以利用争取最多的信息。这涉及研究身份识别、认证、访问控制、加密和监测使用的机制和安全水平，同时在相关环境中找出技术、组织和人员方面的弱点。攻击者通常诱使那些天真或容易轻信他人的用户，透露可用来设计攻击的信息（这就是所谓社交工程）。

21 该图源自S. Ghernaouti-Hélie著的《信息安全与通信：正确的途径与方法》（*Sécurité informatique et télécoms: cours et exercices corrigés*）（Dunod 2006年）。

图 II.6 – 网络攻击的典型阶段



黑客还会寻找和利用已知的－但尚未修复的（打补丁的）－安全漏洞，利用目前可利用的手段（攻击数据库、攻击工具包）渗入系统。撤退阶段旨在掩盖攻击踪迹并确保遗留的踪迹不会使黑客暴露身份。黑客通过使用化名而非法占用合法用户身份，或利用多个中间（接力）系统，掩盖痕迹，增强其匿名性。

第三部分

技术途径

第 III.1节 – 电信基础设施

III.1.1 特点

电话网的地理覆盖范围广泛，是为众多用户提供服务的主要网络。如今，电话网络基础设施不仅可以传输语音，而且能够传输数据，因此只要具备接口，即可通过电话网将计算机连接在一起。近年来，随着互联网网络接入点的普及，网吧数量不断增加。与此同时，越来越多的国家在建设和使用容量更大、接入更为便利的传输基础设施。某些国家亦在部署有线网络，以便进行电视传输。

除固定电信基础设施外，还存在方便用户移动的“无线”基础设施。无线技术包括卫星和空间基础设施以及地面无线电系统。近年来，移动电话已成为诸多发展中国家为公众提供服务的手段。

在全球若干大陆，“全球通”（全球移动通信系统（GSM））已成为传输话音和少量数据的明确标准。然而，新一代的、采用全球移动电信系统（UMTS）标准的、且传输能力更强的移动网络，才是真正为更广泛使用移动多媒体手机铺平道路的网络。尽管如此，全球通网络依然在发展进步，并已具备 GPRS（通用分组无线电业务）功能，通过更高的传输速率满足人们对移动数据应用的需求。

迅速风靡世界的全球通等技术不仅反映了技术的变革，而且反映了经济的变革和人们的行为的变化。在全球通信市场的激烈竞争中，移动通信蓬勃发展。由此我们看到无线电话进入了此前由运营商独断专营的电信市场，同时这也意味着基础设施可被重复用于各种各样的数据传输。

发展中国家无论采取何种技术部署电子服务，其电信基础设施均应当能够：

– 在全面保证质量和最佳安全性的框架内（可以极低的技术和经济成本实现可持续的、稳定的和逐步增加的业务和产品），实现易于建立和维护并满足覆盖要求（国家和国际覆盖）的、一套定义明确的基本业务之间的标准化数字互通（语音、数据、图像）；

– 保障技术和商业的和谐发展 – 避免卡特尔的组成，实现基础设施和业务的和谐发展，确保对主宰运营商的不良行为主动予以监管。

III.1.2 基本原则

电信网络由一套相互配合的信息和传输资源构成，旨在提供通信服务。通过这些服务，人们可以远程获取和共享互连一起的信息资源、实现应用的互连和人员之间的沟通、并远程执行程序和传送信息。

当前，高效的通信基础设施是开展各项经济活动的关键。通信基础设施将各种设备、应用和人员连接一起，使他们无论身居何处、相距多么遥远、所传输的信息类型多么不同，均能够共同工作。

人们首先通过若干标准对网络加以区分，其中包括地理覆盖范围、网络拓扑[22]、采用的技术、支持的应用、操作模式、传输媒介（有线/无线）及专用和公众网络性质等。

最初出现的网络是广域网[23]（电话、用户电报、分组数据交换（Transpac）、互联网等）。随着个人计算机（PC）在80年代的出现，我们看到了局域网的诞生[24]。

近年来，上述网络相互互连，其区分日渐模糊。例如，局域网（LAN）可以与其它局域网相连，进而形成一个更大的网络。此外，网络不再是专门支持某一类应用的网络，语音、数据和视频图像均可通过网络传送（多媒体网络）。

网络分为公众网和属于某一组织、并由该组织拥有专用权的专用网。公众网系指运营商根据具体签订的订购协议，向个人或机构提供电信服务。

广域网的主要传输技术为TCP/IP、帧中继和ATM（异步转移模式）。企业局域网采用的主要传输技术为以太网及形式有所改变的高速以太网（高速以太网、交换以太网）。

在电信领域，光传输和ATM交换技术极大地推动了传输基础设施和网络的发展。通过这些技术，人们实现了高速优质传输、动态带宽分配、灵活可变的速率和多重应用。

III.1.3 网络成份

III.1.3.1 互连媒介

我们需要通过传输媒介将计算机互连成网。这既可以是物理媒介（对绞线、同轴电缆、光纤），也可以是无形媒介（无线电、红外波）。各种媒介的自身特点决定了它们以不同速度传输各种数量信息的可靠性和容量。

互连媒介的传输或容量即是在给定时间内传送的信息数量，表示单位为每秒千（kilo）、兆（mega）或兆兆（tera）比特（例如，100 Mbit/s）。数量与传输媒介的带宽成正比，后者与一个信号无变化地通过媒介的一组频率相对应。

---

22 网络拓扑是将不同网元和节点连接一起的链路图形。

23 广域网（WAN）是将分布在相对较大地理范围（大于100公里）甚至世界范围内的计算机连接一起的网络。

24 网络将处于几公里内的、较小地理范围（约为十公里）的计算机连接一起时称为局域网（LAN）。城域网（MAN）是将属于不同实体的局域网互接一起的网络，地理覆盖范围最高为100公里。目前正在发明用以表述不同类型联网资源或描述具体应用领域的新术语。例如，在专业文献中我们可以看到下列首字母缩略语：HAN（宅域网）–将家中可以遥控的设备（烤箱、录像机、照明和供暖设备等）连接一起的网络；CAN（车域网）；SAN（储域网）等。

III.1.3.2 连接成份

用于连接传输媒介和计算机的连接类型或连接成份取决于媒介类型和传输模式。连接箱或网络接口对由计算机传送或接收的信号加以调整，使其成为能够在媒介上进行传送的信号，从而解决连接性问题。例如，调制解调器（调制器/解调器）提供处理数字信号的数字机器，即计算机和连续传送信号传输媒介（如模拟电话线路）之间的接口[25]。理论上而言，只要电子成分具备适当的硬件和软件连接接口，即可以与网络相连。

III.1.3.3 专业设备和数据服务器

除提供网络接入的用户系统和专用于管理及处理应用的计算机（数据主机和服务器）外，网络传输基础设施亦需要通信处理器。这些处理器事实上是完成管理和建立通信所需的一种或多种功能（资源优化和共享、数据路由、地址和域名管理以及互连等）的计算机。处理器包括路由器、多路复用器、连接器、交换机或互连网关。

必须首先按照通信双方满意的交换协议可靠传送信息后才能够进行通信。应当指出，人们假设由电信网互连一起的系统各不相同。为了在系统间进行对话，系统必须使用相同的通信基准结构，换言之，它们之间必须采用相同的语言并遵循共同的交换规则。

这很像持不同的母语两人之间交流信息，他们首先需要就使用的语言达成一致。其中一方可能会努力使用另一方的语言，或者他们之间可以共同使用一种第三方语言。

如果此后有第三、第四、第五和更多的人加入谈话，而且这些人讲其它语言，则很难为每一对交谈双方进行语言翻译，因为如若如此，他们之间的交流定会十分困难。在此情况下，谈话各方最好能够采用同一种语言。

同样，联网计算机必须遵守相同的通信协议和对话规则，才能够相互通信。这些协议已纳入通信软件之中，主要目的是确保数据在正确的路由上传送，保障远程应用和系统之间的互通。

国际标准或既成事实的标准由全行业认可的机构加以确定。国际标准化组织（ISO）和国际电信联盟（ITU）是为业界提出有关国际标准（例如X.400系列标准）建议的国际标准制定组织。

既成事实的标准虽然并未由上述机构通过，但却在市场上被广泛应用，因此此类标准已成为一种基准，即既成事实的标准。例如，所有由互联网界制定的协议均是既成事实标准。

---

[25] 为在媒介上传输计算机输出的信息，必须对信息进行调制。以模拟形式传送的信息须在接收端得到解调并以数字形式呈现予目的地计算机。调制解调器对计算机发送和接收的信息进行调制和解调。

上述标准特别定义通信协议提供的业务类型并具体规定如何建立协议，从而设计出相互间能够进行通信的数据解决方案。因此，通过在不同机器（异质环境）之间使用同类型协议，机器之间便能够相互通信。互联网上所有机器协议的综合协调是互联网实现普遍性的根本保障。

III.1.4 电信基础设施和信息高速公路

电信基础设施系指能够建立通信业务的所有传输媒介，我们又将此分为传输信道和路由技术与提供给客户的电信解决方案和服务两个方面。人们无须拥有某一基础设施即可将其作为提供具体应用的传输设施。

随着多媒体设备和高性能通信基础设施的出现以及音视频、信息技术和通信的融合，亦出现了完全数字化信息链的概念：在传输基础设施和内容层面，所有来源和用户信息均连续以数字形式出现。

信息高速公路的概念系指通过高性能通信基础设施，广泛提供有助于改善人们生活的公共或商业服务（如卫生、教育、文化、土地规划、行政管理或媒体）。互联网提供的某些服务的性质决定了前者亦可被视为是一种信息高速公路。

III.1.5 互联网

III.1.5.1 总体特点

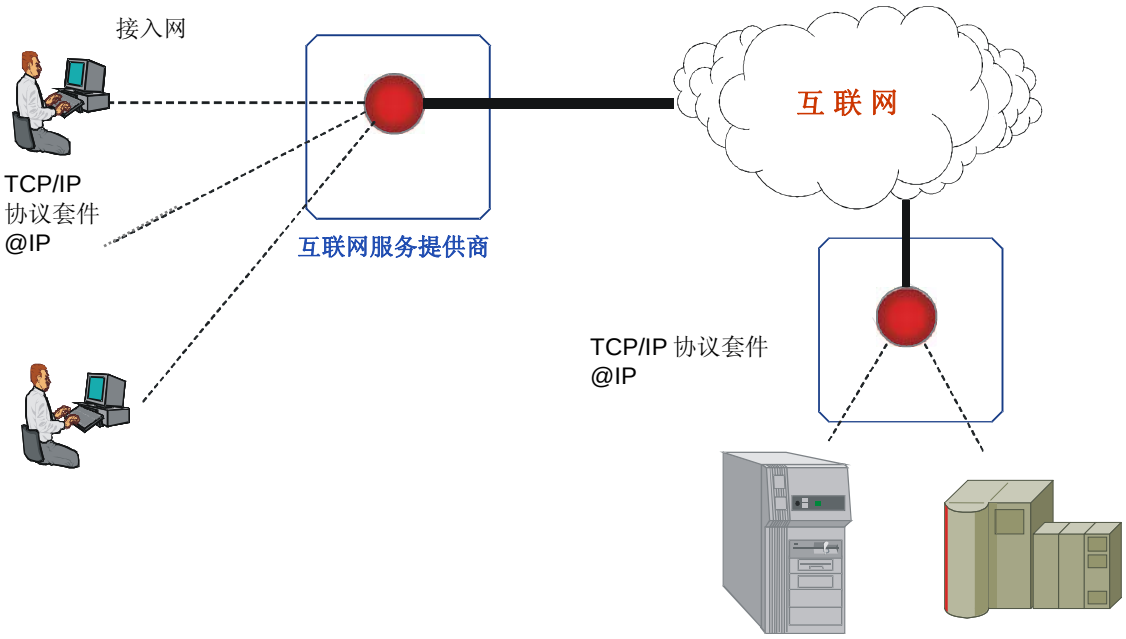
互联网发源于美国。之后，相邻的信息系统和计算机网络均被连接一起，互联网日渐普及。如今，该网络仍在发展，并决定了互联网是网络之网的性质。互联网上端到端之间的各种基础设施相互独立，由不同组织拥有，因此无法对其进行统一监控。

从硬件角度讲，互联网同通信网络一样，由信息系统、连接部件和传输媒介构成。信息系统包括用于访问网络和实现最终用户之间对话的系统（个人计算机、移动电话、寻呼机、个人数字助理等），支持各种应用的系统（网络服务器、数据库服务器等）和专用于网络数据处理的系统（路由器、互连网关等）。

数据通过实际上被连接一起的传输媒介在计算机之间进行交换。当通过移动系统（例如移动电话）接入互联网基础设施时，互联网络即为移动互联网。

分布在不同地方的信息程序和用户之间的数据传送、路由和通信通过TCP/IP系列通信协议实现[26]。互联网的此类标准化交换软件构成了实现不同类型系统之间互操作性的通信接口。计算机在互联网环境中进行通信时，必须具有上述通信协议并拥有为其确定独特身份的IP地址（见图III.1）。

图 III.1 – 通过服务提供商（ISP）、TCP/IP 协议套件和 IP 地址接入互联网

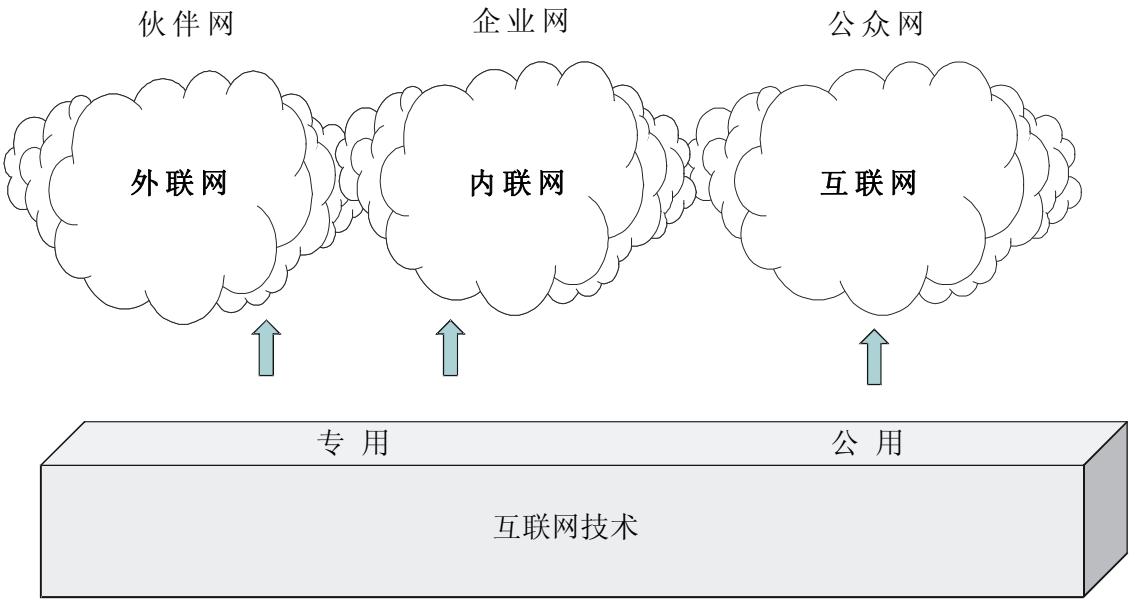


互联网在通信时将全部通信基础设施提供给公众。当某一组织希望仅在其内部专门使用该基础设施时，则需要建立虚拟专用网（VPN）。从满足内部需求的角度而言，相关组织还可以采用互联网技术建立专用网或内联网。向某些合作伙伴（客户、供应商等）开放的内联网被称作外联网（见图III.2）。

万维网（web）与电子邮件一道构成互联网的最为重要的应用。目前已开发出多种网络导航业务。通过安装在用户工作站上的客户机软件 – 浏览器，人们可以远程访问网络服务器。人们还可以利用浏览器搜索、查询或传送信息，甚至运行程序。网上浏览或冲浪得以实行是因为通过网络应用获得的文件为超级文本文件。换言之，文件的设计、结构和格式均适合以非顺序方式、利用创建文件时加入的标签和链接进行识读。读者激活某一链路时，即会被引向文件的另一部分或另一份不同的文件（可能储存于远端计算机）。用户通过激活超级链路实现在各站址之间的冲浪和访问。

[26] TCP/IP：传输控制协议/互联网协议。

图 III.2 – 互联网 – 内联网 – 外联网



III.1.5.2 IP地址和域名

被称作互联网服务提供商（ISP）的专业企业负责管理和控制互联网接入点。每一个ISP本身通过永久电信线路与互联网连接，ISP与其不同客户共享电信线路。ISP除提供上述基本服务外，通常还提供电子邮件管理服务和客户网站托管服务。

在互联网上进行通信时需要提供互联网地址（IP地址），这是一个清晰确定在互联网上进行通信的每一台机器身份的32位二进制序列[27]。

IP 地址以十进制形式表示，包括四个由句号隔开的十进制数。例如，128.10.2.30 这一地址对应的二进制数值为 10000000.00001010.00000010.00011110。由于人们无法牢记此类序列（即便是十进制数），因此往往采用域名（助记式）或逻辑地址来标明互联网环境中各相关资源的身份。这些 IP 地址及相应域名由被称为域名服务器 – 实际生活中使用其首字母缩略形式 – DNS（域名服务器）的电子目录存储和管理。

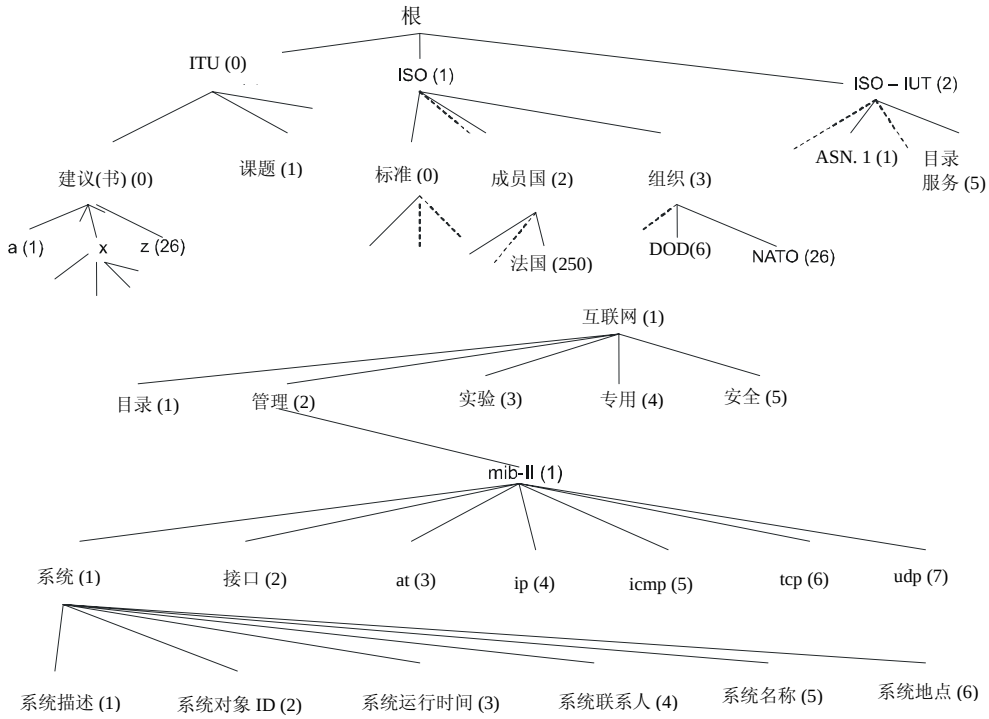
在开放环境中进行通信时，需要在特定域名中分配独一无二的识别符。参与通信的各方必须能够得到识别（地址、系统、应用程序、实体、管理对象等），用于建立通信的实施工具（协议）亦必须得到识别。为了确保全球范围内域名的独特性，目前已制定出一套在相关管理机构登记域名的程序，管理机构负责为每一个将被识别的对象分配一个明确和独一无二的识别符。

[27] IP地址是独一无二的地址，可以得到永久性（静态IP地址）或非永久性（动态IP地址）分配。

国际标准化组织的9834标准具体规定负责注册的管理机构并将其组织为分层的树状结构。树根包括三个分支，分别代表国际电联（ITU）、国际标准化组织（ISO）和国际标准化组织–国际电联联合委员会这三个泾渭分明的首层节点组织。这些是国际注册管理机构。国际标准化组织授权的下一层注册机构特别负责：

- 国际标准化组织的各种标准（0 标准）；
- 国际标准化组织成员（成员机构 2），其中我们可以看到 AFNOR（208）和 ANSI（310）；
- 组织（组织（3）），在此我们可以看到美国国防部（DOD）(6)（见图 III.3）。

图 III.3 – 注册管理机构及其树状结构



通用互联网域名在该逻辑注册结构中得到注册。在此树状注册结构中最有意义的是被称作顶级域名（TLD）的最高级域名根节点。此类域名主要用于识别由两个字母标明的国家（fr、it、uk、ch、nl、de等），以及包括下列在内的职能域名：

- .com　　商业组织；
- .edu　　北美学术机构；
- .org　　组织、机构或其它；
- .gov　　美国政府；
- .mil　　美国军事组织；
- .net　　网络运营商；
- .int　　国际实体；
- .biz　　企业；
- .info　　各种应用；
- .name　　个人；

- .museum　对收藏品进行储存分类，以便对其加以保护并向公众展出的机构；
- .aero　空运行业；
- .coop　合作社；
- .pro　各种专业。

在这些广泛的域名名称中，存在与大公司或重要机构相对应的次域名。

互联网域名分配管理机构（IANA）[28]—互联网域名和号码分配机构（ICANN）[29]中的一个部门，负责域名和地址的分配工作，并确保所有域名和地址均独一无二。可以将域名管理工作下放给低一级的一个机构。

注册域名时需要在域名目录中加入条目，相当于在由经授权的组织管理的注册树中创建一个新的弧形枝。目前世界上存在若干此类机构，最明显的是负责.biz、.com、.info、name、.net、.org等域名的注册机构。

ICANN在法国核准的注册机构（经核准的注册管理目录）是AFNIC[30]。

目前，人们委托在美国领土上，且按照美国法律进行运作的一家美国协会负责互联网地址的分配和管理工作[31]。因此，该协会掌管着互联网的接入权。这种做法的问题是，有关组织和国家均需依附于一家有责任向世界其它地方开放的外国超级机构，而参加其中的非美国代表却十分有限。

依赖于互联网可接入性的可用性（基础设施、服务、数据）安全标准无法由相关组织掌控或管理。相关组织访问互联网时，取决于所得到的 IP 地址和域名情况，因此外部实体掌握了他们对互联网的访问权。

域名目录可被视作由DNS（域名服务器）管理的数据库。ICANN负责协调约十五台DNS根服务器，其中多数位于北美。他们负责管理顶级域名和IP地址，包括上述所有域名（.org、.com等）以及不同国家的244个域名（.cn – 中国、.ga – 加蓬、.lk – 斯里兰卡、.pf – 法属波利尼西亚等）。被称作解析器的本地DNS服务器保存一份根服务器中储存的信息。解析器往往与战略网络接入点相关，或与互联网服务提供商相连，旨在回答用户有关将域名转换为IP地址的问题（见图III.4）[32]。

---

28 http://www.icann.org/index.html

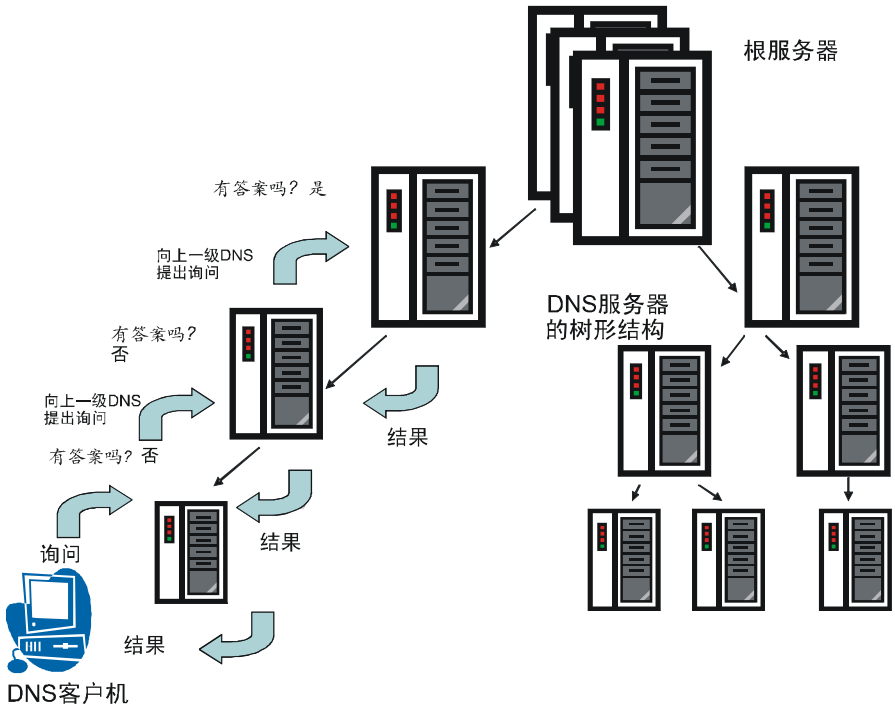
29 http://www.iana.org/

30 http://www.afnic.fr

31 ICANN认为：“互联网域名和号码分配机构（ICANN）是一家国际性非盈利机构，负责分配互联网协议（IP）地址空间、协议识别符、通用（gTLD）和国家代码（ccTLD）顶级域名系统管理和根服务器系统管理工作。这些服务最初由互联网域名分配管理机构（IANA）和其它实体按照与美国政府签订的合同加以提供。目前ICANN行使IANA的职能。”

32 该图源自《信息安全与通信：正确的途径与方法》；（*Sécurité informatique et télécoms: cours et exercices corrigés*）Dunod 2006年出版。

图 III.4 – DNS 服务器的树形结构



应当通过可用性、完整性、可靠性和安全性来确定域名和地址管理所涉及的地址、程序和系统的特点，这一点至关重要。负责传输基础设施的实体有责任保护并有效管理其通信环境。

III.1.5.3 IPv4协议

互联网问世之际出现的第4版本互联网协议（IPv4）[33]目前仍被广泛使用。该协议的作用是将有待传送的数据进行封装，以便建立经互联网传送至其目的地的IP分组数据包。每一个数据包在包含其它信息的同时，亦包含发送系统的源IP地址和目的地系统的IP地址。

在对数据包地址和路由器路由算法进行转译之后，通过将数据传送至所经过的每一个中间系统（路由器）而实现其路由。

IPv4 未包含任何保证安全服务的功能或机制。在 IPv4 中，人们无法对数据包的来源和目的地做出认证，亦无法保证两个实体之间传送信息时数据或 IP 地址的机密性。此外，由于该协议采用无连接模式，因此无法保证：

– 数据的交付（可能造成数据丢失）；
– 将数据交付至应收方手中；
– 数据顺序正确。

33 IPv4: RFC 0791 –www.ietf.org/rfc/rfc0791.txt IPv4及主要TCP/IP协议：
TCP: RFC 0793 – www.ietf.org/rfc/rfc0793.txt – UDP: RFC 0768 – www.ietf.org/rfc/rfc0768.txt – FTP: RFC 0959 – www.ietf.org/rfc/rfc0959.txt – HTTP 版本 1.1: RFC 2616 – www.ietf.org/rfc/rfc2616.txt – 电信网: RFC 0854 – www.ietf.org/rfc/rfc0854.txt

IP 协议（开放系统互连（OSI）结构体系第 3 层）提供不可靠的 IP 数据包交付服务，其操作模式为“尽力而为”模式，换言之，仅根据环境做出最大努力，不保证数据包的交付。事实上，该协议不保证任何服务质量，也不存在任何错后恢复。因此可能出现发送方或接收方不知情的数据包丢失、改变、复制、假冒或交付顺序混乱的情况。由于事先未建立发送方和接收方之间的逻辑关系，因此发送方在不通知接收方的情况下发送数据包，造成数据包丢失、路由改变或以错误顺序到达目的地的情况。

为克服这种缺少服务质量的缺点，在端点系统中安装传输控制协议（TCP），以便在面向连接的模式中（开放系统互连（OSI）结构体系第 4 层）提供可靠的传输服务。然而，TCP 协议却不提供真正意义上的安全性服务。

第 III.2 节 – 安全工具

保证信息、服务、系统和网络的安全需要确保资源的可用性、完整性和机密性，同时还需要保证某些行动的不可否认性以及事件或资源的真实性。

只有将安全措施用于我们确定是确切的数据和程序（数据和程序质量概念）时安全才具有意义，只有这样才能够实现数据和程序的稳定性（数据稳定性和服务连续性概念）。

主要安全性解决方案均使用加密或环境隔离技术、资源备份、事件监测、控制和管理程序以及系统维护、访问控制或管理等手段。

可以通过一系列障碍（保护措施）实现电信数据安全性，这将增加入侵方获得资源的难度。这些方法并未解决安全性问题，而是将安全性问题和责任转到了其它实体身上。安全性解决方案本身必须得到保护和保障才能够提供一定程度的安全性（安全的循环性）。

III.2.1 数据加密

使用加密技术可以保持数据的机密性、检查其完整性并对实体进行认证。

目前主要存在两种数据加密体系：对称（专用密钥）加密和非对称的公钥加密。

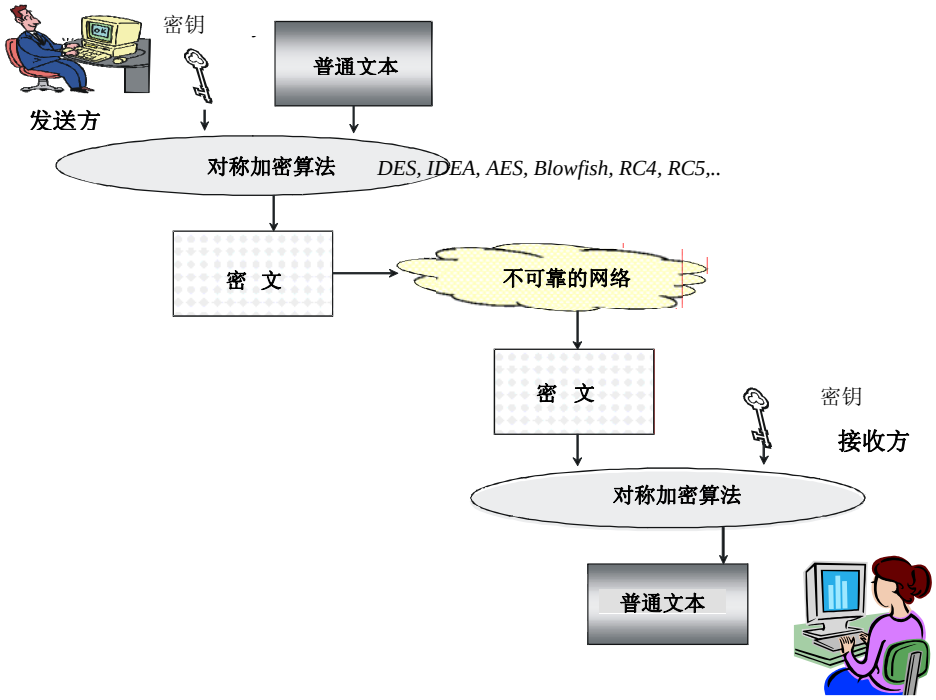
目前采用的加密算法各不相同。无论算法采用对称还是非对称模式，其根本在于对密钥的使用。总体而言，算法的强健性取决于安全管理加密密钥的能力、密钥的长度（密钥的最短长度由算法类别决定）、安装和运行加密算法的物理和软件平台的安全性。

III.2.1.1 对称加密

为了对文本进行加密或解密，我们需要一把密钥和一个加密算法。如果加密和解密采用同一把密钥，则该加密体系称作“对称”体系。发送方和接收方必须拥有和使用相同专用密钥来保持数据的保密性和对数据的理解。这就带来了有关如何对专用密钥分配进行管理的问题（见图 III.5）。

主要对称加密算法包括：DES、RC2、RC4、RC5、IDEA 和 AES。

图 III.5 – 对称加密



III.2.1.2 非对称或公钥加密

非对称加密体系的根本是使用一对独一无二的、相互匹配的密钥。该对密钥由一把公钥和一把专用密钥组成。只有公钥对所有人公开，专用密钥必须加以保密。

发送方利用接收方的公钥对信息进行加密，接收方则用其专用密钥对信息进行解密（见图 III.6）。

以公钥发明人命名的主要公钥加密算法通常使用长度为 512 至 1024 比特（有时为 2048 比特）的密钥，名称分别为：RSA[34]（代表 R. Rivest、A. Shamir、L. Adelman）、Diffie-Hellman[35]、El Gamal[36]。

III.2.1.3 加密密钥

加密密钥必须十分保密。用于加密的秘密密钥须得到秘密保管。

---

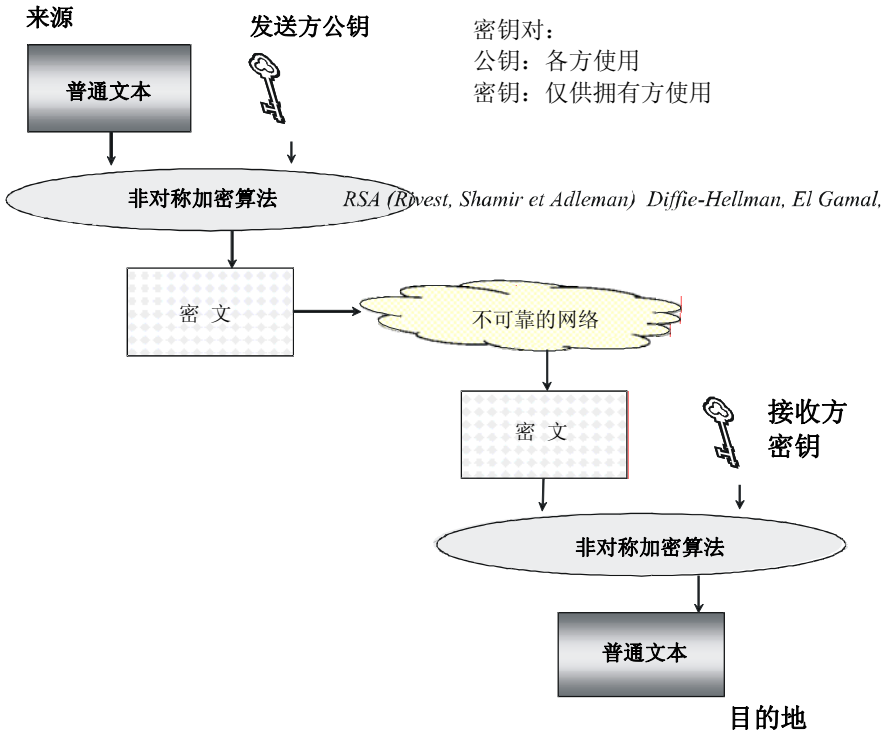
34 RSA：Schneier B著“应用加密法”，1996年，1996年第2版。

35 Diffie-Hellman: www.ietf.org/rfc/rfc2631.txt

36 El Gamal：Schneier B著“应用加密法”，1996年，1996年第2版。

如前所述，加密程序的安全性在很大程度上取决于所用密钥的机密性及其长度，算法的强健性以及下层硬件和软件平台的安全性。

图 III.6 – 非对称加密



III.2.1.4 密钥管理系统

公共密钥基础设施（PKI）用于实施非对称加密体系，支持的主要功能包括：

- 产生一对独一无二的密钥（专用密钥 + 公钥）、向实体分配密钥对、存储管理密钥所需的信息、对密钥进行存档、制定用户在丢失密钥时需追回密钥或管辖机构要求披露密钥时的程序；
- 管理数字证书并对证书予以建立、签署、颁发、核准、吊销和延期；
- 向得到授权的要求获得资源的有关方面分发公钥；
- 对公钥进行认证（数字证书签名）。

III.2.1.5 数字证书

数字证书是一个实体（法人或自然人）或信息资源 – 证书主体 – 的数字身份卡。除其它信息外，该卡包括主体（持有人）的身份、分配给主体的公钥和颁发机构的身份等信息。

X.509 标准（目录鉴权框架）按照数字证书的使用情况，提供建立认证业务所需的体系结构框架，并对数字证书的结构和格式予以规定。市场上诸多解决方案均采用这一标准化结构（见图 III.7）。

图 III.7 – X.509v3 数字证书的主要内容

版本
序号
签名算法
颁发机构名称 序号/颁发机构配对须独一无二
有效性
主体名称
主体公钥
有关主体或加密机制的其它信息
证书签名 签名算法、参数及实际签名

为了对收到的证书进行验证，客户必须得到证书颁发机构对应签名算法的公钥，并对签名进行解密。客户利用这一信息计算出散列值，并将其与证书最后字段中的数值进行比较。如果二者相符，则证书得到认证。之后客户可以确认证书的有效性准确无误。

通过采用以数字证书为基础的访问控制，可以在一台特定服务器上连接诸多用户。控制主要通过客户数字证书中包含的信息加以实施，因此服务器对证书的有效性和颁发方式确信无疑，这就造成了系统安全性方面的漏洞，因为认证服务器的数据可能遭到破坏，甚至可以制造假冒数字证书。此外，控制证书有效性并非轻而易举之事。吊销证书的工作极其艰巨，因为需要将信息传送至所有各方并在证书吊销清单（CRL）中对此加以登记。一旦证书内容出现变化则须立即吊销证书（例如，证书所含信息过时，用户专用密钥遭到破坏，用户已经离开公司等）。系统性查阅相应的数据库会降低访问控制的速度，或无法向用户，包括经授权的用户提供服务器。

III.2.1.6 值得信赖的第三方

无论采用何种名称 – 值得信赖的第三方（TTP）、注册管理机构、认证机构、或证书机构，建立公钥基础设施机构的主要职能在于颁发向实体分配的公钥使用证书凭证（身份证书）。

客户向认证管理机构（网上注册服务机构）提出注册申请（认证申请）。注册服务器可能根据该机构建立的身份识别和认证程序要求客户提供其身份证明。对信息进行核准后，认证服务器生成加密密钥，并以客户的名义制做数字证书，以自身的专用密钥签署证书（对数字证书进行认证）并将其发至客户。客户将使用该机构的公钥确认证书确由所述机构颁发。

认证管理机构是值得信赖的第三方，负责颁发数字证书并核准某些信息的有效性。

III.2.1.7 公钥基础设施的缺点和局限性

若干认证机构并存的情况带来了认证机构间相互认可、实现互操作、确保证书之间的兼容性及其有效范围的问题。尽管如此，亦无需只建立一家全球性认证机构，不然该机构拥有的既成事实的权力将过于广泛，过于巨大，同时需建立的基础设施规模将超出任何一家机构的能力。用户对此类总体上为外国性质的认证机构缺乏真正的信任（证书如何有效？安全如何保障？个人数据如何保护？等等）。

公钥基础设施固有的局限性表现在：

- 基础设施复杂，部署和管理基础设施的成本高昂；
- 建立 PKI 服务要求的安全水平极高；
- 证书的有效性、期限和终止等。

实施 PKI 服务可能存在的问题包括：

- 政治问题：大多数 PKI 基础设施 – 认证机构均属于美国实体，因此产生了针对这些实体提供的服务（专用密钥、公钥和识别数据的创建、存储和分发、公证）的绩效和对实体的信任问题，以及如何保障数据不被滥用、交换过程中保持中立和在与证书颁发机构出现争端时可使用哪些资源来解决争端等问题。
- 技术问题：传统加密体系可能瘫痪，某些数字证书不具备安全保障，可能出现盗用现象，同时基础设施的传统安全措施亦意味着易于遭到破坏。此外，采用密钥基础设施的方法仅仅是对交换安全性问题进行了转移，而非实际解决了这一问题。
- 组织问题：包括基础设施互操作性、部署、管理、维护、安全性和复杂性等问题。

III.2.1.8 签名与认证

数据发送方通过其专用密钥对信息进行加密。任何了解发送方公钥的实体均能够对信息进行解密，从而确认信息确是通过相应的专用密钥创建。

可以采用公钥加密算法以电子方式签署文件（数字签名），具体如下：

- 创建声明发送方身份的信息 – 签名（例如“我叫 Alpha Tango Charlie”），签名通过发送方专用密钥得到加密并附于将发送的信息之后；
- 接收方利用其公钥对信息及其签名进行加密并传送；
- 接收方用自身的专用密钥对信息进行解密并将利用发送方公钥解密的签名拆下。

但是，在此我们必须谨慎行事，因为我们没有任何手段可以防止某人冒充真正的发送方重新使用上述数字签名，同时在窃得伙伴的专用密钥之后，亦可以冒充伙伴创建数字签名。为了加强数字签名的安全性，签名需通过信息内容产生，从而确保信息的完整性和发送方的真实性。

III.2.1.9 数据完整性

通过附加信息摘要可以确认数据在传送过程中未被改变，摘要需与数据同时传送。在数据上使用散列函数即可产生摘要。接收方采用相同的函数重新计算所收到的数据的散列值。如果获得的数值不符，则可以推断得出数据已被修改的结论。文摘本身可以在数据传送或存储之前得到加密。

对称和非对称密钥加密体系均能够确定所传送的数据是否已被改变，因为改变后的数据无法得到解密。这有助于检查数据的完整性，但是却无法确认数据是否并未被彻底毁坏。

为了更有效地控制完整性，可以通过一种函数将最初信息改变为短的随意排列的比特流，从而构成一种数字指纹（摘要）。

一种所谓单向散列函数能够生成信息摘要，即，信息的数字指纹，它的长度短于最初信息，亦无法被人理解。之后利用发送方专用密钥对此进行加密并附于将发送的信息。接收方在收到信息及其指纹后，采用发送方公钥对指纹进行解密，用同样的散列函数重新计算信息的指纹，并将其与收到的指纹进行比较。如果结果相同，接收方即确认发送方的身份，并得到有关信息完整性的保障，因为如果信息被改变（哪怕仅仅是稍稍改变），其指纹将大为不同。

通过结合采用加密、签名和数字指纹技术标注信息，可以确保数据的完整性。这些程序耗费大量处理时间，会大大降低操作环境的性能。

III.2.1.10 不可否认性

不可否认性服务旨在确保已发出或接收到的信息、已采取的行动或发生的交易不被否认或拒绝。通过该服务可以证明某一实体与某一具体行动或事件相关联。

不可否认性以单一的签名或证明创建信息的人的身份为基础。可通过公钥加密算法提供这一服务。值得信赖的第三方也可发挥网络公证机构的作用。

III.2.1.11 以加密为基础的安全性解决方案的局限性

如果市场上出现的加密解决方案不提供保障或不具备核准手段（软件存在后门？保密密钥被复制或被泄漏等？），则只能得到人们的相对信任。同时，没有任何证据表明目前被认为可靠的算法未来会依然如此。

III.2.2 安全的IP协议

由于需要满足人们在安全性方面的要求，因此各方普遍赞成对第 4 版本互联网协议进行修订。此外，还需要提供更为广泛的地址，加大可提供的互联网地址的数量，并实现带宽的动态分配，以支持多媒体应用。因此，出现了被称作“下一代互联网协议”（IPnG）或第 6 版本 IP（IPv6）的、经修订的 IP 协议版本[37]。

III.2.2.1 IPv6协议

1994 年[38]，互联网活动委员会（IAB）[39]开始讨论有关 IP 协议的安全性要求问题。第 6 版本 IP 协议（IPv6）包括认证和保密功能。

与 IPv4 相比，IPv6 主要在下列方面有所改进[RFC 2460]：

- 地址空间扩大，地址层次增加：地址规模从 32 比特（4 个八位字节）增加至 128 比特（16 个八位字节）；地址由十六进制数[40]（每两个八位字节之间以冒号隔开，（例如 0123:4567:89ab:cdef:0123:4567:89ab:cdef）代替十进制点符号；
- 可以进行动态带宽分配，以支持多媒体应用；
- 具有创建虚拟 IP 网络的能力；
- 通过选项报头支持认证和加密程序；
- 包头（packet header）得到简化，方便并加快路由速度。

采用 IPv6 特别要求修改寻址和地址管理机制[41]、在整个互联网环境中安装支持 IPv6 的系统和能够采用两个版本协议的系统，并完成版本迁移的大量同步工作等。

由于上述诸项原因，于 1995 年确定的第 6 版本目前尚未得到广泛安装，同时无论是政府的激励机制还是国际有关机构的建议，似乎都无法强制有关方面在整个网络中采用第 6 版本协议。目前只有为数不多的专用基础设施采用了 IPv6。

具有内置安全性功能的新互联网协议（IPv6）并未得到普遍采用。因此，为了满足网络安全性方面的要求，目前互联网界采用了与 IPv6 和 IPv4 相兼容的称作“互联网协议安全（IPSec）”[42] 的过渡解决方案。互联网工程任务组（IETF）[43]于 1995 年公布了规范有关互联网基础设施安全方式的若干文件（RFC 1825 至 1829）。

---

37 IPv6：1995年的 RFC 1883由1998年12月的RFC2460取而代之 – www.ietf.org/rfc/rfc2460.txt

38 RFC 1636：IAB互联网架构安全性研讨会报告，1994年2月8-10日。

39 www.iab.org/

40 十六进制编号体系的字母（base 16）：0 1 2 3 4 5 6 7 8 9 A B C D E F

41 1995年出版的RFC 1886确定了为支持IPv6而需对DNS进行的修改。

42 RFC 2401 – www.ietf.org/rfc/rfc2401.txt

43 www.ietf.org

III.2.2.2 IPSec协议

通过采用 IPsec，由协议传送的数据包内容得到保密。IPSec 通过加入认证报头（AH）或封装安全有效载荷报头（ESP）在传送层面实现 IP 协议的数据机密性和认证服务。

无论应用产生的流量类型如何，均可在无须进行调整的前提下使用这些安全服务。IPsec 采用点对点模式（通过确保发送方和接收方之间的关系保障数据的安全性）。

认证报头提供 IP 数据包的认证和完整性服务，因此保障数据在传输过程中未被修改，并保证来源地址是在数据包上出现的地址。

封装安全有效载荷报头使得加密机制得以落实（诸如 DES、三重 DES、RC5 或 IDEA 的对称加密），并提供与认证报头类似的认证服务。

加密算法必须使用被生成和分发的密钥。在实施以 IPSec 为基础的解决方案过程中，加密密钥的管理是一项重要的任务。密钥交换协议包括 Oakley 密钥确定协议[44]（即基础为 Diffie-Hellman 的密钥交换算法[RFC 2412]）；互联网安全协会和密钥管理协议（ISAKMP）[RFC 2408]；互联网密钥交换（IKE）[RFC 2409]。

III.2.2.3 虚拟专用网

在互联网接入点处安装 IPSec，可以在这些点之间建立起其端点得到认证的通信信道（见图 III.8）。

这些端点位于组织的系统中，因此实际上得到了保护。根据所采用的有关方案，在连接线之间传送的数据可以得到加密。换言之，可以在并非可靠的基础设施的两个端点之间建立起安全的路由（虚拟专用网概念）。应当指出，“虚拟专用网”中所用的“网络”一词属用词不当，因为两者之间仅仅是建立起了（虚拟）逻辑连接。

III.2.3 应用安全性

大多数应用均具有安全版本，通常均能保证实现通信者之间的认证并对传送的数据进行加密。

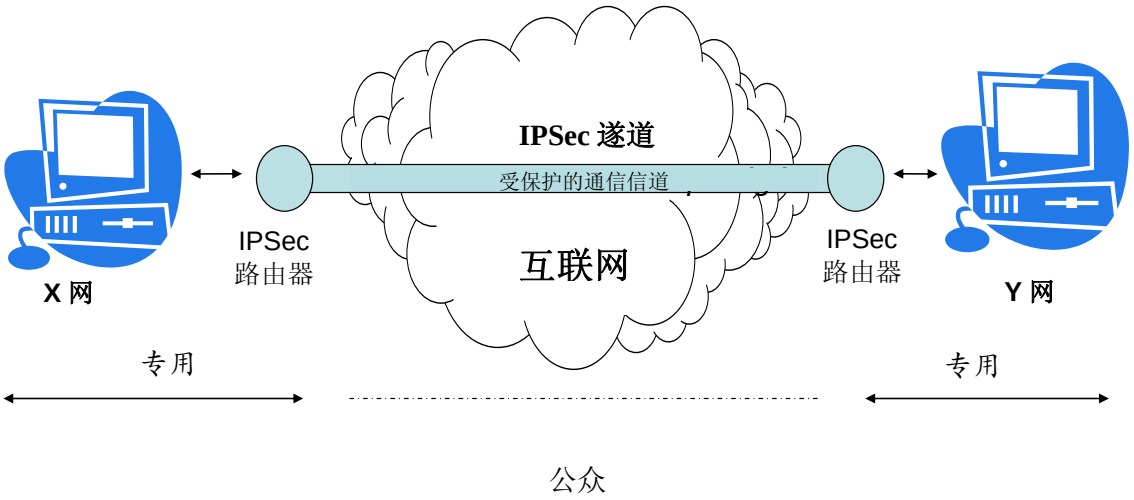
在安装新的应用协议安全版本以外还存在另一种方法，即建立为所有应用提供一般性安全服务的共同安全机制。安全套接层（SSL）软件目前已特别在通过互联网的商业交易中广为采用。

超级文本文件以及内容下载（无论是主动或被动下载）的广泛使用特别带来了有关下列方面的诸多安全性问题：来源、作者、真实性、有害性等等。目前正在出现一些旨在解决这一新的信息系统安全性问题的手段：在 XML 文件上进行签名的技术、水印、电子权的管理等等，从而实现稳定的安全性。即使需要得到安全保障的对象处于安全性得到管理的物理环境之外，也必须保持某种程度的安全性。

---

44 Oakley 密钥确定协议：RFC 2412 – www.ietf.org/rfc/rfc2412.txt

图 III.8 – 利用 IPSec 通信信道建立 VPN



III.2.4 安全套接层（SSL）和安全HTTP（S-HTTP）协议

安全套接层（SSL）是一种确保应用交换安全性的软件，市场上的大多数网络浏览器均支持这一软件。

SSL 连接中的两个通信实体通过认证程序和值得信赖的第三方得到认证，之后，双方商定数据传送将采用的安全级别。用于 SSL 通信的、被传送数据得到加密（见图 III.9）。

从服务器的角度而言，安装 SSL 的影响巨大，因为它的认证要求即意味着需要与经认可的证书颁发机构进行对话，并要求防火墙应用真正支持 SSL 的操作。某些情况下，人们认为认证要求阻碍这一解决方案的部署。

向 HTTP 协议（安全 HTTP 或 S-HTTP）进行扩展是商务网协会（CommerceNet）开发的一种替代解决方案。S-HTTP 提供的安全性功能与 SSL 相同，亦存在同样的认证方面的限制，但它仅支持 HTTP 数据流。该解决方案并未得到广泛采用。

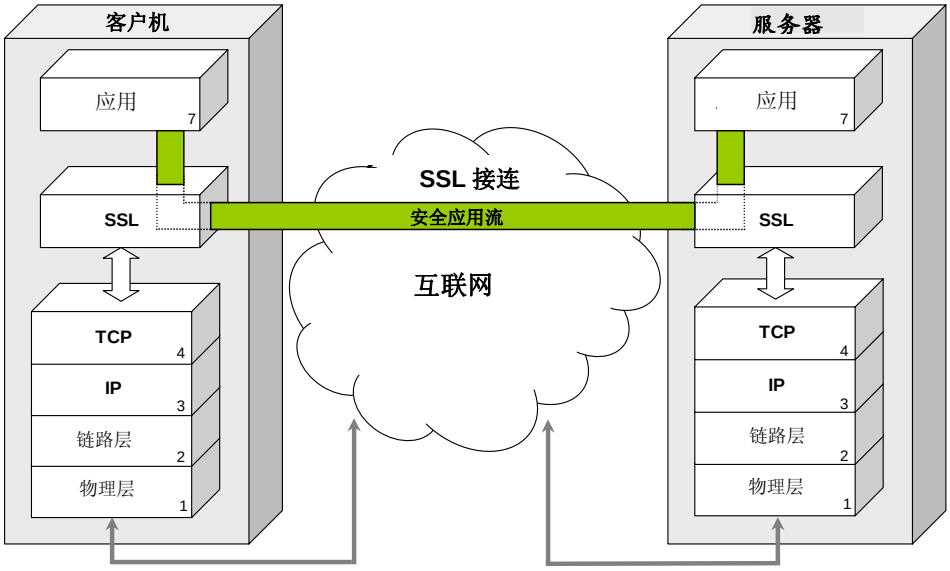
III.2.5 电子邮件和域名服务器安全性

使用电子邮件系统可能出现的安全风险包括：

- 信息丢失、被窃听、改变或破坏；
- 带有病毒、蠕虫或特洛伊木马的信息对系统造成感染；
- 骚扰：信息轰炸、垃圾邮件（junk mail）以及影响个人的垃圾邮件（spam）。后者系指在未得到收信方事先同意、且发送方（垃圾邮件制造者）从未与收信方取得联系的情况下，收信方的邮件地址被加以利用。垃圾邮件大规模散发受感染的信息，在电子邮件引擎内置于病毒代码从而进行自我扩散时，为病毒迅速（垃圾邮件 + 病毒）扩散推波助澜；

– 身份盗窃（入侵者假冒他人，系统上的某一设备发送、听取或截获并非发送给该系统设备的信息等等）；
– 插入、混合、删除或延误信息；
– 以信息系统相关部分出现故障为由拒绝服务；
– 泄露保密信息；
– 否认（参与系统的一方拒绝承认已发送或收到信息）。

图 III.9 – SSL（安全套接层协议）架构



此外，我们还需要将所有与网络及其操作有关的威胁（在路由、域名服务器等层面进行的攻击）考虑其中。

为消除电子邮件系统固有的此种安全局限性，新的软件版本纳入了加密功能，以确保被交换的信息和通信者之间的机密性、数据完整性和真实性。

电子邮件系统的安全要求包括：

– （一条信息或一系列信息）的机密性和完整性；
– 不可否认性（发送证据、接受证据、签名、信息认证）；
– 对电子邮件系统各方（用户、中间成分、信息内存和信息传送代理等）身份进行认证。

最大的风险来自于通过信息传播的病毒、蠕虫或特洛伊木马。为预防病毒传播，应当在每个系统上均安装反病毒软件，从而发现病毒并在可能的情况下防止病毒造成感染。反病毒软件只能发现设计软件时所针对的病毒，不能够预防新形式的病毒传染，因此需要耗费大量管理时间和精力来不断更新此类软件。

另一种可行的做法是建立隔离服务器，对所收到的每一条信息及其所有附件进行严格扫描。通过若干反病毒程序并举的措施，可以提高发现受感染的信息的概率。

用于在互联网上交换电子邮件的、被称为“简单邮件传送协议”（SMTP）的最初协议已经得到改善，可以支持多媒体信息内容，并提供安全机制。此类协议包括 S/MIME（安全/多用途互联网邮件扩展）、PEM（私密性增强邮件）和 PGP（较高私密性）。

所有互联网应用均直接或间接依赖域名服务器（DNS）系统的工作情况，该系统中的 DNS 服务器将逻辑域名与相应 IP 地址进行关联。DNS 服务器在确保信息路由正确方面发挥着关键作用，因此，此类服务器在通信体系架构中是特别敏感的装置，需要得到更多的保护。安全机制（访问控制、认证、登陆、备份、一致性、请求和应答加密等）的目的是防止存储于服务器的信息受到破坏，包括改变信息路径，使其背离最初的目的地、实施拒绝服务袭击（以泛滥成灾的虚假请求造成服务器过载或网络瘫痪）、建立伪造域名服务器，获得错误答复，从而导致传输错误或入侵者的进入。

III.2.6 发现入侵者

入侵、事件或非正常现象一经发生，即须立即得到发现、确认和严格处理，以便确保相关系统能够继续正常工作并持续得到保护。

事件是意料之外的事情。尽管大多数事件本身并不严重，但却可能带来严重后果。非正常现象是一种反常现象，可能导致信息系统运行反常并破坏现行的安全策略。意外（例如配置错误）和故意（有针对性地对信息系统实施袭击）所为是造成非正常现象的原因。入侵是袭击的最大特点，可以被视作是一种事件或非正常现象。

发现入侵者系指通过一系列做法和机制发现可能导致破坏安全策略的错误，并对入侵和袭击做出诊断（包括非正常现象和滥用的发现）[45]。

入侵发现系统（IDS）主要包括三个功能模块，即，数据收集、数据分析和入侵发现及响应模块。

III.2.7 环境隔离

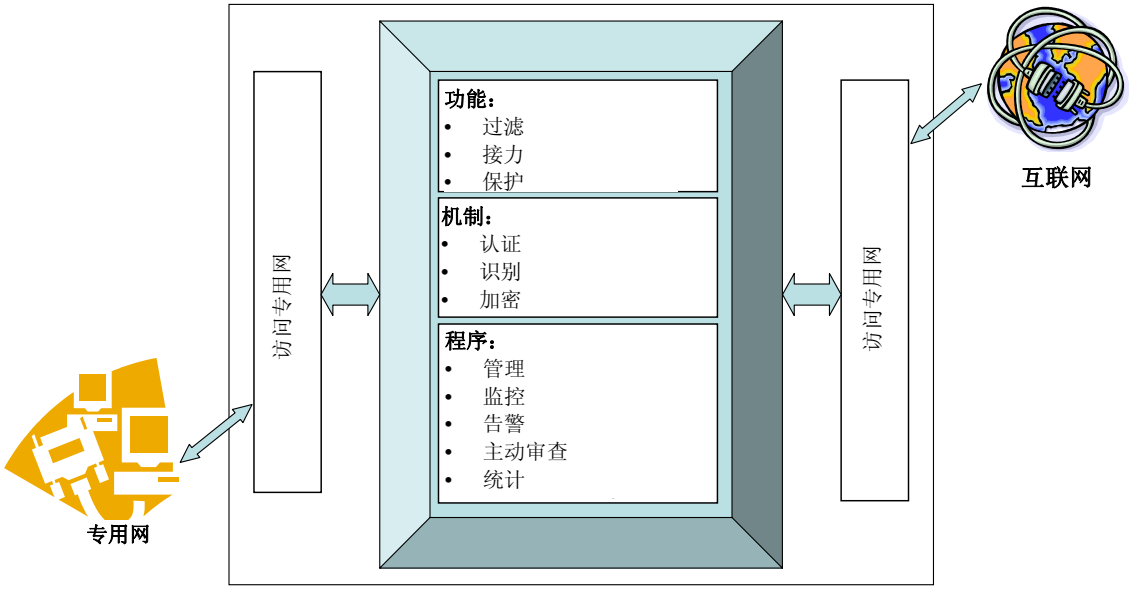
通过安装一个或多个防火墙系统，实现私人环境与公共互联网的隔离和保护。

---

[45] Alessandri及其他人著“为实现入侵发现系统和袭击的分类而努力”
www.domino.watson.ibm.com/library/cyberdig.nsf/papers/5FA980EB952E09D085256AC600535997/$File/rz3366.pdf

防火墙是一种对数据流进行过滤或阻断的系统。防火墙对数据流做出分析，在数据流符合某些条件时对其予以授权，不然则对其加以拒绝。通过对网络进行分区，人们可以创建单独的 IP 环境，即，网络接入点在物理上按照自己的意愿分离出来，相互间毫无关联。这一做法亦可实现具有不同安全等级的两个网络之间的互连（见图 III.10）[46]。

图 III.10 – 防火墙的功能结构



按照相关分析工作的性质和处理情况，可以采用不同类型的防火墙系统。通常防火墙系统按照数据过滤级别进行分类：OSI 模式的 3 层（IP）、4 层（TCP、UDP）或 7 层（FTP、HTTP 等）。

应用防火墙（亦被称作代理（代理服务器、代理防火墙））发挥应用接力的作用。此类防火墙代表用户工作，并建立所要求的服务。符合标准的代理系统的目的在于通过对应用进行接力而提供地址保护，并实现组织内部环境的透明化。该防火墙是所有要求访问互联网的应用的必经交叉点，并要求在用户工作站和防火墙上安装接力应用。

安装和配置防火墙应当以在连接不同系统时所选定的、满足相关安全性和控制要求的网络体系架构为基础。

防火墙是落实安全政策的工具之一，而且仅仅是落实安全策略所采用的硬件和软件设施中的一种设施，因为防火墙本身并不足以为组织的网络和系统提供足够的保护。必须同时按照安全策略确定的目标，配备相关的工具、采取相应的措施和程序。防火墙的有效性从根本上取决于它在其所保护的系统上的定位及其配置和管理。

尽管防火墙和入侵发现系统能够提供某种安全服务，但是它们本身不足以确保信息资源得到全面保护。

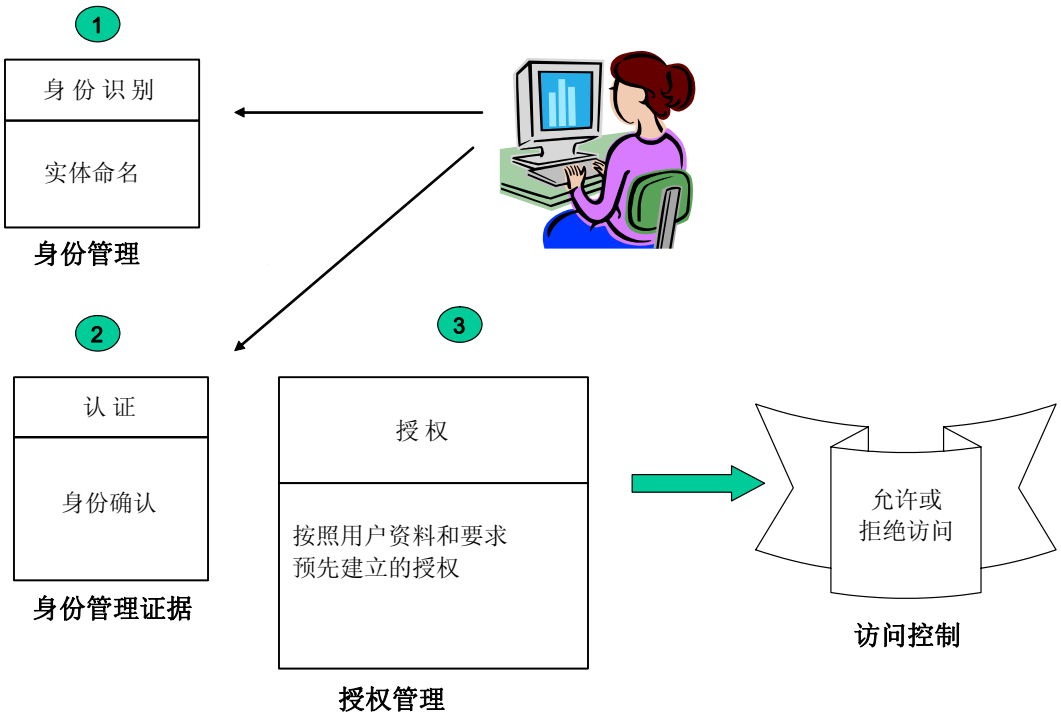
46 该图源自《信息安全与通信：正确的途径与方法》，S. Ghernaouti-Hélie著，Dunod 2006。

III.2.8 访问控制

III.2.8.1 总体原则

以个人身份识别和认证及其所获得的许可或访问权为基础的逻辑访问控制机制旨在限制对信息资源的获取（见图 III.11）。

图 III.11 – 逻辑访问控制机制的基本成分



以得到认证的身份为基础，访问控制机制根据用户资料情况允许用户获得所要求的资源。在此，机制提前假设已针对用户进行过身份管理、身份证据管理和授权管理。

用户资料包括访问授权决策所依据的所有数据，必须按照访问管理政策仔细确定这一资料。

认证的目的在于将身份概念与特定个人相关联。访问授权则需要对有关获取由网络提供的资源和服务的请求进行选择性过滤，以便仅向得到正当授权的实体授予访问权。

认证服务的目的在于验证所表明的身份是真实身份（身份证明）。通常验证下列一项或多项内容：

– 所述实体了解的秘密，即，密码或个人身份号码（PIN）；
– 实体拥有的物件（身份卡、令牌等）；
– 实体的独有特征（指纹、声纹（voiceprint）、视网膜纹等）。

身份验证要求访问申请人表明其身份，并提供只有他自己了解或拥有的一项证据（例如密码、保密密钥、指纹）。之后通过认证服务将该信息与存储于认证服务器中的数据进行比较。

必须极好地保护和保障认证服务器的安全，可以通过提供访问控制和安全系统管理以及对数据库中所存储的数据进行加密等临时性机制保护服务器。认证服务器不可存在漏洞，不可出现故障，该服务器的强健性是信息和电信基础设施整体安全的根本保障。

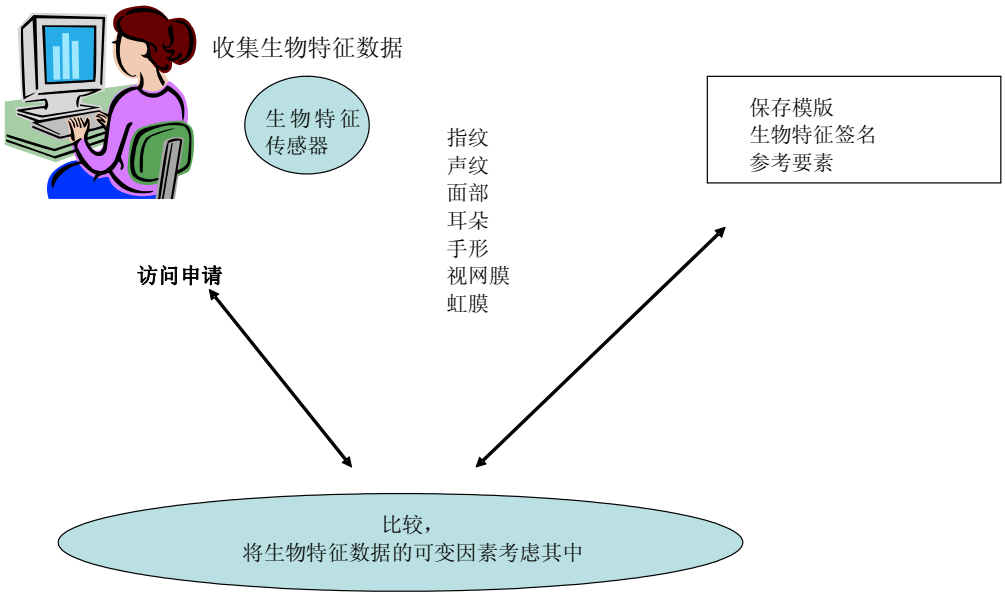
III.2.8.2 生物特征的贡献和局限性

通过生物特征确定个人身份的做法包括使用生物特征数据来在现场接入点或管辖监督范围内（由警方进行查验等）检查个人身份。

通过使用生物特征来控制对信息资源的获取可以消除密码，取而代之的是一种极易由之产生二进制数据数值的人体特性。

为了通过使用个人的人体特性来识别个人并验证其身份，首先需要以“生物特征模板”形式提取并记录个人的生物特征特性。此类记录必须十分可靠，同时须得到安全存储（见图 III.12）。

图 III.12 – 生物特征法访问控制



认证过程可能十分冗长，因为在比较阶段必须考虑到所比较的数据为活的数据，变化是与生俱来的。例如，声音采样永远不可能完全相同，比较的基础是生物特征数据的统计和概率情况。认证系统存在的模糊不清情况意味着无人能够百分之百地对认证结果给予肯定，即，系统无法百分之百地确定“x”即是他或她自己声称的“x”。此类系统的误码率依然很高，因此，不可能保障很高的安全性。如果将“传统的”、以密码为基础的认证机制与生物特征机制结合使用（双重核准），则后者有助于提高所提供的安全性水平。

对生物特征技术的广泛采用亦带来了诸多伦理和人类工程学方面的问题，更不用说其所涉及到的经济、法律和技术以及自然等问题。这些问题包括：

– 可能被视为属于个人的生物特征数据的机密性；
– 有些情况下生物特征数据可能并非独一无二（相同的双胞胎）；
– 生物特征数据传感器常常令人有被侵犯的感觉，在有其它选择的情况下，多数用户拒绝使用这一方式。这类传感器亦对个人自由造成威胁，例如，在公共场所和在人们不知情的情况下运行的诸如摄像头等大量传感器即属这方面的实例；
– 身份盗窃或对生物特征数据进行不当使用或滥用的情况时有发生。

由于以生物特征数据为基础的访问控制解决方案缺乏准确性，而且其购买、部署和运营成本依然十分高昂，因此这类方案尚未构成主流方案。

现对使用生物特征数据实现访问控制的局限性总结如下：

1 用于确定个人身份的生物特征数据会随着时间的推移而发生变化。
2 只有将生物特征数据进行收集并转换为基准采样，才可以将其存储于数据库。进行过数字化处理的生物特征数据更容易被破坏（因此更加易于改变），因此必须尽最大努力对其予以保护。每一次用户提出访问申请，均需要收集其生物特征数据，这就带来了人们对数据收集方式以及相关的被侵犯感如何接受的问题（在许多情况下，被侵犯的感觉令人反感）。
3 由于在认证过程中所分析的人体采样会发生变化，因此通过生物特征数据进行访问控制并非十拿九稳。根据所使用的系统情况，出现虚假的正确或不正确身份识别的概率相对很高，同时，该工作还取决于记录生物特征数据所采用的技术以及工作质量。

III.2.9 通信基础设施的保护和管理

III.2.9.1 保护

物理层（1 层）通过进行线路加扰，即，传输非重要信息，以便在并非重要的持续数据流内保护相关数据流，而帮助提高传输安全性。然而，若真需要保护传输，并使人无法通过捕获由传输媒介承载的信号而推算出的电磁辐射来被动偷听数据的话，传输媒介早已在法拉第笼（Faraday cages）中完全隔离。显而易见，只有在绝对必要的前提下，才可能采用此类保护措施。

必须很好地实现并维护传输媒介、接续箱和连接设备的物理安全性。

必须保护传输基础设施免受任何形式辐射的影响（此类辐射可能危及数据传输程序），同时必须保护传输基础设施免受被动（数据探测）或主动（修改、销毁或创建数据）袭击的影响。

了解如何保护用户连接至关重要。为此，必须能够了解这些用户的身份（谁是用户）和地点（所处位置），并明确其要求（目前传送的应用数据流为何种数据流？）。通过对“谁在何时做何种工作？”这一一般性问题做出答复，我们可以确定有关传输网络的各种安全性要求。

保障数据传输过程中的安全归根结底是在通信基础设施内将安全程序集成一体，因此必须能够对整个程序加以模拟。这往往需要更新所有路由器－某些情况下会带来路由器之间的互操作和路由器更换管理的问题。

此外，在网络层对数据进行加密所产生的数据包大于未加密数据包，其结果是需要耗费更多的带宽和通信资源来对其进行传输。加密亦延长了数据包的处理时间，因此在该层面进行有关安全的工作将对网络性能产生很大影响。

在网络基础设施层进行加密的主要优点是应用以及与传输相关的加密机制非常独立，对用户而言完全透明。

应用层的交易安全（尽可能在接近数据处理应用处进行数据加密）修改应用本身，数据在将其路由至目的地的网络协议交付上游得到加密，而接收应用服务器则对其进行解密。在应用实体（客户机和服务器之间）建立对话阶段，对会话密钥进行认证和商谈。该阶段工作的复杂程度并非一成不变，因此建立时间可能各不相同。但是会话一经完成，加密工作通常可迅速完成。该工作与实施平台和通信基础设施无关。

在实施分布应用的用户工作领域层开展保护工作已不再取决于数据载体或网络，而与用户的切身环境相关。保护应用的困难在于，所实施的保护必须涵盖整个应用环境和用户工作站（不再仅仅是应用本身），同时将此予以延伸，还包括用户的物理环境（出入驻地等）。

保护应用从根本上涉及到个人用户在工作站、应用和物理环境方面的权利问题。

安装在用户工作站中的操作系统的基本功能在该项保护工作中作用显著（其它有关方面在会话过程中无法实时监控，一段时间过后会自动中止连接等）。这也包括网卡保护、应用协议安全模式支持（受保护文档的传输、安全传信等）以及进行镜像和双工操作（通过在磁盘上备份数据、进行写操作和设备冗余等对数据进行保护）。

确保传输基础设施的安全或确保应用的安全从根本上讲是在不同层面解决相同的问题：

- 必须对程序和用户进行认证；
- 发送方和接收方使用相同的加密/解密算法；
- 每一个进行通信的实体均必须拥有算法和加密/解密密钥；
- 必须对加密/解密密钥进行管理；
- 必须在传送之前对数据进行格式化。

III.2.9.2 管理

如果实施得当，系统和网络的管理活动可以确保实现安全性所需的可用性和性能水平。这些活动包括对网络进行监测并对非正常情况或事件（入侵）加以发现 – 这些工作大大有助于网络及网络所服务的信息系统实现总体安全性。

好的网络管理工作有助于提高基础设施、服务和数据的效率。通过网络管理，特别是配置、性能和事件管理，可以实现可用性和完整性方面的安全性目标。

此外，被称作账户管理的网络管理工作可以使人们提供所有的、不仅为用户开具发票所需、而且是履行对安全工作极为重要的监督和审计职能所需的必要数据。在核准证据和验证不可否认性行动方面，这项工作十分有益。

网络管理还有助于实现机密性目标，因为它可以杜绝对数据的探测或对数据进行非授权访问。构成网络管理工作内容的访问控制对于安全性的实际落实至关重要。

网络的性能、服务质量、可用性和可靠性在很大程度上取决于路由器和各种设施的管理质量，好的管理可以确保根据网络状况和流量路由请求开展路由交换工作。对于网络管理人员而言，更新主要网络的路由表是一项极具挑战的工作，因为路由表中任何数值的变化均必须得到统一协调，以避免在传输过程中出现工作不良或数据丢失现象。网络管理协议具有多种目标，包括确保路由表的更新。网络管理通过在路由器配置时建立安全接入点、发现入侵企图时产生报警，并确保路由器管理和监测中心安全性等手段，帮助实现路由器的安全性。

因此，为了避免未得到授权的个人对数据做出修改，能够通过阻止或发现下列行为而提供必要的保护至关重要：

– 修改路由表、IP 数据包等所含的地址；

– 修改所传送数据的路径并对其进行非法拷贝；

– 监测数据流；

– 改变数据包的方向、修改和破坏数据包；

– 拒绝服务、攻击路由器、造成网络泛洪等。

确保数据在电信网络上进行路由的程序十分重要。“网络”服务提供商必须保护此过程涉及到的所有实体，特别是路由器和域名服务器，从而使路由服务质量达到可用性（服务工作正常）、机密性（数据被交付至应收到数据的对方）和完整性（数据在传送过程中不被修改）的安全性标准。

网络服务无法保证将数据交付至经授权的有关方面，因为交付服务并不核准这样的事实，即，交付至正确地址的数据事实上是交付至经授权应收到数据的有关方面。为此，必须进行附加的“访问控制”检查。此外，如果未对数据进行加密且数据在途中遭到破坏，则数据可能被未获授权的第三方读懂。如果数据为敏感数据，应当对其进行加密，以使无关方无法理解。

对信息网络实行监测意味着需不断观察其运行情况。网络监测的目的不仅是确保网络服务质量能够令人接受，而且旨在发现降低网络性能并可能危及资源安全性的问题、事件、错误和非正常情况，以便及时做出相应反应。通过网络监测，我们可以对有关活动和事件予以跟踪，并进行记录，以方便随后做出分析（在审计一节中将详细阐述该内容）。网络监测能够确认网络运行正常，从而确保资源的可用性。因此，在网络管理工作中，网络监测工作至关重要，因为它在性能、事件、配置、用户和安全管理方面均发挥着作用。

第四部分

综合方式

第 IV.1 节 – 新技术监管法的相关内容

IV.1.1 个人数据保护和电子商务[47]

本节讨论特别与电子商务相关的个人数据保护问题，并根据法国和瑞士的情况，确定法律的主要条文。提供在线电子商务服务的系统管理员和安全负责人必须对这些条文谙熟于心。根据这些法律条文，人们可以制定有关网络企业行为的总体原则，并针对发展中国家的情况予以调整和使用。

IV.1.1.1 电子商务：“网下”的违法行为，在“网上”同样违法

我们既可以从与消费者（企业对消费者（B2C））进行的电子商务活动的角度，也可以从公司间（企业对企业（B2B））电子商务的角度来讨论电子商务问题。例如，电子行政管理也可按照同样的方法进行分类，即与市民或其它私营或公共机构间开展的电子业务。鉴于商务法倾向于区分公司与消费者间和公司与公司间的交易，因此从法律角度而言，这是一种重要区分。

无论上述哪种情况，安全性以及在符合相关法律框架情况下采取的适当互联网营销与销售策略，均是电子商务的基石。利用安全工具树立信心，尊重法律，并创建一个有利于数据交换的环境，各国既可以鼓励普通大众采用信息技术和电信业务，并同时建立一种真正的服务型经济。

为制定有关新技术使用的法律框架，人们制定了一批新的、对现有立法形成补充的法律草案，其中许多亦适用于网络世界。但无论如何，“网下”的违法行为在“网上”同样违法！网络世界是一种国际性的和跨国界的空间，因此很难界定谁应对解决电子商务产生的法律问题负有管辖权。有鉴于此，互联网交易必须明确要约的限制，并提供在发生争议时哪些法院具有司法管辖权的准确信息。

IV.1.1.2 保护义务

个人数据保护是电子商务的一项重要因素。消费者必须了解在线广告商或企业收集、使用和传递的数据的性质。他们必须事先了解有关其自身的数据将被如何使用和传递，以及何人将有权访问这些数据。此外，他们还必须知道保护这些数据的措施。在进行商业交易时，必须有一种表述明确、易于发现和查找、可见易懂而又行之有效的有关私密性的政策。政策必须在公司的网站上予以公布。

公司亦需采取充分的安全措施，保护已收集到的并经过处理的客户数据，并确保交易涉及的第三方能够满足安全要求。

---

47 洛桑大学的研究生助理Igli Taschi参与了本节的撰写工作。

IV.1.1.3 尊重基本权利

个人数据保密和数字机密性是人们的基本人权。

《欧洲指令》示例

1995 年以来，人们已制定了关于此问题的欧洲指令，同时自 20 世纪 70 年代早期起，一些国家就通过了有关个人数据保护和控制内含具名信息的公众记录使用的国家立法，以规避对个人数据进行不必要或不恰当的存储的风险。

法国的情况

其中的一个示例是于 1978 年颁布并于 2004 年 8 月修订的法国《信息技术与公民自由法》[《信息技术与公民自由法》]。经修订的版本即刻生效并引入了一些法律概念，以适应信息社会和数字经济中出现的新的处理形式。该法取代了 1995 年 10 月颁布的 95/46/EC 指令，其目的是加强自然人的权利和保护，强化进行数据处理工作的有关方面的义务。

此类立法通常包括与下述内容相关的条款：具名数据或个人数据的定义；访问、拒绝和更正的权利；处理的目的；数据的收集、存储和更新；具名记录的安全性；数据的销售以及对跨境数据流的监控。

通常还有其它法律文件对此进行补充，例如法国 2001 年 11 月 15 日颁布的《日常安全法》[《日常安全法案》]规定，与电子通信相关的数据（计费信息除外），必须删除或采用匿名形式。“间接”数据（访问的 URL、查询过的服务器的 IP 地址、消息的主题行）亦必须被删除。

瑞士的情况

瑞士于 1992 年 6 月 19 日通过了《联邦数据保护法》（德国：1977 年 1 月 21 日颁布的法律；比利时：1992 年 12 月 8 日颁布的法律；加拿大：1982 年颁布的《个人信息保护与电子文件法》；美国：1974 年颁布的《隐私法》；1988 年颁布的《数据库与隐私法规》）。

在瑞士，2000 年 1 月 1 日生效的经修订的《联邦宪法》为数据保护提供了首要保障，其第 13/2 条规定：“人人享有个人数据受到保护和不被滥用的权利”[48]。

最重要的联邦法律条文是 1992 年的《数据保护法》以及 1993 年 6 月 14 日颁布的实施规则。无论数据的收集和处理采用何种媒介和技术，《数据保护法》均适用。无论数据如何处理，该法律均适用于个人、联邦机构、自然人与公司实体。此法的第 3 条将个人数据定义为“所有与已确定或可确定之人相关的信息”。《数据保护法》还具体规定了与敏感的个人数据和资料相关的规则。

处理被宽泛地定义为“独立于所用设备和程序的、任何与个人数据相关的操作，特别是数据的收集、存储、使用、修改、传递、存档或销毁”。然而，该法第 2/2 条列出了一些此法不适用的领域，例如悬而未决的法律诉讼以及“完全由自然人用于个人目的的、并非向第三方公开的个人数据”（a 分段）。在 2000 年 4 月 5 日做出的决定中，联邦法庭裁定，将电信保密

48 法国或瑞士法律条文的引用均为国际电联翻译科在原法文基础上的译文，除非另有说明。

规定扩大至电子信息。《瑞士联邦电信法》第 43 条还包括一条有关保密的义务：“曾经或目前仍在负责提供电信业务的任何人均不得向第三方提供有关用户流量的信息；他亦不得使任何其他人具有将此类信息透露给第三方的能力”。该法第 44 条（经 1997 年 12 月 1 日通过的联邦委员会《邮政通信和电信监督条例》第 6 至 11 条予以补充）规定了相关的监督程序和条件。

瑞士有关保护互联网上个人数据的法规，与欧洲有关同一问题的指令有很多相似之处。

IV.1.1.4 立法的经济价值

对处理个人数据和保护电子通信部门的私密性进行立法，可以鼓励各个机构对其信息技术和网络安全性进行妥善管理（用户数据、通信和员工监督、保存管理、个人数据自动处理等）。各个机构必须配有充足的安全与控制工具。

确保最低安全性（物理与法律保护）所需投资的经济价值，因各机构可能产生的物质损失及可能造成的名誉与形象损害不同而异。因此，立法是安全性的一项内在因素。

IV.1.2 电子商务与网络世界的契约[49]

本节旨在探讨在网络世界进行商业交易所涉及的有关合同的不同内容，并给出瑞士和欧洲有关规管此类交易的主要法律条文。本文引用的瑞士法律以及欧洲的主要指令包括一系列基本原则，其它国家可根据本国国情将其应用于本国法律。

IV.1.2.1 法律选择问题

电子商务所产生的第一个法律问题便是如何定义发生电子交易的地理区域问题。互联网的特点（国际覆盖、数字技术、运作模式）与国家地理边界的概念大相径庭，且信息流不会在各国疆界处止步不前。

无论互联网用户和服务器置于何处，数据和业务均能够被获得并以远程方式得到提供。买卖双方常常在不同国度进行交易。因此，了解出现争议时应适用哪种法律至关重要，而且是任何要约的关键所在。对此，经互联网进行的交易必须指出要约的限制，并提供详细信息，说明出现争议时哪家法院具有管辖权[50]。

签约双方可以商定采用何种法律以及主审法院。若无法律选择条款，则必须确定该合同是属于国际条约，例如 UNIDROIT（国际统一私法协会）的《国际商事合同通则》（1994 年）（一种网络规矩）；还是属于 1955 年 6 月 15 日签署的《海牙公约》的范畴。但除非明确纳入合同之中，否则国际条约不具约束力。

---

49 洛桑大学的研究生助理Igli Taschi参与了本节的撰写工作。

50 *Lex fori*（同缔约地法）是一项国际私法原则，系指进行诉讼的国家的法律。

如果上述两个解决方案均不适用，则应采用合同法的规则。

例如，瑞士于 1987 年颁布的《联邦国际私法法》第 1 条规定[51]：

“[1] 此法案适用于国际情况下的管理：

a. 瑞士法院或行政主管部门的管辖权；

b. 适用法律；

c. 承认并执行国外判决的前提条件；

d. 破产及与债权人达成和解协议；

e. 仲裁。

[2] 国际条约仍予以保留。”

基本原则如下：合同应受与之联系最为密切的国家的法律的管辖（上述联邦法第 117/1 条）。通常，如果在一般性条件下明确予以包括，则系指货物或服务的提供商，但也存在一种例外，即该法第 120 条对消费者合同做出了如下规定：

在下述条件下，针对消费者个人或其家庭使用的、与其专业或商业活动无关的普通消费行为合同，应遵守消费者通常居住地所在国的法律：

a. 要约方在该国收到订单；

b. 在该国，签订合同之前存在要约或广告，且消费者为签订合同采取了必要的法律行动，或

c. 要约方提醒消费者出国并在所去国家提交订单。

[2] 排除法律选择。”

有关地点的内容，例如使用的语言或所列币种，可表明要约方的目标市场，进而说明适用的法律。

如果各方未就法律选择达成协议，则可在被告居住地或总部所在地起诉。

IV.1.2.2 以电子方式签订的合同

适用于以电子方式签订的合同的规则整体上与“所谓”传统合同的适用规则相同。当一方提出要约且另一方接受要约后，合同即已签订。

欧洲指令

欧洲议会与欧洲理事会于 1997 年 5 月 20 日颁布的 97/7/EC 号指令，旨在处理远程销售和电子商务方面的问题。指令规定，在任何远程销售合同签订之前，均应向消费者提供下述信息：

- 供应商的身份，如合同要求预付款项，还应提供其地址；
- 产品或服务的主要特点；
- 包括所有税费在内的货物或服务的价格；
- 交付成本（视情况而定）；
- 支付、交付或履行的安排；

51 英文版《联邦国际私法法》译者：Jerome H. Farnum（文学学士，法学博士）；《瑞士联邦国际私法法》正式文本的英译本， 2004年，苏黎士，瑞美商会/Schulthess（修订版）。

– 规定取消权利，指令第 6 条(3)所述情况除外；
– 当远程通信计算未采用基本费率时，使用此种通信的成本；
– 要约及价格的有效期；
– 酌情提供长期或周期性产品或服务合同的最短期限。

与签订合同相关的最重要的一点涉及如何定义“要约”和“接受要约”的内容。根据《瑞士债务法典》第 7 条，互联网上“展示”的、标有价格的产品及相关的广告信息，并不构成要约，而应被视作投标。该条的内容如下：“[2] 发送费率、价格清单及相关信息本身不构成要约[…]”。[52]

发送电子信息或订单表亦应被视作投标。

当买方接受或点击“购买”后，才构成正式要约并签订合同。就像采购者进入一家商店一样，仅仅访问网站，并不表示其有购买意向。另一方面，在网站上展示商品，仅在卖方所指现货在收到订单后减少，或货物的性质为卖方总有能力满足订单要求的情况下，才能构成要约。

当享受服务的一方，即希望购买所示产品的消费者，收到卖方发出的电子确认函后，则可认为合同已经签订，但这两份文件发出的间隔应很短。需对双方同时得知合同成立与双方并非同时得知合同成立的情况加以区别。

要约和被要约人不在场的合同？没问题，但是...

互联网上签署的合同被视为要约和被要约人不在场的合同，即正如《瑞士债务法典》第 5 条规定，需在合理的时间内接受要约：

“第 5 条:

b. 未出席方之间

[1] 如果在未设置时限的前提下，向某未出席方提出要约，则在提出要约的一方认为合理的、应收到以恰当形式和及时发出应答的时间范围内，受到要约的约束。

[2] 因此，提出要约的一方可以假设其要约及时到达。

[3] 如果及时发出了接受要约的声明，但却在超过时限后才到达提出要约的一方，则要约方仍受其要约约束，除非他毫无延误地给出其有意放弃的通知。”

但是，如果合同数据的交换通过讨论论坛、聊天室、即时消息或互联网电话进行，则应认为双方同时得知了合同内容，因此应须立即接受合同。《瑞士债务法典》第 4/1 条规定：“如果在未设置时限的情况下，向出席的一方提出要约，则在要约未被接受的情况下，应认为要约方不再受约束。”

IV.1.2.3 电子签名

由于非对称加密体系的出现，因此读者能够检查信息的完整性，确保信息在传输过程中未被修改并确认发信人。如此一来，发信人便无法否认其发送过信息（不可否认性概念）。信息安全服务是通过对数字文件进行数字证书“签名”加以实现的。用手写签字作比喻，则电子签名是一种针对数据的数字签名。相关的概念还包括专用和公共加密密钥以及认证管理机构（又称作值得信赖的第三方或 TTP）。

52 英文版《瑞士债务法典》译者：法学博士Rebecca Brunner-Peters等，《瑞士债务法典》第一卷，合同法第1-551条，正式文本英译本，2005年，苏黎士，瑞美商会/Schulthess（修订版）。

若要将纸质文件上的手写签名以电子签名的方式移植到数字世界中来，它必须能够与签名者之间建立起一对一的对应关系，必须能够确定签名者，且其使用的方法必须完全在签名者的独自掌控之下。

瑞士法律认为电子签名与手写签名具有相同的法律效力。《瑞士债务法典》第 14 条规定：

“[1] 签字必须为手写。

[...]

[2之二] 在 2003 年 12 月 19 日颁布的《联邦电子签名法》认可的范围内、由合格的认证业务提供商提供的合格电子签名，应等同于手写签名。违背这一原则的法律或合同条款仍予以保留。”

2003 年 12 月 19 日颁布的《联邦电子签名法》约束电子签名，其中包括电子签名的定义，各类电子签名形式的描述，并列出了涉及电子签名机制实施与数字证书颁发的相关各方。

“第 2 条，定义

本法中：

a. 电子签名系指附加在其它电子数据之上或与之有逻辑关联的、并作为一种认证方法的电子形态数据；

b. 高级电子签名系指满足下述要求的电子签名：

1. 与签名者之间存在一对一的对应关系，

2. 能够确定签名者，

3. 创建时使用的方法完全在签名者的独自掌控之下，

4. 与其关联的数据是随后的变化可被发现的数据；

c. 合格的电子签名系指根据第 6/1 和 6/2 条的规定，以安全的签名制作安排为基础、并在其创建时证书仍然有效的高级电子签名；

d. 签名密钥系指签名者用来制作电子签名的唯一数据，如密码或专用加密密钥；

e. 签名验证密钥系指用于验证电子签名的数据，如密码或公共加密密钥；

f. 合格的证书系指满足第 7 条要求的证书；

g. 证书服务提供商（提供商）系指认证电子环境中的数据并为此颁发数字证书的实体；

h. 确认机构系指根据核准规则，被授权对提供商进行确认和监督的实体；

[…]”。

电子签名和欧洲指令

1999 年 12 月 13 日颁布的 1999/93/EC 指令涉及欧洲电子签名框架。根据加密机制集成度的程度以及提供的安全水平的高低，此框架将电子签名分为三种类型。

电子签名存在诸多类型。首先，可以简单地对某信息进行“签名”，而无须在签名与信息之间建立联系（电子签名的基本概念）。在这种情况下，任何人都可以将签名从信息中“分离”出来，并取代原合法签名者的位置。为克服这一缺点，可通过加密功能将签名与信息内容关联一起，并在收到信息时验证发信方的真实性和信息的完整性（高级电子签名的概念）。

最后，在附件二（有关对颁发合格证书的认证服务提供商要求的）安全性条款的基础上，该指令讨论了安全电子签名问题[53]。

IV.1.2.4 撤消权

通过互联网购买产品的便捷性会导致某些消费者轻率采取行动。在此方面，撤消权尤为重要。

在瑞士，《瑞士债务法典》第 9 条第 1 段对撤消权做了规定，其规定的原则如下：“如果要约方撤消其要约，且此撤消决定在[...]要约前到达另一方，则应认为[...]要约并未生效”。此原则同样适用于接受的撤消。

撤消权与欧洲指令

欧洲联盟 1997 年 5 月 20 日颁布的 1997/7/EC 指令对撤消权做出了规定。指令规定，对于任何远程销售合同，消费者至少在七个工作日内有权撤消，而不会受到处罚，也无需给出任何理由。如果供应商未能履行第 5 条规定的义务，特别是有关行使撤消权的条件和程序，则该期限为三个月。

IV.1.2.5 争议的管理

因有效签订的合同而产生争议的各方（无论该合同是否采用了电子形式），均应提供证据。因此，建议始终保存交易的记录，如电子信息的拷贝或拷屏。

法国的情况

法国的《消费者法典》第 109 条未就应提供何种形式的 B2B 证据做出详细说明。因此，与纸质文件相似，电子邮件亦可被接受。但对于 B2C，超出一定金额的交易则需要书面凭证。此要求的目的是为了保护普通的消费者，因为他们在与商家产生争议时，既无能力也无法律资源与之进行抗辩。

但是，根据电子签名的法律条文，可将电子邮件作为证据。这意味着以电子形式签署的电子邮件，在上述有关电子签名的条款得到遵守的条件下，将被作为有效证据。

---

53 http://europa.eu.int/eur-lex/pri/en/oj/dat/2000/l_013/l_01320000119en00120020.pdf

一般性条件

远程销售合同通常包括一些一般性条件，这些条件构成了合同不可分割的一部分。为在发生争议时这些一般性条件能够生效，这些条件必须易于访问和在线查询，且必须明确告知客户，这些条件是合同的组成部分。

争议的在线解决

鉴于电子商务的国际性质，人们已经为那些避开传统法庭的争议制定了解决办法。争议在线解决机制（ODR）概念的问世，是出于人们为无法履行通过互联网签署的协议寻求立竿见影解决方案的愿望。这种争议的解决方案以调解为基础，其中不仅包括协商、斡旋，还包括仲裁。[54] 对用户而言，此种方式更为快捷、便宜、方便。但由于这种解决方案是基于行为准则和建议的，亦称“软法律”（如互联网域名和号码分配机构（ICANN）的《域名争议统一解决政策》），因此决定难以执行。

IV.1.3 网络世界与知识产权[55]

IV.1.3.1 有关保护知识产权的法律

知识产权受到多种法律的保护，其中主要包括：

- 商标法；
- 版权法；
- 专利法；
- 设计与示范法；
- 植物多样性保护法；
- 半导体布局法；
- 公共盾形徽章及其它公共标志法。

有关不正当竞争的法律亦会对知识产权产生影响。

IV.1.3.2 版权和邻接权

此类法律保护：

- 文学与艺术作品的作者；
- 表演者、录音或电视录像制作人及音像传播企业。

一部作品是对文学或艺术精神的创造；无论其值几何或本意何在，它在本质上均是独特的。精神创造包括：

- 使用科学、文学或其它类语言的作品；
- 音乐与其它声音类作品；
- 美术作品，特别是雕塑和图片作品；
- 具有科学或技术内容的作品，例如设计、规划、地图、雕刻或雕塑作品；
- 建筑作品；
- 应用艺术作品；

---

54 这种争议解决机制是联合国贸易法委员会（UNCITRAL）制定的示范法的主题。

55 洛桑大学讲师，突尼斯理工大学的Sarra Ben Laggha教授参与了本节的撰写工作。

– 摄影、电影和其它图像或音像作品；
– 舞蹈和哑剧；
– 计算机程序（软件）；
– 具备独特属性的项目、或作品和标题的组成部分。

版权为作者（创造作品的自然人）或假定作者（在确定真正作者之前将作品公诸于世的人）赋予了精神权和所有人权。

尽管有些国家存在版权保存，但并非必须将作品交存某机构或进行版权注册。鉴于只有有形的作品才能得到保护，因此只有将思想记录下来才能对其加以保护。

“精神权”本质上系指对作者身份的认可，以及作者拥有决定是否、在何时、以何种方式、用何种名义公布其作品的权利；而“所有人权”与作品的使用相关（拷贝的制作与销售、展示、分销、传播等）。

作品所有权的转移，无论是拷贝还是原件，均不代表版权的转移。版权可以转让和继承。

“邻接权”系指演出者（演出作品的自然人或以艺术形式参加表演的自然人）、录音或电视录像制作人及音像传播企业的权利。

IV.1.3.3 商标法

商标的目的是区别商标所有者的产品和/或服务与其它公司的产品和/或服务。商标用于标识某一客体（并非法律主体，因为法律主体倾向于通过名称或公司名进行标识）。

对下述内容无法提供商标保护：

– 公共标记；
– 与产品属性相关的或使用时体现出的内在形态；
– 误导性标记；
– 与现行法律或道德相悖的标记。

商标必须进行注册才会获得保护。下述情况下，商标注册可能遭到拒绝：

– 与过去为相同产品注册的商标相同；
– 与过去为相似产品和/或服务注册的商标相同或相似，并存在混淆的风险。

IV.1.3.4 专利法

专利为工业发明而设。不能为技术发展的副产品（显而易见的）、各类植物或动物、或本质是用于植物或动物制造的生物流程授予专利；但可以为微生物流程和使用此类流程获得的产品授予专利。

专利将授予（在特定条件下）专利的申请人（发明人，其法律继承人或因其它原因拥有该项发明的第三方）。

如果几个发明者独立地发明了相同的产品或流程，则专利将授予第一个提交申请的发明人或申请为优先的发明人。

IV.1.3.5 网站的知识产权保护

互联网特别是网站的知识产权保护涉及多种法律[56]：

- 关于域名：
  - 域名注册本身并不表明对所有者授予了具体专有权；
  - 为保护域名，必须依靠法律基础，即：
    - 商标法；
    - 公司名称法；
    - 命名权；
    - 竞争法；
- 关于网站的内容：
  - 特别是通过互联网传播作品；
    - 如果内容专为网站制作，则受版权保护；
    - 现有作品的数字化及其在线传播属于一种复制，因此需要得到原作者的同意；
    - 与其它网站的链接：由于并不涉及复制，因此仅使用简单超级链接并不构成对专有权的侵害；深度链接（绕过某网站的主页，将用户指向另一网站内的某特定网页）则另当别论。目前的问题是网页是否是一种作品。通常，此类问题通过竞争法加以解决，其中决定性标准是超级链接的使用方法。在此，公平使用是核心概念。

IV.1.3.6 技术和法律保护的补充性质

为确保版权得到尊重，目前正在不断引入技术措施。立法工作也在不断进行，以确保这些措施不会被避开。因此，版权在享受法律保护和技术保护的同时，还享受以技术保护为基础的法律保护。

IV.1.4 垃圾邮件（Spam）：一系列法律方面的考虑[57]

IV.1.4.1 背景及烦扰行为

广义而言，垃圾邮件[58]系指发送推介性的信息，其特点如下：

- 推介性的信息被大量和重复发送；
- 信息具有商业目的或存在恶意（网络欺诈、计算机接管、引入病毒、广告软件、间谍软件等恶意软件）；
- 通常在所有者不知情的情况下获得其地址（违反了与个人数据保护相关的规则）；
- 内容通常非法、具有误导性或有害。

---

56 见Philippe Gilliéron著《知识产权与互联网》，洛桑大学（洛桑大学企业权利中心（CEDIDAC），第53号），2003年。

57 洛桑大学的研究生助理Igli Taschi参与了本节的撰写工作。

58 “垃圾邮件（spam）”一词最初为Hormel注册的商标，其原文为“腌制的猪肉和肉类（spiced pork and meat）”– 在第二次世界大战期间为美国士兵提供的一种腌牛肉。目前，spam被用来描述发送推介性的电子邮件，是源于Monty Python剧团一部著名的系列剧。在该剧中“spam”一词被反复吟唱，而其他主要演员的声音均被其淹没。

由于垃圾邮件是一种推介性的邮件，因此有时会被认为是一种侵略性销售或广告技巧。如今，其形式已从单一的电子邮件信息，发展为手机或便携 PC 等新型多媒体设备的短信（SMS）。

垃圾邮件为互联网所有用户均带来了成本。这些成本通常与用户处理此类信息以及获取反垃圾邮件工具所需的时间相关。从用户丧失信心，生产力的下降等角度来看，垃圾邮件亦带来了社会成本。

根据从事打击垃圾邮件的 Clearswift 公司在 2005 年 9 月 13 日的《网络日报》上公布的研究结果，垃圾邮件被归纳为以下几类：

垃圾邮件的类别	2005年6月
卫生	43.86%
产品	37.65%
金融	9.06%
色情	5.32%
网络欺诈	1.41%
在线赌博	0.1%
其它	2.32%

垃圾邮件存在多种形式的“骗局”（scam），其中最普通的一种便是所谓的“尼日利亚”来信[59]。网络欺诈包括以知名机构的名义发出信息，例如某家银行，请收件人与假冒网站连接，并要求其输入访问密码和其它敏感信息，而这些信息最终将在用户不知情的情况下被使用。

垃圾邮件亦可用于破坏的目的或阻塞收件人的邮箱，使其无法接收信息并无法使用互联网资源。邮件“爆炸”有多种形式：通过大邮件造成处理和临时存储问题，向大量收件人发送海量邮件，以造成服务器泛洪，或非法占用发信人的地址。

IV.1.4.2 垃圾邮件的法律补救方法

可通过多种法律打击垃圾邮件，特别是数据保护和反不正当竞争法；垃圾邮件制造者还涉嫌刑事犯罪。

---

59 发件人自称是一位最近刚去世的富翁的继承人。有时发件人来自一个遥远的国度。“继承人”称其在主张继承权时出现了问题，并请求受害者允许其使用他的银行账户，做为补偿，受害者将因此获得一大笔款项。受害者必须预付与交易相关费用。毫无例外，这些骗局均是为了骗钱。

瑞士的情况

瑞士没有明确的有关反垃圾邮件的法律条款。

从数据保护角度而言，根据瑞士联邦数据保护委员会及其文件 –《关于以电子邮件方式传播的无用广告信息的备忘录（垃圾邮件）》[60]，电子地址是一种可用于确定某个人身份的个人数据。根据《数据保护法》第 12/3 条 –“通常，如果受到影响的某人将其数据向大众公开，且并未明确表示禁止对其数据进行处理，则不会对此人的权利造成侵害。”在未经当事人允许的情况下（第 13/1 条），垃圾邮件制造者对电子地址的恶意处理（第 4/2 条）构成了对隐私的侵害（第 4/3 条）。因此，它违反了有关数据保护的规定。

“第 4 条原则

1 所有个人数据处理都必须采取合法的形式。

2 处理必须是善意的且不能过度。

3 个人数据的处理必须基于其收集的目的，或符合具体情况的要求，或有法律依据。”

《数据保护法》规定有关人员可以寻求法院的帮助（第 15 条，该条参引了《瑞士民法典》第 28 ff 条）。

欧洲指令

1995 年 10 月 24 日颁布的有关个人保护的 95/46/EC 号指令，对个人数据处理和此类数据的自由流动做出了规定，并为记录的构成与数据处理制定了最低标准。第 10 条规定，数据主体必须了解收集数据的目的以及控制人员的身份。

法国的情况

在法国，《信息技术与公民自由法》将因计算机记录或处理引起的隐私权侵害并入了《法国刑法》。该法 2004 年修正案引入了第 14 条，对滥用个人数据规定了更为严厉的惩罚。

美国的情况

美国是垃圾邮件的最大原产地。2004 年 1 月 1 日，国会通过了《反垃圾邮件法》（CAN-SPAM Act），规定对寄送垃圾邮件者予以起诉。此法禁止从网站“大量收集”电子邮件地址并禁止使用以“字典攻击”方式生成地址的程序，此种程序对字母和数字随机进行组合。

当垃圾邮件用于广告目的时，垃圾邮件亦应被归类为不正当竞争。

垃圾邮件、广告和不正当竞争

互联网广告由有关广告的一般性法律条款而非特定法律框架予以规管。2001 年 11 月，瑞士商业传媒公平竞争委员会提出了有关垃圾邮件的建议性意见，认为垃圾邮件是一种特别激进的销售方式。从广告的角度而言，无论是从事“传统”业务还是电子商务，只有在符合某些基本规则时，才可以使用此种方法。

---

60 见www.edsb.ch/f/doku/merkblaetter/spam.htm

这此规则包括：

- 保护使用互联网的青年用户；
- 尊重人类；
- 尊重广告的公平性、真实性和诚实性；
- 尊重互联网用户的合法隐私权；
- 易于浏览。

《瑞士联邦反不正当竞争法》第 3 条规定：“特别当某人有下述行为时，会产生不正当竞争：

[…]

b. 提供有关其自身、业务、公司名称、产品、作品、提供的服务、价格、库存、销售或业务方式的不准确或错误信息，或通过提供此类信息，使第三方获得对其竞争对手的优势；

c. 展示或使用某种不准确的职务名称或称呼，使他人相信其具备某些与众不同之处或能力；

d. 采取某种措施，导致与另一人的商品、作品、服务或业务的混淆。”

但是，只有第 3 条第 h 段的内容是真正涉及问题的本质的内容。该条规定：“特别当某人有如下行为时，会产生不正当竞争：

[…]

h. 通过采用特别激进的销售方式，妨碍客户做出决定的自由。”

如果以上述强度将其用于商业目的，则垃圾邮件属此条的规管范围。

垃圾邮件与犯罪意图

如果垃圾邮件制造者的行为具有犯罪意图，则可能受到刑罚。即使他们发送的信息本身是商业性的，但其内容仍可能会使他们面临起诉。

垃圾邮件与色情

大多数垃圾邮件均邀请读者访问色情网站。根据《瑞士刑法》第 197 条的规定，这是一种刑事犯罪，特别是使不愿意接收此种内容的用户（第 197/2 款）或 16 岁以下儿童（第 197/1 款）收到此种信息。

垃圾邮件、欺诈病毒和出售违禁物品

根据《瑞士刑法》第 146 条的规定，欺诈是一种刑事犯罪。欺诈被定义为从受害者身上取得经济利益以达到自身致富的目的。从这一角度看，“尼日利亚来信”理应被视作欺诈。

垃圾邮件有时是病毒感染电脑的最佳途径。根据瑞士法律，如果因病毒进入造成数据被破坏（如受害者的数据被修改、删除或无法使用），则可以根据《瑞士刑法》第 144之二条对垃圾邮件制造者提起诉讼。

瑞士法律亦禁止通过垃圾邮件销售药品。瑞士药品和医疗设备法第 32 条规定，禁止鼓励过度使用、滥用或不当使用药品的广告，亦禁止有关瑞士市场不准许出售或需要提供处方才可出售的药品的广告。

IV.1.4.3 垃圾邮件的规管

目前存在两种大相径庭的垃圾邮件规管方法：“选择加入”法（opt-in approach）和“选择退出”法（opt-out approach）。

“选择加入”法又称允许营销。由于此种方式仅向用户发送该用户以选中选项框的方式，明确表示同意接收的特定广告，因此更加尊重互联网用户；同意也可以采用推断的方式，但在此情况下，须将此签约的商业性质及后果明确告知来访用户。

“选择退出”法属于“解除签约”的范畴，而且用户有权在收到信息后拒绝接收。所有发送的广告均须允许接收者解除签约。“选择退出”法的记录可采用合法的形式收集（如购买“选择加入”的用户清单），也可以通过随机程序收集。

瑞士和美国立法机构采用了“选择退出”法，而正如 2002/58/EC 指令所示，欧洲联盟倾向于使用“选择加入”法。此项指令涉及电子通信部门对个人数据的处理以及隐私的保护（有关隐私和电子通信的指令）。

由于垃圾邮件制造者倾向于以匿名的方式从国外进行操作，因此诉讼费用高昂且过程复杂，通常需要聘请律师。

IV.1.4.4 处理垃圾邮件的技术手段

技术限制

通过技术手段设定限制可以抑制垃圾邮件，例如限制每条信息的收件人数量、限制每个信源发送信息的数量，以及单位时间内的信息数量。

黑名单

黑名单工作原理是以服务器的信誉作为标准对邮件进行分类。最近发送过垃圾邮件的电子邮件服务器的信誉将受到损害，人们会假设该服务器在将来可能发送更多的垃圾邮件。服务器可通过 IP 地址加以确定。

使用关键字过滤

关键字过滤程序会将包含某类关键字的邮件拒之门外。由于垃圾邮件制造者可以轻易写出绕过过滤程序的邮件，因此这些程序并无效果。

特征对比技术

垃圾邮件存在于大量发送的相同信件之中。特征对比技术在归纳信息内容的特征之后，将其与垃圾邮件内容的数据库进行对比。

反恶意软件政策

越来越多的“恶意软件”（病毒、特洛伊木马、机器人（bot）等）正被用作在受感染电脑上安装电子邮件服务器的工具，其目的在于更方便地传播垃圾邮件。反垃圾邮件亦意味着对恶意软件穷追不舍。

反垃圾邮件软件有助于在电子邮件服务器层过滤和阻止垃圾邮件，从而限制其扩散，但这并非总能奏效。合法信息无法传递给收件人（误报概念），而真正的垃圾邮件却得以通过（漏报概念）。

用户的态度是与垃圾邮件做斗争的关键因素。如果用户采用恰当的方式对信息进行处理（他们应意识到身份有被窃取的风险、在以在线方式公布其电子邮件地址之前检查其地址将做何用途、使用多个电子邮件地址、避免使用某些网站、学会避免打开来自未知发件人的邮件、不阅读垃圾邮件而直接将其删除，不回复不点击垃圾邮件中的超级链接等），则问题的范围可以得到限制。

IV.1.4.5 技术与法律手段间的互补

由于法律补救措施对垃圾邮件的影响甚微，因此需要采用技术方案。在反垃圾邮件过程中，必须从技术和法律两方入手。每有一位因法治而放弃行动的垃圾邮件制造者，或通过技术手段有效阻止其发送垃圾邮件，均意味着千百万封垃圾邮件将会无法大行其道。

IV.1.5 与网络世界相关的主要法律问题摘要[61]

IV.1.5.1 商用互联网的法律地位

商用互联网的法律地位由所使用信息技术工具的法律地位确定。

对于电子邮件，相关问题为邮件的内容、邮箱地址，以及地址可用于确定 – 和盗窃 – 个人的身份、明确的标记或公司名称。这些问题统归各国民法管辖。

对于网站，作品的概念（无论是否为音像作品）会引发版权问题。超级链接存在内容、责任和是否受到保护的问题，以及与搜索引擎相关的问题。

IV.1.5.2 网络合同

网络签约引发的不仅仅是法律问题。它还需要通过技术手段来切实签订合同（使用的工具和程序（全球性、无形性，非本地性））。

从法律角度而言，下述内容十分重要：

- 要约、要约的形态（远程或当地）、要约的接受；
- 广告与请求、垃圾邮件等；
- 执行；
- 要约的在线接受以及表明接受要约所使用的信息技术；
- 撤消权；
- 法律和管辖权的选择。

上述内容均见诸于欧洲不同指令，即：

- 2000 年 12 月 22 日颁布的、有关民事和商业问题管辖权、判决的确认与执行的欧共体理事会（EC）44/2001 号规则；
- 有关电子商务的 2000/31/EC 号指令；

---

61 洛桑大学的研究生助理Igli Taschi参与了本节的撰写工作。

– 1998 年 6 月 22 日颁布的 98/34/EC 号指令，该指令制定了提供信息的技术标准和规则程序；
– 关于保护远程销售合同中消费者利益的 97/7/EC 号指令 。

相关法律还包括联合国贸易法律委员会（UNCITRAL）1996 年制定的电子商务示范法，世界贸易组织（WTO）1998 年日内瓦部长会议有关全球电子商务的宣言，以及 1997 年美国和欧盟有关电子商务的联合声明。

IV.1.5.3 电子文件和签名

以电子形式签署的电子文件产生了有效性问题。人们的目标是确保签名的法律有效性，以便确定签名人，确认该签名人具有签署该文件的意图，并因此对文件的内容负责。

相关法律条文的实例包括 1999 年 12 月 13 日颁布的、欧共体有关电子签名框架（欧洲联盟）的 1999/93/EC 号指令；1997 年 3 月 15 日颁布的 59 号法律（意大利）；2000 年 6 月 30 日颁布的《全球与国内商务活动电子签名法》（美国）；2000 年 5 月 25 日颁布的《电子通信法》（英国）。

IV.1.5.4 电子支付

涉及信用卡、支票或电子货币的电子支付可能会被第三方截获，例如在业务供应商与接收方通信期间，相关信息被滥用。

关于法律条文的示例，请参见 2000 年 9 月 18 日颁布的 2000/46/EC 号指令，该指令就电子货币机构业务的采取、开展和审慎监督做出了规定。

IV.1.5.5 域名保护

域名是一种商业价值颇高的新型无形资产。必须从域名与下述内容之间的关系考虑域名问题：

– 商标和域名；
– 明显的标记；
– 业务名称与域名。

除与商标、名称及专利相关的国家立法之外，美国的《反网域名称抢注消费者保护法》（ACPA）在此十分具有针对性。

IV.1.5.6 知识产权

互联网的知识产权提出了与版权、商标和专利有关的问题。《世界知识产权组织（WIPO）版权公约》、《世界知识产权组织表演和录音制品公约》、欧洲立法中 1995 年颁布的《信息社会的版权与相关权利绿皮书》、欧洲议会的 2001/29/EC 号指令、欧洲理事会 2001 年 5 月 22 日颁布的、有关协调信息社会版权与相关权利某些内容的规定，均涵盖了知识产权问题。

IV.1.5.7 保护数字隐私

滥发邮件是对数字隐私权的侵害（见关于保护远程销售合同中消费者利益的 97/7/EC 号指令，关于电信部门个人数据处理和隐私保护的 97/66/EC 号指令，该两项指令均禁止使用垃圾邮件进行直销）。

IV.1.5.8 其它法律问题

在确定恰当的有关互联网使用法律框架时必须考虑的众多其它法律问题之中，应对下述问题予以考虑：

- 反托拉斯立法（见美国 2000 年 4 月颁布的《促进竞争者间合作的反托拉斯指导原则》）；
- 供应商和技术中间商的责任（供应商应在何种程度上对互联网用户的活动、犯罪行为、儿童色情等负责）；
- 通邮秘密的不可侵犯性。

第 IV.2 节 – 前景

IV.2.1 教育 – 培训 – 提高网络安全所有利益攸关方的安全意识

互联网的所有利益攸关方均需要意识到有关安全问题的重要性，同时认识到如果能明确阐明并以明智方式落实一些基本的措施，将能加强使用者对数据处理和包括互联网在内的通信技术的信心，这一点十分重要。互联网应该成为所有人的财产，不应仅给犯罪活动带来可乘之机。

在安全问题上，必须采取有效步骤，培育出一种文化并通过多学科并举途径，控制信息技术被用于犯罪目的所带来的风险。国家和各类组织都必须用战略的眼光看待这些问题。

在数据处理和通信技术上，必须提供广泛的教育、宣传和培训，而非仅限于在安全和震慑力方面下功夫。提高安全意识决不应仅限于倡导一种安全文化，首先必须要有一种信息技术的文化。各利益攸关方必须掌握方法，学习管理在使用新技术当中所发生的与技术、运营和信息相关的风险。

互联网所具有的虚拟性质和娱乐特点，更可以蒙蔽年轻人和初学者，使他们看不到其造成危害的严重性。对于沦落为其牺牲品的各类组织（公司、行政管理或社区组织）及个人，它都会造成极为可怕的严重后果。控制技术方面的风险比追查黑客或设置技术障碍更为重要。缺乏足够的能力、理解错误或技术实施不当带来的疏忽大意以及系统管理员权限过大、管理不善等等，有时都会造成最为严重的恶果。

IV.2.2 解决安全问题的新途径

除数字世界存在薄弱环节外，对信息通信技术和基础设施，以及市场上推介的安全解决方案进行驾驭亦存在固有的困难，对此我们应认真审视自身对这一难以管理的技术的依赖。受制于信息技术系统的数据，已经成为一种令人难以忽视的危险因素。

认为技术和法律解决方案，将能从战略、战术和运营上弥补信息技术和电信的概念错误和管理不善带来的问题，只是一厢情愿。更为重要的是，只有以透明公开、易于核实和驾驭有方的方式实施传统安全措施，才能够卓有成效地保护人员、组织和国家的敏感或重要资源。

建立一种包括预防、保护、防范和应急反应在内的综合安全机制，意味着在人员、法律、技术和经济方面采取手段来具体加以实施。

IV.2.3 安全策略的特点

通常而言，无懈可击的安全策略以风险分析为基础，是一种全面和连贯协调的策略，可以针对特定环境的安全需求提供具体的反应机制。

这一策略必须：

- 简明扼要，易于理解；
- 可以由训练有素和负责安全的人员加以执行；
- 易于实施；
- 易于保持和完善；
- 易于核实，易于操作。

安全策略不应一成不变，它必须定期得到审查、优化和调整，以适应其所实施环境的发展变化。必须能够根据利益相方使用的流程、环境和所处的地理位置，按照使用者的特点加以调配和确定。安全策略将随着时间和空间变化而发生变化。

安全策略可被细分为访问控制、保护、危机管理、后续跟踪和优化以及建立信任等方面的详细策略。

IV.2.4 识别敏感资源，保护敏感资源

通过制定有关安全所涉及的全部资源和参与者的完整和准确的库存资料，人们可以更加清晰地了解资源的使用环境和保护需求。必须确定不同种类资源的价值，以便明确其敏感程度（或重要性），从而决定哪些为优先保护对象。敏感程度取决于如果数据丢失、被篡改或泄露而产生后果的严重程度。资源的敏感性和价值越高，对该组织造成的后果就越严重。

每种资源均应被视为一个具体的安全指标，其相关的风险及其产生方式（借助于使用者的过失、参数错误、事故以及恶意利用、蓄意破坏、逻辑攻击等等）以及内在的可行安全机制（配置、参数等）和技术及组织方面的限制因素，均应明确无误，以便确定有关具体指标安全策略在技术和组织上的可行性。

IV.2.5 网络安全的目标、使命和基本原则

网络安全的目标是：

- 机密性（严禁非法访问）：保持信息秘密，做到未经授权，不得访问；
- 完整性和准确性（无虚假信息，无错误）：保持数据和程序的完整性和完好状态；
- 可用性（无延误）：保持持续、不间断和未受损害的可用性；
- 长久性（未遭破坏）：按需长期储存数据和软件；
- 不可否认性和可归责性（无纠纷）：保证行动的原型、来源、目的地和真实性；
- 尊重数字隐私权；
- 认证（对资源身份没有疑虑）。

每种使命均可细分为下列组成成份：

- 制定基于以往风险分析的安全计划；
- 确定采用新技术带来的薄弱环节的范围；
- 保持保护与风险的齐头并进；
- 在组织结构、措施、工具和程序方面落实并核实安全工作；
- 监督、审计、控制和开发信息系统及其安全性；
- 按照安全水平要求优化信息系统的性能；
- 实现需求与风险和成本的协调统一。

旨在推进网络安全行动的基本原则如下：

- 词汇（需要就定义安全性的共同语言达成一致）；
- 一致性（网络安全，只有在用于防范、发现、保护和用于纠正由过失、恶意或自然因素造成的损害时所采用的工具、机制和程序被和谐地整合一起，才能够得以实现）；
- 管理层的意志（管理层的职责是提供执行和管理网络安全计划所需的手段）；
- 财务（安全和防控措施的成本必须与面临的风险成比例）；
- 简明性、通用性和审慎行动（安全措施对于使用者来说，必须简明、灵活，易于理解，而且不具任何刺激性，不至招引潜在攻击）；
- 变化和连续性（安全机制必须随机应变，应随着时间的推移适应系统的改变和不断变化的需求及风险，同时系统必须保持恒定运行状态）；
- 评估，控制和调整（以确保安全水准与实际需求保持一致）。

IV.2.6 成功因素

IV.2.6.1 战略指导原则

安全战略的成功实施要求：

- 具有战略意志；
- 制定简明、准确、易懂和可行的安全策略；
- 发布安全策略；
- 对安全实行集中管理并在某种程度上实现安全程序的自动化；
- 所涉及的人员、系统和工具之间相互信任，人员人品高尚；
- 确立注册、监督和审计程序；
- 具有绝不损害资源的决心；
- 在国内和国际上均可实行的法律框架；
- 尊重法律约束力；

IV.2.6.2 针对互联网用户的指导原则

下列指导原则代表互联网用户可采纳的简明、经济和相对有效的措施，从而使其资源和电子活动更加安全[62]：

- 关掉未在用的计算机；
- 切勿打开陌生人发送的电子邮件；
- 使用定期更新的防毒软件做基本保护；
- 切勿泄露自己的密码，并频繁更换密码；
- 切勿在互联网上泄漏你自己或他人的个人数据；
- 切勿允许他人使用你的账户浏览互联网；
- 使用加密系统保护数据；
- 切勿访问不道德的网站和下载或传播非法程序或文档；
- 切勿在互联网上从事现实社会中明文禁止和受惩处的活动（欺诈、诽谤等等）；
- 切勿为自己拥有的保护水平洋洋得意；
- 切记正如我们的现实社会一样，互联网上任何一种活动都是个人所为，而且这一个人可能并不那么诚实可靠。

IV.2.6.3 保证电子邮件系统安全的指导原则

下列基本指导原则有助于保护电子邮件系统。

通过下列方式保护服务器：

- 使用防病毒软件；
- 利用某些参数配置标准（尺寸、添加附件等）过滤信息；
- 正确配置；
- 高效率管理，保证可用性；
- 避免默认的维护账户；
- 提供物理保护。

就用户而言：

- 安装、管理和强制使用防毒软件；
- 确定使用邮件系统的规则（切勿打开可执行的文档等）；
- 提高对潜在风险的意识；
- 获取恰当使用信息技术资源的承诺；
- 正确配置各用户的工作站和邮件应用程序；
- 使用电子邮件系统的安全版本；
- 针对机密信息使用加密程序并认证其来源。

---

62 摘自《互联网安全意识》（*Sentiment de sécurité sur Internet*），Anne-Sophie Perron撰写的的有关法律、犯罪和安全的硕士后毕业论文，2005年，洛桑。她曾在S. Ghernaouti-Hélie手下工作。

IV.2.6.4 保护互联网-内联网环境的指导原则

下列有关使用防火墙的基本原则将有助于保护互联网-内联网环境：

- 防火墙须能防止和防范未经授权的访问（带有安全操作系统的可信赖系统概念）；
- 所有流量（来访和出访）均必须通过防火墙经转；
- 只有经安全策略定义为有效和获得授权的流量，才可被允许穿过防火墙；
- 防火墙的配置必须保证能够过滤掉任何未经明确授权的东西；
- 防火墙不能够同时用作公司的网络服务器；
- 如果内部网络上的数据是极为敏感的数据，则必须通过一台不与内部网直接连接的机器访问互联网；
- 防火墙不能防范未经其经转的攻击和非法访问，而且对于防范来自公司内部的犯罪，亦毫无作用。

防火墙并非防毒软件，它也必须得到保护，防止病毒的感染。绝对地讲，每一个提供连接功能的系统（电子邮件服务器、通信服务器等）、每台包含数据（档案、数据库服务器等）的机器和每位用户的工作站，都必须配备防毒软件。

第五部分

附件

附件 A – 主要安全术语词汇表[63]

访问控制（Access control）

防止资源（一种服务、系统、数据或程序）被不恰当或未被经授权加以使用的机制。

事故（Accident）

给某一实体造成伤害的无法预见的事件。

主动攻击（Active attack）

篡改目标资源的攻击（影响其完整性、可用性、机密性）。

匿名（Anonymity）

其名称未知或有意不透露其名称的实体，这一特点使其能够在不被识别（假名）的情况下使用资源。应做出相关规定，尊重某些用户在互联网上发表声明时有确凿理由不愿暴露身份的意愿，以避免过多地限制他们的言论自由，鼓励他们自由发表个人观点和信息，确保其不会受到公共和私营实体在网上对其进行未经授权的监督。另一方面，司法和公安部门，在国家法律、《欧洲人权公约》和其它国际条约（如《网络犯罪公约》）的范围内，应有能力获取那些从事非法活动的人员的个人信息。

防病毒（Antivirus）

病毒检测程序。

资产（Asset）

具有一定价格的东西，而且对其所有者，它代表着某种形式的资本（敏感资产概念）。就安全而言，确定资产并按照其重要性加以分类十分重要，只有这样才能对资产采取必要的和充分的保护措施，从而避免丢失资产或至少将资产丢失带来的负面影响降至最低程度。

非对称密码算法（Asymmetric cryptographic algorithm）

基于密钥对使用的算法（一个密钥用于数据加密，另一个用于解密）。

攻击（Attack）

针对个人或资源所采取的并造成伤害的袭击、入侵或行动。现实中存在不同类型的计算机关联攻击。

---

63 选编自S. Ghernaouti-Hélie著《信息安全与网络：正确的途径与方法》（*Securité informatique et réseaux, cours et exercices corrigés*）的词汇表，2006年，Dunod。

可审计性（Auditability）

为实现分析和审计的目的，一个应用环境自身可被进行分析的程度。

审计员（Auditor）

从事审计工作的人员。

认证（Authentication ）

认证权限的行为。认证用于确认（或驳回）一项行动、一条声明和一条信息的真实性（原始的、真正的）。认证特别用于核实一个实体的身份，保证该实体与此前其记录在案的身份相匹配。

真实性（Authenticity）

具有真实性的特性。这一特性是对正确性的证实或认证。经常是用来表明一种事实，即一条信息或一个事件未被改动，修改或伪造，而且确系由自称为原创者的实体制做。

管理机构（Authority）

行使特定职能的权力机构，一般指负责发放数字证书的机构。

授权（Authorization）

授权、允许、给予权利的行为，允许采取某些行动、授予权利、获得一项服务、信息、系统等的访问权。

可用性（Availability）

资源可被获得和使用，以满足相关要求的（不得拒绝经授权许可的对系统、服务、数据、基础设施等的访问。）安全标准。

后门，陷门（Backdoor, trapdoor）

通常指软件中所编入的代码的一部分，使未经授权的实体在所有者不知情的情况下，控制其系统，拷贝其信息等。

备份计划（Backup plan）

所预见的一套技术和操作手段，确保无论碰到任何问题，均能保证信息的可持续性和各项活动的连续性。

破坏（Breach）

由入侵或攻击行为造成的影响或性能劣化，其影响可以是：有形的（物理或材料的改变、逻辑功能失常、程序混乱等）；逻辑上的（无可用性、丧失完整性、泄密）；战略上的（尤其涉及财务，在托管、运输、电信、专业技术、硬件和软件的采购/租用、人事、外包、运营损失（利润率、现金流、客户损失）、资金或货物损失等诸多方面带来额外的成本。）。

缺陷（Bug）

一种程序设计错误，以此类比，由功能故障反映出的概念或实施上的缺陷。

证书，公共密钥证书（Certificate, public-key certificate ）

由认证管理机构（值得信赖的第三方）发放的一套数据，用于提供安全服务（机密、认证、完整性）。数字证书使用公共密钥加密，证书中包含主体的公共密钥数值，由认证管理机构发放的证书加以证实。

认证管理机构（CA）（Certification Authority (CA)）

负责制定、签署和发布公共密钥证书的值得信赖的第三方。

首席安全官(CSO)（Chief security officer (CSO)）

负责信息技术系统安全的官员。

密码（Cipher）

用于将明文转换为密文的加密算法。

密文（Ciphertext）– 见密报

合规性（Compliance）

符合、遵照和遵从标准。

机密性（Confidentiality）

保守信息和交易的秘密，其性质是机密的。保密的目的是防止信息透露给未经授权的第三方，保护信息在存储、处理或传输过程中，均不会被有意或无意被他人读取、偷听和非法拷贝（数据机密性概念）。

“小甜饼”（网络跟踪器）（Cookies）

访问某些网站时，在互联网用户不知情的情况下写入其硬盘的文档，用于收集有关用户的数据，主要是为了定制提供的网络服务。

对策（Countermeasure）

系统的安全功能、措施、程序或机制，旨在减少系统的薄弱环节，在威胁变成现实之前进行反击。

密码分析（Cryptanalysis）

用于分析以往加密信息的一套方法，以便对其进行解密，因此密码分析也被称为“解码”。加密系统越强健，密码分析就越困难。

密报，密文（Cryptogram, ciphertext）

已被转换为密码的数据；加密的数据、文本或信息；通过加密获得的数据。

密码算法（Cryptographic algorithm）

用于数据加密的算法，使数据具有保密性，以数学函数和加密密钥为基础。

密码期限（Cryptographic period）

系统密钥未发生变化的时间段。

密码术（Cryptography ）

用于编写信息的一种数学应用，其方式是使该信息对于那些没有办法解密的人来说无法辨认。见加密。

DDoS（分布式拒绝服务）（distributed denial of service）

几个系统同时发起的一种饱和（或拒绝服务）攻击。

摘要（Digest）

当散列函数被用于一系列数据时所形成的字符串。

数字签名（Digital signature ）

类同于手写签名，通过非对称加密算法获得的数字签名，用以认证信息的发送人并确保信息的完整性。

直接损失（Direct losses）

由安全缺陷直接造成的可确认的损失。

劝阻（Dissuasion ）

用于威慑恶意攻击者实施攻击的方式，向他们说明，他们从中得到的收益与被他们威胁要攻击的系统遭受的损失相比是微不足道的。

DoS（拒绝服务）（denial of service）

一种饱和攻击，旨在造成被攻击目标的瘫痪，使其不能再按照预期的要求运行。

效率（Efficiency）

能达到预期效果并产生有益结果的质量。能发挥应有作用并具备保护资源的真实能力的安全措施所具有的特点。

应急计划（Emergency plan）

所预见的一套技术和组织方法，旨在以最佳的方式应对所发生的、给机构带来危害并影响其顺利运行的严重事件。

加密，编密码（Encryption, encipherment）

为保证机密性而对数据进行的密码转换（密报）。加密旨在使数据对于那些没有解密密钥的人无法读懂。使用算法和密钥可以对明文进行加密，以便创建密文，而后者又可以借助相对应的解密密钥进行解密（某些不可逆转的加密除外）。加密的反向操作为解密或解密码。

道德（Ethics）

有关是与非的行为准则。一套由某个群体采用的道德法则。

故障（Failure）

功能失灵、失效，使资源无法被使用。

防火墙（Firewall）

用以隔离或掩蔽资源、过滤数据、控制流量的硬件或是软件，以保护与互联网连接的机构内部信息环境。

点火（恶意攻击）（Flaming）

一种发送大量不良信息以诋毁某个讨论群体声誉的专门技术。

泛洪攻击（Flooder）

一种恶意程序，用以降低接入服务提供商与互联网用户之间的通信速度或切断用户的连接。

非法闯入，黑客（Hack, hacker ）

非法闯入某个系统的行为。未经授权许可、不合法地闯入他人系统的个人（无论出于何种原因）。这种攻击或被动，或主动。

非法闯入（Hacking）

用于破坏信息技术系统的一系列操作工作。

散列函数（哈希函数）（Hash function）

在加密中，此函数亦被称作摘要函数。该函数从信息数据入手，产生一个信息摘要，即，一种比原有信息更短和无法理解的数字指纹。然后利用发送者的专用密钥进行加密，附在将发送的信息后面。在收到这一信息及其指纹时，接收者利用发送者的公共密钥对指纹进行解密，再使用同样的散列函数重新计算所收到信息中的指纹，然后将结果与所收到的指纹进行对比。如果对比后结果相同，则接收者已核实发送者的身份，且确定信息完整，因为即使信息只被稍加改动，其指纹亦会大为改变。

识别，身份确定（Identification）

借助这一过程可以认出此前已经识别的实体。

身份（Identity）

如可能，在域名中以独一无二的明确方式认定和判别一个具体实体时所采用的信息。

影响（Impact）

表示攻击造成的后果的程度（**财务影响**：攻击造成的成本；**逻辑影响**：对可用性、完整性、机密性的破坏；**战略影响**：危害机构的生存；**有形影响**：真正的、直接的、可以观察到的影响）。

影响的严重性（Impact gravity）

通过某一事件的发生频率对其严重性所做的评估。对影响的严重性进行量化非常重要，以便能够准确地确定安全需求，并明确其轻重缓急，例如：无影响或可忽略的影响（0）、影响轻微（1）、较大影响（2）、严重影响（3）、灾难性影响（4）。

可归责性（Imputability）

在某一特定时间将某一项行动明确地追查归责到一个具体使用者身上的品质。实际上，此为查清违规事件由谁负责的能力。

间接损失（Indirect losses）

由安全缺陷间接导致的损失。

完整性（Integrity）

某物原封未动的状态。如果安全标准得到遵守，则可以确保资源未经授权不得改动（修改或毁坏）。

内联网（Intranet）

利用互联网技术构建的机构内部的专用网络，通常利用防火墙与互联网隔离开来。

入侵发现系统（IDS）（Intrusion detection system （IDS））

用于发现安全策略违规事件和诊断潜在破坏行为的系统。

IPSec（互联网协议安全）（Internet Protocol security）

一种能够提供安全服务的 IP 版本。IPSec 在公共互联网上开启两位通信者之间的一个逻辑通信信道（IP 隧道）。信道的两端已得到认证，其间传输的数据可以进行加密（加密信道或虚拟网络概念）。

IPv6（互联网第6版本协议）（Internet Protocol version 6）

IPv4 的升级版，特别包含了执行安全服务的内置机制（源实体和目的地实体的认证，所传输数据的机密性）。

密钥（Key）

加密或解密用的密钥，通常为一个用于加密算法的数学数值。除非公开，否则加密密钥不得对外透露：密钥是保护另一个秘密（为保证其机密性而经过加密的信息）的保密手段。

密钥管理（Key management）

加密密钥的管理。依照安全策略对密钥进行生成、发放、归档和销毁的工作。

逻辑炸弹（Logic bomb）

由某个具体事件（如生日日期）触发的一种恶意程序，意在破坏其所在的系统。

基本服务丢失（Loss of essential service）

一个系统或机构正常运行所需的资源全部或部分地无法使用或出现故障。

恶意行为（Malevolent）

有意破坏机构资源的敌对行为，可以由机构内部或外部的人员直接或间接地参与实施（盗窃硬件、数据，泄露机密信息，违法破坏等）。

恶意软件（Malware）

对诸如病毒、蠕虫或特洛伊木马，或其它类型的或多或少独立行动的攻击软件程序的一个统称。

伪装程序（Masquerade）

基于系统诱饵的攻击类型。

不可否认性（Non-repudiation）

防止信息发送者事后否认曾发送过此信息或有过此行为的能力；能够保证可以拿出提交给第三方的证据，并用于证明此事件或行为确有发生。能证明某条信息是由某人在特定时间发出的、而且事后未经修改的证据。这类证据应能由第三方在任何时间加以核实。如果没有不可否认性的要求，信息的发送者和接收者可能会否认他们发送过或接收过所述信息。

不可选择（No-opt）

一种客户对自身信息将被如何使用无法做出选择的服务（有可能他们的数据隐私权将受到侵犯）。

公证（Notarization）

对用作证据的数据进行登记。

单向散列函数（One-way hash function）

一种可以计算数据指纹、但不能生成带有特定指纹数据的函数。这一函数必须避免产生冲突，即：由不同的信息生成同样的特征。

被动攻击（Passive attack）

不改动目标的攻击（被动监听，泄密）。

密码（Password）

在要求访问某一资源的认证过程中，经授权的用户出具的、证明其身份的保密信息。

补丁（Patch）

旨在修补软件安装后所发现的缺陷的软件更新程序。

渗透测试（Penetration tests）

用于分析和测试系统受保护的程度和安全机制的强健性。

窃用电话（飞客）（Phreaking）

由个人或运营商承担费用的、对电信服务的非法使用或误用（由电话窃贼（飞客）实施）。

预防（Prevention）

为规避危险或风险所采取的一套措施，旨在出于保护的目的，防止威胁变为现实并减少事件的发生频率。

隐私权保护（Privacy protection）

保护性措施，用以保证有关互联网用户活动的信息不被泄露给无关系的各方，同时保证信息用途不超出信息所有者同意的界限。在此系指个人有权核实有关他们自身的信息。通过观察用户在互联网上的行为方式和他们所访问过的网站可以直接或间接地收集有关他们的信息。

专用密钥（私钥）（Private key）

属于某个实体而且必须加以保密的、在非对称加密机制（公共密钥加密）中使用的密钥。

特权管理基础设施（PMI）（Privilege-management infrastructure（PMI））

支持对特权、授权和清除加以管理的基础设施。

保护（Protection）

保护的行为，被保护的状态，属于一种安全措施，有助于发现、抵消或减少攻击带来的影响。

公共密钥（公钥）（Public key）

通常而言，在非对称密码中，一个实体的公钥必须提供给打算向其发送加密数据的人，以便于可以利用相对应的私钥对这些数据进行解密。

公共密钥密码（Public-key cryptography）

一种使用两个密钥密码或一对密钥的非对称加密体系：一个是保密的私钥，另一个是可对外公开的公钥。两个密钥互为补充，不可分离。同时也不可能利用二者之间的数学关系计算出私钥。

公共密钥基础设施（PKI）（Public-key infrastructure（PKI））

支持实施非对称（公钥）加密，特别包括加密密钥和数字证书管理与分发的基础设施。

可靠性（Reliability）

系统在一定时期内无任何事件发生、正常运转的能力。

否认性（Repudiation）

否认自己全部或部分地参与了某一交流活动的事实。

撤销（Revocation）

有关私钥已经丧失其完整性的通知。相对应的公钥证书不可继续使用。就合同而言，亦系指收回或接受某个要约的权利。

风险（Risk）

以概率和影响衡量的、将变为现实的威胁的相对可能性。

风险分析，风险评估（Risk analysis, risk assessment）

识别和评估风险的过程（对其发生和带来影响的概率进行估算）。

风险管理（Risk management）

由一家机构对风险进行不断分析的过程，旨在控制风险并将其限制于一个可接受的水平。可以被用于确定最适于保护机构资产的安全策略。

蓄意破坏（Sabotage）

恶意行为、野蛮破坏、有意损害，旨在妨碍机构、基础设施、服务或资源的正常运行。可导致产生损失。

安全性（Safety）

无损害的品质。

安全套接层（SSL）（Secure sockets layer （SSL））

由 Netscape 开发、并得到市场上多数网络浏览器支持的一种使互联网上交流实现安全性的软件。

安全（Security）

某人或某物无危险困扰的情形。旨在防范有害事件或限制其影响的机制。例如，**物理安全**系指在物理或物质方面保护环境所采取的措施，而**逻辑安全**则系指软件程序和保护手段。

安全管理员（Security administrator）

负责确立和实施全部或部分安全策略的个人。

安全审计（Security audit）

对一家机构为保护其环境所使用的所有涉及安全的成份 — 参与者、策略、措施、解决方案、程序和手段，进行有计划的分析，其目的在于监督合规性、评估所部署的组织、技术、人力和财物资源与发生的风险是否匹配，并使绩效得到优化、合理化和加强。

安全措施（Security measures）

为了满足安全策略制定的安全目标所采用的各种技术、组织、法律、财务、人力和程序资源以及行动方式，通常按照它们各自的职能作用加以分类（预防措施、保护措施、威慑措施等）。

安全需要（Security need）

针对需要保护的环境，与需要保护的资源和价值相关的可用性、完整性和机密性程度的确定和表达。

安全策略（Security policy）

由机构确立的安全参考框架，其中反映出其安全战略和制定的实施方法。

敏感性（Sensitivity）

一个说明其价值或重要性的实体的特点。

会话密钥（Session key）

通信方开始工作会话时利用非对称加密体系生成的密钥，其寿命期仅限于该会话时段。该密钥利用对称加密算法对大量数据进行加密。

安全版-http （S-http）

http 协议的安全版本，能够使客户与网络服务器间能进行安全的交流。

嗅探程序（Sniffer ）

用于窃听网上传输中数据的软件。

嗅探（Sniffing）

一种被动窃听行为，目的是为了大量获取连接参数，然后在其合法所有者不知情的情况下利用它们从事未经授权的违法活动。

社交工程（Social engineering）

恶意攻击者所使用的技巧、程序和措施，通常是利用用户轻信的心理，专门获取用户的密码和连接参数，并窃取他们的数字身份，以便冒充经授权的访问者戏弄和损坏用户的系统。

垃圾邮件制造者（Spammer）

系指制作或发送垃圾邮件的人。

滥发邮件（Spamming）

用于向某个电子信息系统大量发送推介性信息的专门技术。

电子欺骗者（Spoofer）

从事电子欺骗的个人。

电子欺骗（Spoofing）

用于窃取 IP 地址、从而破坏系统的专门技术。

间谍软件（Spyware）

用于将敏感信息从受感染的计算机发送至攻击者的程序。

隐写术（Steganography）

用于将一条信息隐藏于另一条信息的、以便对其进行隐蔽传输或存储的专门技术。水印是一种在图像里暗藏持久印记的隐写应用。

威胁（Threat）

某种危险的迹象、征兆、预兆。极有可能发生的、并转变为对环境或资源的攻击及对安全的破坏的行动或事件。

流量分析（Traffic analysis）

对源实体与目的实体间信息流的观察和研究（在线、缺席、数量、方向、频率等）。

陷门（Trapdoor）– 见后门

特洛伊木马（Trojan horse）

隐藏在合法程序中的一种恶意程序，为劫持系统而潜入系统之中（窃用处理器时间、损坏、篡改和破坏数据及程序、造成功能故障、窃听等）。

信赖（Trust）

有保证的依赖某人或某物（一种定性的、主观的、高度相对的标准）。

用户宪章（User charter）

由机构起草的文件，具体列明其员工在使用该机构为他们提供的信息技术和电信资源时所享有的权利、义务和职责，并由各相关方签字。

用户简表（User profile）

为进行访问控制和计费而制定的用户特征列表，有助于管理用户所连接的网络和系统（识别和认证参数、访问权利、授权及其它有用信息等）。

虚拟专用网络（VPN）

该概念系指利用 IPsec 在无安全保证的公共网络上，开通一条安全的专用通信信道，经常被机构用于通过互联网连接其不同办公地点，同时又能保证数据交流的机密性。

病毒（Virus）

在用户不知情的情况下潜入系统的恶意程序，该程序具有自我复制能力（以同样的形态，或通过变异变成多形病毒），毁坏它们被执行时所处的环境，并感染它们所接触到的其它用户。不同种类病毒的不同之处在于其签名、行为方式、自我复制方式、感染机器的方式、所造成的故障等。**蠕虫、特洛伊木马**和**逻辑炸弹**均是属于普通病毒系列的恶意代码。

薄弱环节（Vulnerability）

可以导致有意或无意地违反安全策略的安全缺陷。

附件 B – 可作为安全管理参考的ISO/IEC 17799:2005标准目录

引言
0.1 什么是信息安全?
0.2 为什么需要信息安全?
0.3 如何确立安全需求
0.4 安全风险评估
0.5 选择控制
0.6 信息安全的起点
0.7 关键成功因素
0.8 制定自己的指导原则
1 范围
2 术语和定义
3 此标准的结构
3.1 条款
3.2 主要安全类别
4 风险评估和处理
4.1 评估安全风险
4.2 处理安全风险
5 安全策略
5.1 信息安全策略
5.1.1 信息安全策略文件
5.1.2 信息安全策略的审议
6 信息安全的组织
6.1 内部组织
6.1.1 信息安全的管理承诺
6.1.2 信息安全的协调
6.1.3 信息安全的职责划分
6.1.4 信息处理设施的授权程序
6.1.5 保密协议
6.1.6 与有关管理机构的联系
6.1.7 与特殊利益集团的联系
6.1.8 信息安全的独立审查
6.2 外部各方
6.2.1 确定与外部各方相关的风险
6.2.2 涉及客户时的安全问题的处理
6.2.3 在第三方协议中解决安全问题
7 资产管理
7.1 资产的责任制
7.1.1 资产库存
7.1.2 资产所有权
7.1.3 资产的可被接受的使用
7.2 信息分类
7.2.1 分类的指导原则
7.2.2 信息的标注和处理

8 人力资源安全
- 8.1 就业前
  - 8.1.1 角色和职责
  - 8.1.2 筛选
  - 8.1.3 就业的条款和条件
- 8.2 就业期间
  - 8.2.1 管理责任
  - 8.2.2 信息安全的意识、教育和培训
  - 8.2.3 奖惩程序
- 8.3 就业的终止或变更
  - 8.3.1 终止的责任
  - 8.3.2 资产的退还
  - 8.3.3 访问权的取消

9 物理和环境安全
- 9.1 安全区域
  - 9.1.1 物理安全防线
  - 9.1.2 物理门禁控制
  - 9.1.3 保证办公室、房间和设施的安全
  - 9.1.4 防范外部和环境方面的威胁
  - 9.1.5 在安全区域里工作
  - 9.1.6 公共访问、交付和装载区域
- 9.2 设备安全
  - 9.2.1 设备的选址和保护
  - 9.2.2 支持设施
  - 9.2.3 布缆安全
  - 9.2.4 设备维护
  - 9.2.5 外部设备的安全
  - 9.2.6 设备的安全处置或再利用
  - 9.2.7 财产的搬运

10 通信和运营管理
- 10.1 运营程序和职责
  - 10.1.1 文件记载的运营程序
  - 10.1.2 变更管理
  - 10.1.3 职责的划分
  - 10.1.4 开发、测试和运营设施的分离
- 10.2 第三方服务交付的管理
  - 10.2.1 服务交付
  - 10.2.2 监督和审查第三方的服务
  - 10.2.3 管理第三方服务的变更
- 10.3 系统规划和验收
  - 10.3.1 能力管理
  - 10.3.2 系统验收
- 10.4 防范恶意和移动代码
  - 10.4.1 对恶意代码的控制
  - 10.4.2 对移动代码的控制

10.5 备份
10.5.1 信息备份
10.6 网络安全管理
10.6.1 网络控制
10.6.2 网络服务的安全
10.7 媒介处理
10.7.1 可搬动媒介的管理
10.7.2 媒介的处置
10.7.3 信息处理程序
10.7.4 系统文件的安全性
10.8 信息交流
10.8.1 信息交流政策和程序
10.8.2 交流协议
10.8.3 经转中的物理媒介
10.8.4 电子消息处理
10.8.5 业务信息系统
10.9 电子商务服务
10.9.1 电子商务
10.9.2 在线交易
10.9.3 向公众公开的信息
10.10 监督
10.10.1 审计日志
10.10.2 监督系统的使用
10.10.3 日志信息的保护
10.10.4 管理员和操作员日志
10.10.5 故障日志
10.10.6 时钟同步
11 访问控制
11.1 访问控制的业务需求
11.1.1 访问控制政策
11.2 用户访问管理
11.2.1 用户注册
11.2.2 特权管理
11.2.3 用户密码管理
11.2.4 用户访问权的审查
11.3 用户的职责
11.3.1 密码的使用
11.3.2 无人值守的用户设备
11.3.3 清除桌面和清除屏幕的政策
11.4 网络访问控制
11.4.1 关于网络服务使用的政策
11.4.2 针对外部连接的用户认证
11.4.3 网络中设备的识别
11.4.4 远程诊断和配置端口的保护
11.4.5 网络的分隔
11.4.6 网络连接控制
11.4.7 网络路由控制

- 11.5 操作系统的访问控制
  - 11.5.1 安全的登录程序
  - 11.5.2 用户识别和认证
  - 11.5.3 密码管理系统
  - 11.5.4 网络设施的使用
  - 11.5.5 会话超时
  - 11.5.6 连接时间的限制
- 11.6 应用和信息的访问控制
  - 11.6.1 信息访问限制
  - 11.6.2 敏感系统的隔离
- 11.7 移动计算和远程办公
  - 11.7.1 移动计算和通信
  - 11.7.2 远程办公

12 信息系统的获取、开发和维护

- 12.1 信息系统的安全需求
  - 12.1.1 安全需求的分析和规范
- 12.2 应用中的正确处理
  - 12.2.1 输入数据的验证
  - 12.2.2 内部处理的控制
  - 12.2.3 信息的完整性
  - 12.2.4 输出数据的验证
- 12.3 密码控制
  - 12.3.1 有关密码控制的使用政策
  - 12.3.2 密钥管理
- 12.4 系统文档的安全性
  - 12.4.1 操作软件的控制
  - 12.4.2 系统测试数据的保护
  - 12.4.3 程序源代码的访问控制
- 12.5 开发和支持程序的安全性
  - 12.5.1 变更控制程序
  - 12.5.2 操作系统变更后对应用程序的技术审查
  - 12.5.3 对软件包变更的限制
  - 12.5.4 信息泄漏
  - 12.5.5 外包的软件开发
- 12.6 技术薄弱环节的管理
  - 12.6.1 对技术薄弱环节的控制

13 信息安全事件的管理

- 13.1 报告信息安全事件及其弱点
  - 13.1.1 报告信息安全事件
  - 13.1.2 报告安全弱点
- 13.2 信息安全事件的管理和改进
  - 13.2.1 职责和程序
  - 13.2.2 从信息安全事件中吸取教训
  - 13.2.3 收集证据

14 业务连续性的管理

14.1 业务连续性管理的信息安全问题

14.1.1 将信息安全纳入业务连续性管理程序

14.1.2 业务的连续性和风险评估

14.1.3 制定和实施包括信息安全在内的连续性规划

14.1.4 业务连续性规划框架

14.1.5 试验、保持并重新评估业务连续性规划

15 合规性

15.1 遵守法律要求

15.1.1 确定适用的立法

15.1.2 知识产权（IPR）

15.1.3 组织机构纪录的保护

15.1.4 数据保护和个人信息的隐私权

15.1.5 避免对信息处理设施的滥用

15.1.6 密码控制的监管

15.2 遵守安全策略和标准以及技术要求

15.2.1 遵守安全策略和标准

15.2.2 检查是否符合技术要求

15.3 信息系统审计方面的考虑

15.3.1 信息系统的审计控制

15.3.2 信息系统审计工具的保护

参考文献和索引

附件 C – ITU-D在网络安全和打击垃圾邮件方面的职责

欲了解更多信息，请访问：
www.itu.int/ITU-D/cybersecurity

本“网络安全与打击垃圾邮件计划”的重点工作和行动与信息社会世界峰会（WSIS）《日内瓦行动计划》和《突尼斯议程》的合力几乎可以一一对应（如下表所示）。2005 年的《突尼斯议程》将国际电联确定为牵头机构，以推进和协调实施《日内瓦行动计划》中有关树立使用 ICT 的信心和提高安全性方面的行动。在 2006 年 3 月召开的“国际电联世界电信发展大会”上通过的《多哈行动计划》中，各成员决定，网络安全和打击垃圾邮件是项目 3 的重中之重。

WSIS C.5行动方面（树立使用ICT的信心和提高安全性）与国际电联在网络安全和打击垃圾邮件方面的职责

WSIS C.5行动方面	国际电联与C.5相关的职责
12. 信心和安全是信息社会的主要支柱。	处理人们关注的网络安全方面的问题，以实现网络提供安全和可接入电子服务应用的潜力。
a) 促进各国政府在联合国的合作以及与所有利益攸关方在其它相关论坛的合作，以增强用户信心，建立信任并保护数据和网络的完整性；考虑信息通信技术目前所面临的威胁和潜在威胁；并解决其它信息安全和网络安全问题。	为最大限度地降低、防止和发现网络威胁，有必要进一步促进相关工作的范围并展开合作，从而支持有关网络安全信息的收集和传播工作，同时通过交流最佳做法，实现成员以及政府、企业与民间团体之间有效的相互帮助，相互沟通和工作恢复。
b) 各国政府应与私营部门合作，通过以下方式防止、发现和应对网络犯罪和对信息通信技术的不当使用：在考虑到这些领域持续开展的工作的基础上制定指导方针；考虑制定有利于有效查处不当使用的立法；加强有效互助；强化国际层面对此类事件的防范、发现和恢复工作提供的机构支持；鼓励开展教育，提高认识。	制定有关网络安全的导则、规划工具和手册。 为政策制定机构及其它相关部门创建网络安全工具包。 帮助成员国制定与预防网络犯罪有关的法律和示范性立法。 为落实网络安全，制定有关技术战略和技术发展的培训材料。

WSIS C.5行动方面	国际电联与C.5相关的职责
c) 各国政府和其它利益攸关方应积极加强对用户的教育，提高对网络私密性和保护隐私方法的认识。	帮助人们提高认识，明确关键问题所在，以支持培育网络安全文化，同时推荐能够支持 ICT 应用和尽量减少网络威胁的最佳做法范例。
d) 在国家和国际层面对垃圾信息采取适当行动。	就垃圾邮件和网络威胁（包括应对措施）达成共识。 酌情考虑到其它利益攸关方的工作：经济合作与发展组织（OECD）以及关于网络安全和垃圾邮件的主要协议的缔约国。
f) 利用信息通信技术使用安全领域内的互补和相互强化举措以及针对隐私权、数据和消费者权益保护的举措或指导方针，进一步加强信任和安全框架。	确定网络安全要求，并就部署安全的 ICT 应用提出解决方案。 帮助人们提高认识，明确关键问题所在，以支持培育网络安全文化，同时推荐能够支持 ICT 应用和尽量减少网络威胁的最佳做法范例。
g) 分享信息安全和网络安全领域的有效做法，并鼓励所有相关各方采纳这些做法。	开发工具，以方便有关技术和政策议题及网络安全最佳做法方面的信息共享。 成为区域和区域间合作的推动者，并对在区域层面开展的相关能力建设工作给予支持。

WSIS C.5行动方面	国际电联与C.5相关的职责
h) 请有关各国建立事件实时处理和响应联络点，并在这些联络点之间搭建一个合作网络，以便共享应对事件的信息和技术。	行动可包括在感兴趣的成员国之间达成有关加强网络安全的谅解备忘录（MoU）等。 实施利益攸关多方的全球性项目[...]，提供多个领域的解决方案，其中包括： 1) 成立国家联络点。 2) 突发事件的响应、监控和预警。 审议建立和运作监控、预警和突发事件响应及恢复能力方面的最佳做法，各成员国可以使用这些最佳做法建立其国家能力。
i) 鼓励进一步开发有助于在线交易的安全可靠的应用。	确定网络安全要求，并就部署安全的 ICT 应用提出解决方案。
j) 鼓励相关国家对联合国正在进行的树立信息通信技术使用信心并提高其安全性的工作做出积极贡献。	邀请国际电联成员国、部门成员和部门准成员： – 就 ITU-D 第 1 研究组本议题提交文稿，并参与电信发展局正在进行的项目活动； – 通过从事《日内瓦行动计划》第 12[64]段列出的活动，帮助在国家、区域和国际层面树立使用 ICT 的信心并提高安全性。

64 第12段即为WSIS行动方面C.5的全文，已在本文件第1列中列出。

ITU-D 在网络安全和打击垃圾邮件方面的职责

在国际电联成员国于 2002 年和 2006 年国际电联全权代表大会（PP02 和 PP06）与 2002 年和 2006 年世界电信发展大会（WTDC-02 和 WTDC-06）所通过的决定框架内，ITU-D 在网络安全、网络威胁和打击垃圾邮件方面的职责被涵括在以下决定之中：

1. WTDC-2002 和 2006 项目 3 – 信息通信战略与 ICT 应用。

2. WTDC-2006 第 45 号决议 – 关于加强在网络安全、打击垃圾邮件等领域的合作机制。

3. WTDC-2006 第 2 号决议附件 2 – ITU-D 第 1 研究组第 22 号课题 – 保证信息与通信网络安全 – 培育网络安全文化的最佳做法。

4. 第 130 号决议（2006 年，安塔利亚，修订版） – 加强国际电联在树立使用信息通信技术的信心和提高安全性方面的作用。

1. WTDC-2006《多哈行动计划》项目 3（信息通信战略和 ICT 应用）

重点

a. 在本项目中有必要解决与电子服务/应用有关的安全隐患，以便充分发挥网络的潜力，提供安全和可以获得的电子服务和应用。

b. 该项目应就垃圾邮件和网络威胁（包括应对措施）问题达成共识。

c. 为最大限度地降低、防止和发现网络威胁，有必要进一步促进相关工作的范围并展开合作，从而支持有关网络安全信息的收集和传播工作，同时通过交流最佳做法，实现成员以及政府、企业与民间团体之间有效的相互帮助，相互沟通和工作恢复。

d. 电信发展局也应成为区域和区域间合作的推动者，并对在区域层面开展的相关能力建设工作给予支持。

e. 其中可特别包括在感兴趣的成员国之间达成有关加强网络安全的谅解备忘录（MoU）等。

任务

a. 制定有关网络安全的导则、规划工具和手册。

b. 为政策制定机构及其它相关部门创建网络安全工具包。

c. 为落实网络安全，制定有关技术战略和技术发展的培训材料。

d. 组织讲习班、会议和研讨会，讨论网络安全的技术、政策及法律和战略问题。

e. 帮助成员国制定与预防网络犯罪有关的法律和示范性立法。

f. 确定网络安全要求，并就部署安全的 ICT 应用提出解决方案。帮助人们提高认识，明确关键问题所在，以支持培育网络安全文化，同时推荐能够支持 ICT 应用和尽量减少网络威胁的最佳做法范例。

g. 开发工具，以方便有关技术和政策议题及网络安全最佳做法方面的信息共享。

h. 酌情考虑到其它利益攸关方的工作：经济合作与发展组织（OECD）以及关于网络安全和垃圾邮件的主要协议（例如《伦敦行动计划》和《首尔-墨尔本反垃圾邮件谅解备忘录》）的缔约国。

2. WTDC-2006 第 45 号决议 – 关于加强在网络安全、打击垃圾邮件等领域的合作机制（摘录）

忆及

大会对项目 3（信息通信战略和 ICT 应用）的基本支持，确认项目 3 在《突尼斯议程》C5 行动方面（树立使用信息通信技术的信心和提高安全性）负主要责任；

注意到

有关网络安全的世界电信标准化全会（WTSA)（2004 年，弗洛里亚诺波利斯）第 50 号决议仅限于对减少这种现象影响的技术问题进行研究；

敦促成员国

为落实本决议提供必要的支持，

做出决议

责成电信发展局主任

a) 结合项目 3 并根据各成员提交的文稿，组织成员国和部门成员会议，讨论如何增强网络安全，包括在感兴趣的成员国之间达成一项《关于打击垃圾邮件和网络犯罪的谅解备忘录》；

b) 向全权代表大会（2006 年，安塔利亚）汇报这些会议的结果。

第 45 号决议的输出成果：关于加强在网络安全和打击垃圾邮件方面合作的项目

电信发展局在项目 3 的协调之下，开发一个利益攸关多方的全球性项目，将现有举措综合联系一起，以解决发展中国家的需求。

该项目计划于 2007 年启动，将着重为下列领域提供解决方案：

1. 强大的立法
2. 制定技术措施
3. 建立业界合作伙伴关系，尤其是与互联网服务提供商、移动运营商和直接营销协会
4. 教育消费者和业界参与者，使其了解有关反垃圾邮件的措施及互联网安全实践

5. 在政府、业界、消费者、企业和反垃圾邮件集团之间开展国际合作，以便以一种全球协调的方式解决该问题。

除上述领域之外，在讨论和演讲的过程中，下列领域（排名不分先后）亦被认为对于成员国的合作和帮助非常重要。在此方面，ITU-D 可以与在网络安全和打击垃圾邮件领域具有公认专业知识的相关实体进行合作：

a. 建立基本的意识

b. 制定适当的国家立法

c. 人和机构的能力建设

d. 实施（能力建设领域）

e. 有关网络安全的国家政策和战略

f. 国家和其它利益攸关方之间的信息交流

g. 国家联络点的建立

h. 现有举措的进展监督与评估

i. 突发事件的响应、监测与预警

j. 网络安全薄弱环节与威胁的评估

k. 网络与网络安全的有效工具及应用

l. 合作伙伴关系

m. 国际合作

有关此项目：

– 题为“关于加强网络安全和打击垃圾邮件方面合作的项目”，将于 2007 年启动，为期 4 年，并将成为电信发展局《2007 年运作规划》的一部分。

– 在每年国际电联理事会会议上，将就其实施过程中取得的进展向该会议提交年度报告。

– 本项目在实施过程中将考虑 WTDC06 有关发展部门在网络安全和打击垃圾邮件方面的职责的决定。

– 本项目的主要目的是为发展中国家在会议确认的对网络安全和打击垃圾邮件合作极为重要的领域提供帮助。

– 有关立法方面，在帮助发展中国家制定符合《网络犯罪公约》的国家立法时，应酌情考虑到欧洲理事会的相关工作。

– 本项目框架下各项活动的实施，应由各国明确请求，重点应放在发展中国家。

– 本项目开发完毕之后，应呈交潜在的融资实体，包括成员国、私营部门和国际组织（例如世界银行和欧洲委员会）。

3. WTDC-2006 第 2 号决议 – ITU-D 第 1 研究组第 22 号课题 – 保证信息与通信网络安全 – 培育网络安全文化的最佳做法

a) 对有关下列问题的意识进行调查、制定目录、予以说明并提高这些方面的意识：

- 国家政策制定机构在与其它利益攸关方一道建立网络安全文化时面临的主要问题；
- 与建立网络安全文化有关的信息与帮助的主要来源；
- 国家政策制定机构与其它利益攸关方一道组织网络安全工作和培育安全文化过程中所采用的成功的最佳做法；
- 发展中国家在解决网络安全问题方面所面临的独特挑战以及应对这些挑战的最佳做法。

b) 审议建立和运作监控、预警和突发事件响应及恢复能力方面的最佳做法，各成员国可以利用这些最佳做法建立其国家能力。

就上述第 3 a)节列出的各项问题向成员国提交一份或多份报告。这些报告应该反映，安全的信息通信网络对于建设信息社会和各国的社会经济发展是不可或缺的。

4. 第 130 号决议（2006 年，安塔利亚，修订版） – 加强国际电联在树立使用信息通信技术的信心和提高安全性方面的作用

做出决议

按照国际电联的能力和技术专长，在其内部重点开展这一工作，

责成秘书长和三个局主任

1 审议：

i) 国际电联和其他相关组织迄今所做的工作，以及为了树立使用 ICT 的信心和提高安全性而采取的应对目前和未来威胁的各项举措，例如打击垃圾邮件问题；

ii) 根据国际电联《公约》和《组织法》，在顾问组的协助下，审查在落实本决议以及国际电联发挥 WSIS C5 行动方面协调方/推进方作用方面所取得的进展；

2 根据 WSIS 有关所有国家普遍和非歧视地享用 ICT 的条款，推动对所需工具的使用，以便增强各成员国对使用 ICT 的信心并提高安全性；

3 继续将网络安全通道（Cybersecurity Gateway）作为向全世界传播国家、区域和国际网络安全举措方面信息的途径；

4 就这些活动的情况向理事会做出年度报告并酌情提出提案，

责成电信发展局主任

1 根据世界电信发展大会（2006 年，多哈）以及按照该届大会第 45 号决议（2006 年，多哈）随后召开的会议的结果，与相关合作伙伴密切合作，开发加强网络安全和打击垃圾邮件方面合作的项目，以满足发展中国家的要求；

2 在现有资源允许的范围内，为这些项目提供必要的财务和行政支持，并通过合作伙伴协议，为落实这些项目寻求更多的资源（现金和实物）；

3 确保在国际电联作为 WSIS C5 行动方面的协调方/推进方的各种活动中协调这些项目；

4 将这些项目与电信发展部门（研究组有关这一主题的活动和项目协调一致；

5 继续与相关组织合作，目的是通过联合举办的讲习班和培训项目等手段交流最佳做法，并传播信息；

6 就这些活动的情况向理事会做出年度报告并酌情提出提案。

国际电联电信发展部门在实施信息社会世界高峰会议 C.5 行动方面（树立使用信息通信技术的信心并提高安全性）过程中所开展的活动概览

1. 引言

很多发展中国家的人民依然无法使用物理的基础设施，例如医院、学校和公共行政服务，而信息通信技术（ICT）有可能通过电子卫生、电子教育、电子商务和电子政务提供这些基本服务。

今天，信息技术和电信领域的快速发展使医生与病人之间的电子交易、在线公共行政服务的获得以及使用互联网向偏远地区的客户出售商品和服务均已成为可能。使用 ICT 应用填补基本服务获取的空白、赋权发展中国家使之成为信息社会的完全参与者，亦可能成为现实。

要完全实现信息社会给政府、企业和人民带来的益处，首先必须解决安全和信任问题，各种有关网络犯罪的解决方案、可实施的立法、身份盗窃、数据隐私和对于关键性信息系统的保护必须到位。促进社会和经济发展高度依赖于 ICT，而关键信息系统和数据能够在顷刻之间被获取、操纵和破坏，这两种特质均使网络安全成为新兴的信息社会和知识经济所面临的主要挑战之一。

2. 活动和举措

作为成员国在全权代表大会和世界大会与全会上所通过的职责之一，同时亦是发挥其作为 WSIS C.5 行动方面协调方/促进方的角色，国际电联正与其合作伙伴一起采取各种措施，树立人们使用 ICT 的信心和提高安全性。

本报告简要介绍已经实施和正在规划中的行动，将各项活动分为五个领域（**确保 ICT 应用的安全、立法、政策战略和能力建设、提高意识**和**成员国之间的合作**）。该报告同时提供了其它有关为实现 WSIS C.5 行动方面所进行的活动的相关信息，并邀请所有感兴趣的各方与国际电联携手，共建人们对 ICT 的信心并加强其安全性。

2.1 确保 ICT 应用的安全性 – 项目实施

在电子政务、电子商务、电子支付和电子卫生等关键服务中，保护敏感数据、确保数据和交易的完整性和确立各方的身份是非常重要的。在这些服务中使用 ICT 的一个主要障碍就是对于安全性的担心。只有首先解决这些安全和信任问题，并提出切实可行的解决方案，才能真正实现 ICT 在提供可承受得起的增值服务方面的潜力。

有些国家已经开始使用切实可行的解决方案，通过安全和信任技术，利用 ICT 的潜力提供关键服务，从而实现从简单的信息传播系统到进行关键交易和向其人民提供各种服务的跨越。

由于国际电联的努力，几个发展中国家首次积极参与到基于安全和信任技术的解决方案的部署和使用之中，从而将 ICT 的益处扩展到政府和卫生服务等领域。

在巴巴多斯、不丹、保加利亚、布基纳法索、柬埔寨、喀麦隆、科特迪瓦、格鲁吉亚、牙买加、巴拉圭、秘鲁、塞内加尔、土耳其和赞比亚实施基于公共密钥基础设施（PKI）使用先进安全和信任技术的项目，包括生物特征认证、智能卡、ITU-T X.509 数字证书和数字签名技术。计划将于 2007 年进行更多项目。(http://www.itu.int/ITU-D/e-strategy/e-applications/archive04.html)

2.1.1 格鲁吉亚

该国际电联项目主要是解决为安全传输、获取和处理数字化的政府文件提供成本效益高的解决方案这一挑战，从而增强政府的效率和透明度。我们向格鲁吉亚交通与通信部的高级官员提供了解决方案，增强工作流程的自动化，并使各位官员能够以数字的方式签署和传送官方文件，从而取代缓慢而昂贵的纸质文件方式。对于敏感文件的获取必须经过授权，这一点也通过安全和信任解决方案成为可能，并确立了该部委内部授权人士的身份。

2.1.2 巴拉圭

本项目为运营商和服务提供商与国家监管机构（CONATEL）以电子的方式交流敏感信息（例如收入申报）提供了一个安全和值得信任的基于互联网的机制平台。本项目使用安全和高信任度的 ICT 解决方案，从而简化向公共电话运营商颁发牌照的程序，提高监管机构商业流程的效率。

2.1.3 巴巴多斯和牙买加

国际电联向上述两国提供了帮助，以建立数字认证和认证管理机构运作方面的国家政策框架。国际电联的帮助还包括技术规范的定义和实施国家平台的政策指导，以帮助巴巴多斯和牙买加发布和管理数字证书、提供强有力的认证服务，确保电子政务和电子商务交易的安全性和信任度。牙买加国会在 2006 年底通过了《电子交易法》，国际电联还向其提供了专家援助，以确保身份管理平台及相关政策符合该立法。该国家公共密钥基础设施由国际电联和牙买加政府共同出资，计划于 2007 年开始运作。

2.1.4 喀麦隆

本项目能够使敏感政府文件通过互联网进行安全传送，并向那些根本没有物理行政基础设施的城镇和农村地区的人民提供基于互联网的政府服务。很多基于电子签名和加密技术的解决方案，例如强大的认证、数据机密性、数据完整性和不可否认性，使我们能够解决某些网络安全威胁，包括身份盗窃。

2.1.5 保加利亚

国际电联帮助保加利亚实施一个网络安全平台，该平台使用 PKI 和 PKI 支持的应用，确保交通与通信部、财政部、部委委员会和通信管理委员会（CRC)之间能够有高度安全的通信。该平台允许高级政府官员之间进行安全、高效和成本效益高的互动，这样就可以作为面对面会晤的补充，提高工作效率。参与互动的官员之间所交流的数据通过使用数据机密性、不可否认性、数据完整性和基于证书的强大认证技术实现加密和数字签名。

2.1.6 土耳其

本项目的一个战略目标是通过开发一套安全的卫生信息媒介，使卫生服务提供商（基本医疗和二级医疗）、卫生从业人员和普通市民能够使用最新的 ICT 方便和安全地获得卫生信息，从而改善土耳其的卫生服务。

本项目的基石包括开发能够支持家庭医生系统的医疗信息系统、实施电子病历、开发能够在医疗服务提供商（包括基本医疗中心、医院和公共/私营保险机构）之间能够进行互可兼容的系统。

2.1.7 不丹

为解决很多不丹农村人口常常要长途跋涉数天到行政中心城市获取服务的需求，国际电联在该国实施了一个基于公共密钥基础设施（包括生物特征认证、强大的加密和数据完整性技术）的国家平台。该网络安全平台由国际电联和不丹政府共同出资，其提供的服务包括身份管理与核实、基于证书的认证、数字签名、数据机密性和数据完整性服务。由于国际电联的支持，不丹偏远地区的用户能够获取基于信任和安全技术的关键服务，从而将 ICT 的能力和益处延伸到向农村和城市人口提供服务方面。

2.1.8 有关网络安全和打击垃圾邮件的全球项目

国际电联组织了第一次成员国和部门成员会议，讨论增强网络安全（包括打击垃圾邮件）方面合作的方法。本次会议旨在实现下列三个主要目标：

a) 就网络安全和垃圾邮件领域达成共识甚至是协议，现在急需一套能够加强成员国之间合作的机制到位。

b) 为感兴趣的成员国加强网络安全（包括垃圾邮件）方面的合作确定谅解备忘录等可能的机制。

c) 基于成员国提交的文稿，以报告的形式向 2006 年全权代表大会提交提案，以供考虑。

在本次会议上，各成员国认为网络安全和打击垃圾邮件全球合作的主要挑战包括：

a. 建立基本的意识
b. 制定并实施适当而强大的国家立法
c. 建设人和机构的能力
d. 实施（能力建设领域）
e. 制定有关网络安全的国家政策和战略
f. 方便国家和利益攸关方之间的信息交流
g. 成立国家联络点
h. 监控和评估现有举措的进展
i. 为突发事件的响应、监控和预警实施解决方案
j. 评估网络安全的薄弱环节和威胁
k. 为网络和网络安全提供有效的工具和应用
l. 合作伙伴关系
m. 国际合作

人们一致认为，国际电联应在整合现有举措方面发挥关键性作用，为现有举措提供一个统一的框架，从而解决发展中国家的需求。本次会议的报告已提交于安塔利亚举行的 2006 国际电联全权代表大会。本次会议进一步认同，该报告是国际电联制定网络安全和打击垃圾邮件

合作机制的重要活动。本项目将通过一个题为“关于加强网络安全和打击垃圾邮件方面合作的项目”得以实施，2007 年启动，为期 4 年，并将成为国际电联发展部门 2007 年运作规划的一部分。

有关该项目：

- 本项目在实施过程中应考虑到国际电联在网络安全和打击垃圾邮件方面的职责。
- 本项目的主要目的是为发展中国家在会议确认的、对网络安全和打击垃圾邮件合作极为重要的领域提供帮助。
- 有关立法方面，在帮助发展中国家制定符合《网络犯罪公约》的国家立法时，应酌情考虑到欧洲理事会的相关工作。
- 本项目框架下各项活动的实施，应由各国明确请求，重点应放在发展中国家。
- 本项目开发完毕之后，应呈交潜在的融资实体，包括成员国、私营部门和国际组织（例如世界银行和欧洲委员会）。

2.2 立法

帮助发展中国家制定示范性法和反垃圾邮件法

参与国际电联监管机构全球专题研讨会的与会者请求国际电联帮助其制定反垃圾邮件立法。2006 年版的国际电联刊物 – 《电信改革趋势》第 7 章中描述并分析了反垃圾邮件示范法的内容，包括有关使用清晰的、可执行的互联网服务提供商（ISP）行为准则的条款。这些可执行的行为准则将禁止 ISP 客户将 ISP 用作垃圾邮件和其它相关不良行为的来源，例如欺骗和网络钓鱼（网页仿冒），同时也将禁止 ISP 与其它不能遵守类似行为准则的 ISP 达成对等协议。**《2006 年电信改革趋势》**第 7 章 – “阻挡国际垃圾邮件浪潮”现已可以在如下网址获得：www.itu.int/ITU-D/treg/publications/Chap%207_Trends_2006_E.pdf

2.3 政策、战略和能力建设

2.3.1 讲习班和研讨会

国际电联组织了国家和区域层面的讲习班与研讨会，以解决若干国家有关网络安全的政策与技术战略问题，例如阿塞拜疆、巴巴多斯、喀麦隆、智利（南锥共同体国家）、拉脱维亚（中东欧、独联体和波罗的海国家）、蒙古、巴基斯坦、巴拉圭、秘鲁（拉美安地斯地区）、罗马尼亚、塞舌尔群岛、阿拉伯叙利亚共和国和乌兹别克斯坦。

有关网络安全技术、政策和战略的人力与机构能力建设活动已经在喀麦隆、赞比亚、巴巴多斯、牙买加、保加利亚、不丹和叙利亚展开。

2.3.2 全球性会议

由来自 120 个国家的 50 名安全专家和超过 500 名代表参加的一个全球性会议于日内瓦召开，大会讨论了有关发展中国家电子签名、数字认证和加密解决方案的技术、战略、政策和法律事宜。

2.3.3 国际电联阿拉伯区域电子政务和 IP 研讨会

安全和信任是本次会议上的两个主要话题。本次会议最终形成《迪拜宣言》，强调国际电联有必要继续参与电子应用和服务方面的网络安全活动。本次会议将阿拉伯区域的政策制定机构聚集一堂，讨论共同面临的问题，并试图为网络安全方面的主要挑战建立一个共同的框架，同时还就该地区感兴趣的具体领域（例如身份管理和电子签名）为 2007 年规划了后续活动。

2.3.4 世界卫生信息技术大会期间举行的联合国研讨会

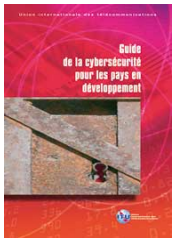
国际电信联盟（ITU）、世界卫生组织（WHO）、联合国教科文组织（UNESCO）、联合国训练研究所（UNITAR）及业界合作伙伴在世界卫生信息技术大会期间组织了一次联合国研讨会。本次会议主要讨论了卫生方面的网络安全问题。该联合国研讨会于 2006 年 10 月 10 日在日内瓦 Palexpo 展览馆举行，将联合国下属四个机构的成员聚集一堂，讨论网络安全在医疗和卫生交易及应用方面的重要作用。欲了解更多详情，请访问下列网站：
www.worldofhealthit.org/about/about_partners.asp

2.4 提高意识

2.4.1 出版物及文章

《发展中国家网络安全指南》，©ITU 2006

本网络安全参考指南是为帮助发展中国家和最不发达国家在信息社会主要安全挑战方面建设本地能力和提高意识而制定的。本书解释了垃圾邮件、恶意软件（病毒、蠕虫、特洛伊木马等）、数据隐私、缺乏认证、对数据机密性和数据完整性的需要等主要问题，同时还提供了网络安全立法的案例研究及可以用于保护关键基础设施的方法范例。本指南的英文和法文版均可以从 ITU-D 网站免费下载，地址为：www.itu.int/ITU-D/e-strategy/publications-articles/



《数据隐私、安全及防止网络犯罪的立法研究》– ©ITU 2006

ICT 的某些方面需要从立法的角度加以保护，尤其是有关数据安全及知识产权的现有立法以及在新型信息高速公路上的旧有犯罪形式，例如身份盗窃、欺诈和勒索。显而易见，需要

对原有立法进行修订，以适应 ICT 的需要，同时应认识到与计算机相关的新型犯罪行为的存在，因此需要以新的安全设备对信息流进行认证。

本研究性出版物主要探讨为保护发展中国家的国家利益、保证 ICT 和电子商务的发展、确保基础设施拥有足够的立法保护，必须解决的主要立法问题。三项普遍原则即机密性、完整性和可用性，已被确认是网络安全的重要组成部分。这三个方面彼此重叠，密切相关。有时候，很难确定不同类别之间的界线，从而决定某一具体领域应该适用哪一类立法。本出版物的电子版本可以在 ITU 信息通信战略网站上下载，地址为：
www.itu.int/ITU-D/e-strategy/publications-articles/

《发展中国家网络犯罪新指南》 ©ITU 2007

2006 年底，国际电联完成了一份全新参考资料的撰写工作，其目的是提高对网络犯罪问题的意识，方便人力和机构能力建设活动。本书同时也提及有必要就网络威胁和应对措施达成共识。全书共 160 页，主要目的是为发展中国家提供指导和参考资料。该书首先简要介绍了各种形式的网络犯罪，包括网络犯罪份子的特点。此后解释了目前互联网存在的薄弱环节及网络攻击、数字证据以及计算机法学与计算机调查的基本原则。此书还提供了有关网络犯罪的术语词汇表及参考资料。这一新指南及前一本（有关网络安全的）指南，将成为网络安全和网络犯罪方面人力与机构能力建设规划活动的来源资料。该指南首先以英文出版，随后将被翻译成国际电联所有六种正式语文。感兴趣的国家可以在 2007 年第二季度获得纸质版本，并将可以从国际电联网站上下载。

2.5 成员之间的合作

为方便成员之间交流经验与最佳做法，国际电联通过其发展部门（ITU-D）研究组提供一个平台。各成员可以在此就如何应对网络安全和打击垃圾邮件方面的挑战探讨共同的解决方案。2006 年 9 月，召开了第一次 ITU-D 研究组关于网络安全课题的会议。在该会议上，新周期的工作计划得以批准。在 2006-2009 年间，该 ITU-D 研究组课题的工作计划和预计输出成果包括：

a) 对有关下列问题的意识进行调查、制定目录、予以说明并提高这些方面的意识：
   - 国家政策制定机构在与其它利益攸关方一道建立网络安全文化时面临的主要问题；
   - 与建立网络安全文化有关的信息与帮助的主要来源；
   - 国家政策制定机构在与其它利益攸关方一道组织网络安全工作和培育安全文化过程中所采用的成功的最佳做法；
   - 发展中国家在解决网络安全问题方面所面临的独特挑战以及应对这些挑战的最佳做法。

b) 审议建立和运作监控、预警和突发事件响应及恢复能力方面的最佳做法，各成员国可以利用这些最佳做法建立其国家能力。

就上述第 3 a)节列出的各项问题向成员国提交一份或多份报告。这些报告应该反映，安全的信息通信网络对于建设信息社会和各国的社会经济发展是不可或缺的。

3. 小结

网络安全是各国普遍关心的问题，应严肃对待。对于发展中国家而言，基于安全和高信认度平台的 ICT 应用，能够在卫生、金融、公共管理和商务方面为人们提供关键服务。除有必要保护其关键基础设施和维护敏感数据与交易安全之外，发达国家亦可从中获益。

只有政府、业界、国际组织、民间团体和其它利益攸关方携起手来，通力合作，才能有效解决我们在这一领域所面临的挑战。

各合作伙伴应努力提高关于挑战和机遇的意识，建设本地能力，制定可以得以实施的立法，实施能够实现安全和高信认度解决方案的项目，制定合适的政策，以实现大家一致认同的目标，即为所有人建立一个具有包容性的、安全的和全球性的信息社会。

国际电联在其职责框架内，正在采取各种举措，实施项目，方便信息交流，建设能力，提高意识并创建合作与伙伴关系平台，以便在全球层面解决网络安全问题。为实现 WSIS 所确认的目标，国际电联请所有感兴趣的合作伙伴与其合作，共同保障 ICT 使用的安全性，并树立起人们对 ICT 使用的信心。

附件 D – 国际电联电信标准化部门2005-2008年研究期内正在研究的与安全有关的主要课题

摘自
www.itu.int/ITU-T/studygroups/com17/questions.html

分配给国际电联电信标准化部门（ITU-T）第 17 研究组的课题（2005-2008 年研究期）

第 17 研究组：安全、语言和电信软件

第 2/17 号课题 – 目录服务、目录系统和公共密钥/属性证书

2.1 目录服务

a) 需要有哪些新的、能充分利用得到广泛支持的目录服务（如 X.500 和 LDAP）的服务定义和特征？

b) 需要对 E 和 F 系列建议书做哪些修改和/或需要哪些新建议书，以便于对现有服务定义和特征进行增强和修正其中的不足？

2.2 目录系统

a) 为了更好地支持现有和潜在的目录客户，需要对目录做哪些增强，如加强各复制站点间目录信息的一致性，支持在用户规定的集总目录属性上运行，当检索大量返回结果时改善其性能，或解决多个目录服务提供商在同一名称下拥有不同信息造成的混乱？

b) 目录还需要哪些进一步的增强，以便于能与利用 IETF LDAP 技术规范所执行的服务进行互操作和支持，其中包括访问目录可能用到的 XML？

c) 目录还需要哪些进一步的增强，使其能在各种环境下使用，如无线网络和多媒体网络？

d) 目录还需要哪些进一步的增强，以改进其对智能网、通信网和公共目录服务等领域的支持？

e) 需要对 X.500 系列建议书做哪些修改和/或需要哪些新建议书，以便于对目录进行增强和修正其中的不足？

目录系统的工作将与 ISO/IEC JTC 1 一起，在他们推广与 X.500-X.530 建议书共同案文的 ISO/IEC 9594 时协作进行。特别在 LDAP 领域，还将继续与 IETF 保持联络和密切合作。

2.3 公共密钥/属性证书

a) 公共密钥和属性证书需要哪些进一步的增强，使其能在各种环境下使用，如诸如无线网络和多媒体网络的资源受限的环境？

b) 公共密钥和属性证书需要哪些进一步的增强，以提高其在生物特征识别、认证、访问控制和电子商务等领域的有用性？

c) X.509 需要做哪些修改，以便于对其进行增强和修正其中的不足？

公共密钥和属性证书的工作将与 ISO/IEC JTC 1 一起，在他们推广与 X.509 建议书共同案文的 ISO/IEC 9594-8 时协作进行。特别在 PKI 领域，还将继续与 IETF 保持联络和密切合作。

第 4/17 号课题 – 通信系统的安全项目

安全这一主题范围甚广。安全可以适用于电信和信息技术几乎所有的领域。安全需求的规范方式，可以是自下而上，或自上而下的：

– 自下而上的方式，即特定领域的专家负责设计安全措施，加强和保护网络的某个特定部分，如生物特征识别、密码术等。这是使用最广的一种方式，但与各个机构研究安全的方式相比，又是支离破碎的。

– 自上而下的方式，是用高水准和战略的眼光看待安全问题。它要求纵览全局，同时也是一种更加困难的方式，因为，要找到了解网络各个部分细节及其安全需求的专家，比专业知识仅限于一、两个特定领域的专家更加困难。

– 另外一种替代方式，是将自下而上和自上而下的方式结合起来，通过协调，变各自为战为统一行动。事实证明，面对各种各样的利益和工作议程，这一做法极具挑战性。

本课题专注于愿景的制定以及对国际电联电信标准化部门内部全方位的通信安全活动进行协调和组织。在与其它研究组和其它标准制定组织（SDO）进行协作时，将采用自上而下的方式处理安全课题。这一项目的方向是集中力量开展项目并更加注重战略内涵。

问题

a) 通信系统安全项目有哪些实际成果？

b) 该项目要取得实际成果都需要哪些流程、工作项目、工作方法和时间表？

c) 国际电联需要制定和维护哪些安全概略和手册？

d) 需要组织何种安全讲习班？

e) 为推动安全工作，需要开展何种工作来与其他 SDO 建立有效的合作关系？

f) 有哪些关键的阶段性成果和成功标准？

g) 如何激发部门成员和主管部门对安全工作的兴趣并保持其发展势头？

h) 安全特性对于市场如何能变得更具有吸引力？

i) 如何向各国政府明确阐述依赖于强健和安全的电信基础设施，对于保护全球经济发展的重要利害关系和紧迫需要？

第 5/17 号课题 – 安全体系架构和框架

考虑到对于通信环境的安全威胁和目前防范威胁的安全对策的发展，应当探索新的安全要求和解决方案。

应当研究新型网络的安全和新业务的安全。

问题

a) 应如何定义完整和连贯一致的通信安全解决方案？

b) 完整和连贯一致的通信安全解决方案的体系架构是什么？

c) 实施安全架构、确立全新安全解决方案的框架是什么？

d) 实施安全架构、评估（和随后改善）现有安全解决方案的框架是什么？

e) 安全的架构支柱是什么？

   i) 新兴技术的安全架构是什么？

   ii) 端到端安全的架构是什么？

   iii) 移动环境的安全架构是什么？

   iv) 需要什么样的技术安全架构？例如：

      a) 开放系统的安全架构是什么？

      b) 基于 IP 的网络的安全架构是什么？

      c) 下一代网络（NGN）的安全架构是什么？

f) 应如何修改上层和下层安全模型建议书，以使其能适应不断变化的环境，可能还需要哪些新的建议书？

g) 就现有安全方面的建议书而言，体系架构标准的结构应如何确立？

h) 应如何修改安全框架建议书，以使其适应新兴的技术，可能还需要哪些新的建议书？

i) 如何使用安全服务提供安全解决方案？

第 6/17 号课题 – 网络安全

目前已推出了众多的保护和发现机制，如防火墙和入侵发现系统（IDS），但其中多数都只专注于技术方面。这些技术解决方案固然重要，但需要更多地从国际标准化角度审议和探讨网络安全问题。

问题

应研究下列网络安全问题：

- 有关薄弱环节信息的发布、共享和对外透露的流程；
- 网络世界中事件处理操作的标准程序；
- 保护关键网络基础设施的战略。

第 7/17 号课题 – 安全管理

问题

a) 应如何确定和管理电信系统的安全风险？

b) 应如何确定和管理电信系统的信息资产？

c) 应如何确定电信运营商所面临的具体管理问题？

d) 应如何按照现有的 ISMS 标准恰当地构建电信运营商的信息安全管理系统？

e) 应如何处理和管理电信领域发生的安全事件？

第 8/17 号课题 – 电子生物特征识别

问题

a) 如何利用安全可靠的电子生物特征识别方法改进对用户的识别和认证？

b) 国际电联电信标准化部门如何利用 IEC 60027 新的部分 – “生理子集”，为安全的电子生物特征识别设备分类所需的恰当模型提供内容？

c) 应当使用何种安全水平基准系统来将安全可靠的电子生物特征识别解决方案进行分级？

d) 应如何确定电信领域生物特征认证技术的问题？

e) 应如何确定基于密码技术（如 PKI）的电信生物特征认证技术的要求？

f) 应如何确定基于密码技术（如 PKI）的电信生物特征认证技术的模型和程序？

第 9/17 号课题 – 安全通信服务

问题

a) 应如何确定和定义移动通信或 web 服务领域的安全通信服务？

b) 应如何识别和处理通信服务背后的威胁？

c) 有哪些安全技术可以支持安全通信服务？

d) 应如何保持和维护通信服务间的安全互连？

e) 安全通信服务需要哪些专门的安全技术？

f) 新兴安全 web 服务需要哪些专门的安全技术或协议？

g) 安全通信服务应采用何种安全应用协议？

h) 什么是针对安全通信服务及其应用的全球安全解决方案？

附件 E – 参考资料

描述在电信界实施的国际电联电信标准化部门（ITU-T）安全标准的说明性参考资料：

《电信和信息技术中的安全问题：为构建安全电信实施 ITU-T 现有建议书的相关问题概览》。ITU-T，2004 年 10 月：*www.itu.int/itudoc/itu-t/86435.html*

部分参考著作

ANDERSON, Ross, Security Engineering, A Guide To Building Dependable Distributed Systems, Wiley, 2001, ISBN 0-471-38922-6

BISHOP, Matt, Computer security: art and science, Addisson-Wesley, 2002, ISBN 0-201-44099-7

BLACK, Ulyses, Internet Security Protocols, Protecting IP Traffic, Prentice Hall, ISBN 0-13-014249-2

DENNING, Dorothy E., Information Warfare and Security, Addison-Wesley, 1999, ISBN 0-201-43303-6

DUFOUR, Arnaud; GHERNAOUTI-HÉLIE, Solange, Internet – PUF, Que sais-je? N° 3073 – ISBN: 2-13-053190-3

FERGUSON, Niels; SCHNEIER, Bruce: Practical Cryptography, Wiley, 2003, ISBN 0-471-22357-3

GHERNAOUTI-HÉLIE, Solange; Internet & Sécurité – PUF Que sais-je? N° 3609 – ISBN: 2-13-051010-8

GHERNAOUTI-HÉLIE, Solange, Sécurité informatique et réseaux, cours et exercices corrigés – Dunod 2006.

PANKO, Raymond, Sécurité des systèmes d'information et des réseaux, Pearson Education (version française), 2004

POULIN, Guillaume; SOYER, Julien; TRIOULLIER, Marc-Eric, Sécurité des architectures Web, «ne pas prévoir c'est déjà gémir», Dunod, 2004.

SCHNEIER, Bruce, Beyond Fear, Thinking Sensibly About Security In An Uncertain World, Copernicus Books, 2003, ISBN 0-387-02620-7

SCHNEIER, Bruce, Secrets et mensonges, la sécurité numérique dans un monde en réseau, Vuibert, (version française) 2001, ISBN 2-711786-846

SCHNEIER, Bruce, Cryptographie Appliquée, Algorithmes, protocoles et codes source en C, 2e édition, Vuibert, 2001, ISBN 2-7117-8676-5 – version française de SCHNEIER, Bruce, Applied Cryptography, Protocols, Algorithms and Source Code in C, Second Edition, Wiley, 1996, ISBN 0-471-11709-9

SINGH, Simon, Histoire des codes secrets, JC Lattès, 1999, ISBN 2-7096-2048-0

STALLINGS, William, Cryptography And Network Security, principles and practice, Prentice Hall, 1999, ISBN 0-13-869017-0

STALLINGS, William, Network And Internetwork Security, principles and practice, Prentice Hall, 1995, ISBN 0-13-180050-7

STALLINGS, William, Network Security Essentials, applications and standards, Prentice Hall, 2000, ISBN 0-13-016093-8

参考网站

法文网站：

法国总理网站：www.premier-ministre.gouv.fr

（请特别参见：*Technologie de l'information dans la thématique: communication*）

www.internet.gouv.fr：与信息社会发展有关的网站

法国公共服务门户网站：www.service-public.gouv.fr。由此可访问各种在线服务，请参见«*se documenter*»栏目。

法国法律公共服务网站：www.legifrance.gouv.fr

法国文件服务网站：www.ladocfrancaise.gouv.fr

www.foruminternet.org/：有关法律、互联网和网络的信息与讨论论坛

法国国家公民自由委员会网站：www.cnil.fr

法国打击 ICT 关联犯罪行为中央办公室网站：
www.interieur.gouv.fr/rubriques/c/c3_police_nationale/c3312_oclctic

信息系统与网络安全瞭望台：www.ossir.org

Clusif：www.clusif.asso.fr。

网络犯罪大观：https://www.clusif.asso.fr/fr/production/ouvrages/

其它网站

CERT：www.cert.org（计算机应急响应小组）

NIST：www.nist.gov（美国国家标准与技术研究所）

NSA：www.nsa.gov（美国国家安全局）

CSE：www.cse.dnd.ca（加拿大电信安全中心）

CESG：www.cesg.gov.uk（英国国家信息保障技术管理局）

BSI：www.bsi.bund.de（德国联邦信息安全办公室）– 德文和英文双语网站

DSD：www.dsd.gov.au （澳大利亚和新西兰防御信号司）。网站专注于数字监控和信息安全。

国家白领犯罪中心：IFCC – 互联网欺诈投诉中心：
www1.ifccfbi.gov/index.asp；Internet Fraud – Crime Report – 2004:
www1.ifccfbi.gov/strategy/2004_IC3Report.pdf

新闻简报

密报 – Bruce Schneier: [schneier@counterpane.com]
crypto-gram-list@listserv.modwest.com

互联网权利论坛快讯：infolettre@listes.foruminternet.org

US-CERT 安全公报：security-bulletins@us-cert.gov

网络警察信息快讯：cyberpolice.over-blog.com/
cyberpolice.over-blog.com [newsletter@over-blog.com]

附件 F – 经济合作与发展组织（OECD）信息系统与网络安全指导原则：逐步培育安全文化

序言

自经济合作与发展组织（OECD）于 1992 年推出《信息系统安全指导原则》以来，信息系统与网络的使用以及整个信息技术环境均发生了巨大的变革。这些持续的变革带来了大量的优点，但同时也要求政府、企业、其它组织和个人用户更加重视安全问题，因为正是他们开发、拥有、提供、管理服务和使用信息系统与网络（此后统称“参与者”）。

更加强大的个人计算机、融合技术和互联网的广泛使用已经取代了过去较为封闭的网络内中等强度和孤立的系统。今天，各参与者日益互连，而且这种连接常常超越国界。此外，互联网能够支持能源、交通和金融等关键基础设施，并在塑造企业与企业之间进行商业交易、政府向个人及企业提供服务以及个人与个人之间沟通与信息交换的方式方面，发挥着重要的作用。构成通信和信息基础设施的技术的性质和类别也已发生巨大的变化。基础设施接入设备的数量和性质已经大大增加，现已包括固定、无线和移动设备，而且越来越多的接入是通过“总是在线”的连接方式而实现的。因此，所交换信息的性质、数量和敏感度均已大大拓宽。

随着互连程度的日益提高，信息系统和网络现在面临的威胁和薄弱环节在数量和种类上均大大增长。这就为安全提出了新的问题。为此，本指导原则适用于新型信息社会的所有参与者，并指出需要提高对安全问题的意识和理解，逐步培育“安全文化”。

F.1 逐步培育安全文化

本指导原则通过促进安全文化的培育 – 即强调信息系统和网络开发过程中的安全问题，以及在信息系统和网络的使用与互动过程中采纳新思维和新做法。如今，网络和系统的安全设置与使用往往是亡羊补牢式的，本指导原则宣告与这一时代的诀别。参与者越来越依赖于信息系统，网络和相关服务，而上述种种均需要可靠和安全。只有充分考虑到所有参与者的权益以及系统、网络和相关服务的性质，才能提供有效的安全性。

每一位参与者都是确保安全的重要因素。参与者应各司其职，充分意识到相关的安全风险和防御措施，承担责任，采取切实措施，加强信息系统和网络的安全。

促进安全文化的培育，既需要领导力，亦需要广泛的参与。最终应当使人们高度重视安全规划和管理，理解所有参与者均需重视安全问题。安全问题应当成为各级政府、企业和所有参与者共同的关切及责任。本指导原则构成了在全社会培育安全文化的基础。这将使得所有参与者在设计和使用信息系统和网络时考虑到安全因素。本指导原则建议所有参与者采纳并提升安全文化，将其作为思考、评估和实施信息系统和网络运营的一种方法。

F.2 目标

这些指导原则的目标是：

- 在所有参与者中促进安全文化的培育，将其作为保护信息系统和网络的一种方式。
- 提高人们的意识，使其充分认识到信息系统和网络的风险，化解上述风险的政策、做法、措施和程序，以及采纳和实施上述政策、做法、措施和程序的必要性。
- 提高所有参与者对于信息系统和网络的信心及其对提供和使用信息系统及网络的方式的信心。
- 形成一套基本的参考文件，帮助参与者理解安全问题，并在为信息系统和网络安全制定和实施连贯的政策、做法、措施和程序时，尊重道德价值。
- 在制定和实施安全政策、做法、措施和程序的过程中，酌情促进所有参与者之间的合作与信息共享。
- 促使所有参与者在开发和实施标准的过程中将安全做为重要的目标之一。

F.3 原则

下列九个原则是相辅相成的，应当做为一个整体来阅读。这些指导原则关乎所有层面的参与者，包括政策和操作层面。根据这些指导原则，各参与者的责任因其角色的不同而有所不同。所有的参与者均将受益于意识、教育、信息共享和培训，这一切将使其更好地理解和实施安全问题。加强信息系统和网络安全的努力必须符合一个民主社会的价值观，尤其是对开放和自由的信息流动的需求以及对个人隐私[65]的基本关切。

65 除此《安全指导原则》之外，OECD还就世界信息社会重要事宜的其它指导原则制定了补充建议。这些建议关乎隐私（1980年 OECD《关于隐私保护和个人数据跨国流动的指导原则》）以及密码学（1997年 OECD《关于密码学政策的指导原则》）。应将本《安全指导原则》与其对照阅读。

***1)* 意识**

参与者应充分意识到确保信息系统和网络安全的必要性，以及为增强安全性他们能做哪些工作。

对于风险和现有保护措施的意识是确保信息系统和网络安全的第一道防线。信息系统和网络既可以通过内部风险也可以通过外部风险受到影响。参与者应当理解，安全方面的失灵不仅可能大大损害他们自身控制下的系统和网络，而且亦可能通过互连和相互依存损害他人的系统和网络。参与者应了解其自身系统的设置及可得到的更新，其系统在网络中的位置，为增强安全性他们可以实施的良好做法，以及其他参与者的需要。

***2)* 责任**

所有参与者对于确保信息系统和网络的安全均负有责任。

参与者依赖于互连的本地或全球信息系统及网络，因此应当理解他们在确保信息系统和网络安全方面所应承担的责任。他们应当根据自身的角色承担相应的职责。参与者应定期回顾其自身的政策、做法、措施和程序，以评估它们是否与其环境相适应。产品和服务的开发、设计与供应商应当解决系统和网络安全问题，并及时发布相关信息，包括更新信息，从而允许用户更好地理解其产品和服务的安全功能，以及他们与安全有关的责任。

***3)* 应对**

参与者应当以及时与合作的态度行动起来，预防、发现和应对安全事件。

各参与者均应充分意识到信息系统和网络的互连可能带来的快速而广泛的破坏力量，因此应当以及时与合作的态度行动起来，处理突发安全事件。他们应当酌情分享有关威胁和薄弱环节的信息，并实施快速而有效的合作程序，从而预防、发现和应对突发安全事件。如果条件允许，应包括跨国信息共享与合作。

***4)* 道德**

参与者应尊重他人的合法权益。

鉴于信息系统和网络已经深入到社会的每一个角落，因此参与者有必要认识到，他们的作为或不作为可能会有损他人。因此，道德准则是至关重要的。参与者应努力制定和采纳最佳做法，并推进能够意识到安全需求和尊重他人合法权益的行为准则。

***5)* 民主**

信息系统和网络的安全应当符合一个民主社会的基本价值观。

安全工作的落实应当符合民主社会所承认的价值观，包括交流思想与想法的自由、信息的自由流动、信息与通信的机密性、个人信息的适度保护、开放和透明等等。

6) 风险评估

参与者应进行风险评估。

风险评估能够明确威胁和薄弱环节，其基础应当足够广泛，以反映主要的内部和外部因素，如技术、物理和人为因素、政策以及可能对安全产生影响的第三方服务。风险评估能够决定可接受的风险水平，帮助遴选适当的控制策略，以根据受保护信息的性质和重要性，管理可能对信息系统和网络带来的潜在危害。由于信息系统之间日益互连，风险评估应当考虑可能由他人引起或可能对他人造成的危害。

7) 安全工作的设计与落实

参与者应将安全作为信息系统和网络的基本要素。

系统、网络和政策需要适当地设计、实施和协调，以优化安全性。在这一过程中，一个主要但不是唯一的焦点是设计和实施适当的保护措施和解决方案，以避免和限制已确认威胁和薄弱环节可能带来的潜在危害，同时技术和非技术保护措施与解决方案亦是不可或缺的，且应当与该组织的系统和网络的信息价值成正比。安全应当是所有产品、服务、系统和网络的基本元素，也应当是系统设计架构不可分割的一部分。对于最终用户来说，安全工作的设计与落实主要意味着为其系统遴选和设计产品及服务。

8) 安全管理

参与者应当以综合的方式进行安全管理。

安全管理应当以风险评估为基础，且应当是一个动态的过程，以反映各个层面的参与者的活动及其运作的各个方面。安全管理应当包括对新兴威胁的前瞻性应对，并解决突发事件的预防、发现和应对，系统恢复，持续维护，审议和审核等。信息系统和网络安全政策、做法、措施与程序应当彼此协调，相互交融，以形成一套连贯的安全体系。安全管理要求取决于参与水平、参与者的角色、涉及风险以及系统要求。

9) 再评估

参与者应定期回顾并重新评估信息系统和网络的安全，并对安全政策、做法、措施和程序做出适当修改。

新的威胁和薄弱环节层出不穷，变幻莫测。参与者应当不断回顾、重新评估并酌情修改有关安全的各个方面，以化解这些不断变幻的风险。

理事会有关《信息系统与网络安全指导原则：逐步培育安全文化》的建议

理事会，

考虑到 1960 年 12 月 14 日《经济合作与发展组织公约》，尤其是第 1 b)、1 c)、3 a)和 5 b)条；

考虑到 1980 年 9 月 23 日《理事会关于〈隐私保护和个人信息跨国流动指导原则〉的建议》[C(80)58(Final)]；

考虑到 1985 年 4 月 11 日 OECD 成员国政府通过的《跨国数据流动宣言》[C(85)139 附件]；

考虑到 1997 年 3 月 27 日《理事会关于〈密码政策指导原则〉的建议》[C(97)62/FINAL]；

考虑到 1998 年 12 月 7-9 日《关于在全球网络上保护隐私的部长级宣言》[C(98)177/FINAL 附件]；

考虑到 1998 年 12 月 7-9 日《关于电子商务认证的部长级宣言》[C(98)177/FINAL 附件]；

认识到信息系统和网络正在为政府、企业、其它组织和个人用户越来越多地使用，其价值亦随之不断增长；

认识到信息系统和网络作用的日益重要，稳定和高效的国民经济与国际贸易以及社会、文化和政治生活日益依赖于信息系统和网络，这就要求我们做出特别努力，以保护和形成对信息系统和网络的信心；

认识到信息系统和网络及其在世界范围内的普及伴随着越来越多的新风险；

认识到在信息系统和网络上存储与传播的数据和信息可能受到各种未授权访问、使用、误用、篡改、恶意代码传输、拒绝服务或破坏的威胁，因此需要适当的保护；

认识到有必要提高人们的意识，使其了解信息系统和网络的风险，以及应对上述威胁的现有政策、做法、措施和程序，并鼓励将适当的行为作为培育安全文化的关键步骤；

认识到有必要审议目前的政策、做法、措施和程序，以确保其能够应对信息系统和网络威胁所带来的各种挑战；

认识到通过培育安全文化提升信息系统和网络的安全性，符合各国的共同利益，因为它能促成国际协调与合作，从而应对因安全方面的失灵可能对国民经济、国际贸易以及参与社会、文化和政治生活可能带来的潜在危害；

进一步认识到，本建议附件所述的《信息系统与网络安全指导原则：逐步培育安全文化》是以自愿为基础的，不影响各国的主权；

同时认识到，这些指导原则并非为了表明，对于安全问题有放之四海而皆准的解决方案，亦不表明，对于某一具体的情形，应当采取何种政策、做法、措施和程序最为恰当，而是提供一套原则框架，帮助人们更好地了解各参与者如何能够受益并贡献于安全文化的培育；

向开发、拥有、提供、管理、服务和使用信息系统和网络的政府、企业、其它组织和个人用户推荐《信息系统与网络安全指导原则：逐步培育安全文化》，

建议各成员国：

制定新的或修正已有的政策、做法、措施和程序，并通过采纳和促进本指导原则中所倡导的安全文化，反映并考虑到《信息系统和网络安全指导原则：逐步培育安全文化》；

在国家和国际层面开展磋商、协调与合作，实施本指导原则；

在公共和私营部门（包括政府、企业、其他组织和个人用户）传播本指导原则，并鼓励所有相关方根据其自身的角色付起相应的责任，并采取必要措施，实施本指导原则；

向非成员国及时和适当地提供本指导原则；

每五年审议一次本指导原则，以促成关于信息系统和网络安全问题的国际合作；

责成 OECD 信息、计算机和通信政策委员会促进本指导原则的实施；

本建议取代 1992 年 11 月 26 日《理事会关于〈信息系统安全指导原则〉的建议》[C(92)188/FINAL]。

程序性历史

《安全指导原则》初版于 1992 年完成，并于 1997 年得到审议。本次审议是由信息安全和隐私工作组（WPISP）根据信息、计算机和通信政策委员会（ICCP）的一项授权，于 2001 年进行的，并于 9 11 惨剧之后得以加速。

起草工作由 WPISP 的一个专家组承担。该专家组分别于 2001 年 12 月 10-11 日在华盛顿特区、2002 年 2 月 12-13 日在悉尼、2002 年 3 月 4 日和 6 日在巴黎召开会议。WPISP 分别于 2002 年 3 月 5-6 日、2002 年 4 月 22-23 日以及 2002 年 6 月 25-26 日在巴黎举行会议。

本 OECD《信息系统和网络安全指导原则：逐步培育安全文化》于 2002 年 7 月 25 日在 OECD 理事会第 1037 次会议上作为建议获得通过。

国际电信联盟
电信发展部门 (ITU-D)
Place des Nations, CH-1211, GENEVA 20
Suisse

欲了解更多信息，请联系：
信息通信技术应用及网络安全处
电子邮件: cybmail@itu.int
www.itu.int/ITU-D/cyb

瑞士印刷
2007年，日内瓦