1 从互联网到网络空间

引言

1946 年，世界上第一台电子计算机 ENIAC 于美国宾夕法尼亚大学诞生；1969 年，美国国防部高级研究计划署开发的世界上第一个分组交换网络——互联网始祖 ARPANET 正式运行；1990 年，由万维网之父蒂姆·伯纳斯-李（Tim Berners-Lee）创建的全球第一个网页浏览器 WorldWideWeb[1]在欧洲核子研究组织（European Organization for Nuclear Research，CERN）隆重登场 …… 历史的巨轮随着层出不穷的奇思妙想和推陈出新的科技神器滚滚向前，互联网在飞速发展的同时正不断颠覆媒体、通信及制造等各行各业，互联网应用已渗透到人类生产、生活的方方面面。根据互联网世界统计（Internet World Stats，IWS）的数据显示，截至 2020 年 6 月，全球互联网用户数量达到 46.48 亿，占世界人口的比重为 59.6%。互联网已经成为承载国家政治、经济、文化、科技、军事的重要基础设施，它开辟了继陆、海、空、天之后的人类第五疆域：网络空间。

网络空间的迅速发展，促使国家安全的疆域从传统的陆、海、空、天的物理空间向数字化的网络空间拓展。网络空间安全国际形势日趋复杂，“制网权”成为大国战略较量的核心和焦点，保障网络空间安全与维护国家主权密不可分。那么，到底什么是网络空间？网络空间是如何从互联网发展而来？网络空间的安全问题源自何处？网络空间又有什么本质属性呢？希望本章能给你带来一些思考和启发。

本章纵观互联网发展历程，跟踪网络空间安全现状，就网络空间安全挑战及网络空间的特性进行概述。全章分为 3 节。1.1 节透过互联网发展中的里程

[1]https://worldwideweb.cern.ch/browser/.

碑事件，探索互联网的核心技术及影响互联网安全的根本原因。1.2 节从网络空间的定义和特点出发，概述网络空间安全现状及各国安全战略，并分析网络空间安全面临的主要挑战及网络空间安全学科体系架构，该体系将贯穿全书。1.3 节简要介绍网络空间的基础理论网络科学，包括网络科学的定义和性质，并探索复杂网络与网络空间安全之间的联系。最后对本章进行总结。表 1.1 为本章的主要内容及知识框架。

表 1.1 从互联网到网络空间

网络空间	知识点	概要
发展历史	• 计算机和计算机系统 • 互联网及 TCP/IP 协议 • Web 的产生与发展 • 网络战争打响	信息技术、开放共享、创新思维推动互联网发展
学科体系	• 网络空间的定义及其特点 • 网络空间安全定义 • 网络空间安全现状 • 网络空间安全战略 • 网络空间安全学科体系架构	① 基础理论是网络空间安全的理论基石 ② 系统安全、数据安全、网络安全及应用安全是网络空间安全的主要组成部分
基础理论	• 网络科学概述 • 复杂网络的性质 • 复杂网络与网络空间安全	网络空间有其内在的规律和秩序，主要体现为小世界特性和无标度特性

1.1 互联网发展漫话

伟大的发明往往并非一蹴而就，它们大多是科技发展累积的结果。以史为镜，见兴衰。20 世纪是一个伤痕累累但又富有激情和创新的世纪，英雄辈出，科学技术日新月异。自 1904 年英国物理学家约翰 • 安布鲁斯 • 弗莱明（John Ambrose Fleming）制造出第一只电子管之后，人类飞速迈入电子计算的时代。二进制的提出，电子管、晶体管的出现，信息理论的发展，无一不为计算机乃至互联网的产生和发展贡献力量。本节，我们将一起跨越时间长河，回顾 20 世纪最伟大的发明——互联网是怎么产生，又是如何快速发展演变的。

二进制由德国伟大的数学家、哲学家莱布尼茨发明，它是计算机编码、存储和操作信息的基础。

1.1.1 计算机和计算机系统

作为一名计算机科学技术的发烧友，如果你来到硅谷，计算机历史博物馆可是一个不可错过的打卡胜地。在这里你会看到计算机史上许多独特的、型号不一的“古董”。在 *Revolution: The First 2000 Years of Computing*一展中，放在大展牌旁边的不是声名赫赫的 ENIAC，而是一把中国的算盘，这不得不说是一件令人欣喜的事。事实上，在公元前五世纪，古希腊就出现了与中国算盘相似的计算工具，那为什么中国的算盘却被当作了计算机的开端呢？想一想这两者的区别，你很快就会发现，中国的算盘相比古希腊算盘多了一套计算口诀，显然，我们可以将其看作一套可以运行的指令。当然，尽管算盘拥有计算机的指令控制功能，但其操作仍然是手工的，错误总是难以避免。让计算自动化的进行这一人类长期追求的梦想，直到信息时代才得以实现。

你可以通过 https://computerhistory.org/exhibits/revolution/在线浏览部分展品。

1. 用机器解放重复计算的双手

“数”是我国古代传统六艺之一，印刷术的出现使得数表大行其道，航海家和天文学家从中获益良多。诸如《海航天文历》《利息表》等早期的数表编撰工作通常由一群专业的计算员完成。18 世纪末，法国大革命成功后，法国数学界召集了一大批专家和学者，采用人工流水线的方式重新编制统一度量衡后的《数学用表》，用于天文计算、航海导航和土地测量等。然而，这些海量数据计算带来的不仅仅是复杂烦琐的工作量，更严重的是其中的错误可能导致生命危险和财产损失。即使耗时耗力，历经数次校对，这部数学用表仍然错误百出。如何提高手工计算编制数表的正确率，这一问题很长一段时间悬而未决，直到一位天才数学家，查尔斯 • 巴贝奇（Charles Babbage）想出了一个绝妙的主意。

知识的每一个进步，如同每个新工具的发明，都会节省人类的劳动。——查尔斯 • 巴贝奇

19 世纪早期，伴随着机械化的盛行，纺织工业得到了快速发展。在法国机械师约瑟夫 • 玛丽 • 杰卡德（Joseph Marie Jacquard）发明了自动提花编织机以后，机械自动化的序幕正式拉开。自动提花编织机通过穿孔卡片控制丝绸的编织图案，使得编织效率大幅提高，这一技术不仅促进了丝织行业的发展，也为人类打开了一扇信息控制的大门：**通过类似穿孔卡片这样的媒介，可以自动控制机器的操作顺序。**受此启发，巴贝奇萌生了用自动化的机器来代替重复、枯燥、乏味、还容易出错的手工计算的想法，将机械原理和数学相结合，计算机械化的思维由此产生。

穿孔卡片和穿孔纸带代表着程序控制思想的萌芽，在早期电脑中被广泛地用于存储程序和数据。

1822 年 6 月 14 日，巴贝奇向英国皇家天文学会递交了一篇名为 *Note on the application of machinery to the computation of astronomical and mathe-*

matical tables[1] 的论文，基于“有限差分法”设计的差分机正式问世并获得英国财政部拨款。然而差分机的制造工作却举步维艰，按照巴贝奇的设计，差分机的运行依赖于数以千计的曲柄和齿轮，而当时的工艺制造水平很难达到其精度要求，历时 20 年，耗费一万七千英镑后，差分机的制作宣告失败。但巴贝奇提出的“机械记忆”及工艺制造等思想毫无疑问影响了计算机的发展，同时也推动了机械行业的进步。

一万七千英镑在当时可以购买 22 台蒸汽机车或两艘战舰。

尽管在差分机的研制上遭遇了巨大挫折，巴贝奇仍然没有放弃追求“用机器解放双手”这一宏伟目标。他开始酝酿一个更大胆的计划——研制一台通用的计算机。结合逻辑学和数学最先进的思想，巴贝奇设计了这台机器并将其命名为“分析机”，它包括齿轮式的“存储仓库”“运算器”“工厂”以及在其之间运输数据的输入输出部件。巴贝奇甚至为其进行了“控制器”装置的设计[2]。分析机的组成部件看起来如此熟悉，它们和现代计算机五大部件的逻辑结构如出一辙。随后，巴贝奇进一步重新设计了差分机 2 号，当然，无论是分析机还是差分机 2 号，在巴贝奇有生之年并未得以实现。事实上，完成这项工作必需的技术基础在近一个世纪后才准备就绪。1985 年，伦敦科学博物馆依照巴贝奇的图纸，着手忠实还原差分机 2 号，这项工作于 2002 年最终全部完成（如图1.1所示）。运行正常的差分机 2 号充分印证了巴贝奇设计理念的正确性。

这一段曲折的历史可以参阅科普作家詹姆斯·格雷克（James Gleick）编著的《信息简史》[2] 一书。

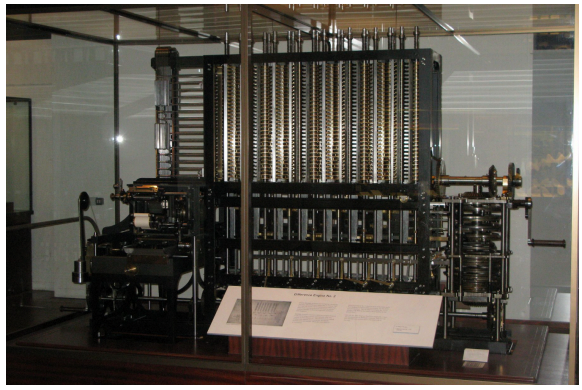


图 1.1 差分机 2 号

2. 图灵机和 Bombe 机

在巴贝奇提出分析机漫长的一个世纪后，1936 年，还在剑桥国王学院就读的阿兰·图灵（Alan Turing）在《伦敦数学协会会刊》上发表了堪称计算机原理开山之作的 *On Computable Numbers, with An Application to the Entschei-*

dungsproblem[3]，他将“计算”这一日常行为抽象成为一种由机器来操作的机械过程。判定性问题即能否通过一种有限的、机械的步骤判断“丢番图方程”（Diophantine Equation）是否存在有理整数解，这一问题由德国数学家大卫·希尔伯特（David Hilbert）在 1900 年巴黎国际数学家代表大会上提出。图灵针对这一问题的思考是这样的：**是否所有数学问题都存在确定的解？假如存在这样的解，是否可以通过有限的步骤计算得到呢？是否存在一种机器，可以采用机械的方式不断运行并在有限的时间内将这个解计算出来呢？**在这篇论文中，图灵提出了一种想象的、简单的“逻辑机器”——图灵机，如图1.2所示，这台机器具备必要的三大组件：无限长的纸带、可以左右移动的读写头以及包括内部状态存储器和控制程序指令的控制器。他用二进制这种机器能识别、理解并存储的“符号”，将现实的世界与纯数字的抽象世界连接在一起，解决了计算机中最主要的难题——计算逻辑表达的问题，由此奠定了现代电子计算机理论和模型的基础。图灵机的理论模型不但对判定问题进行了解答，更证明了计算机实现的可能，并给出了实现的参考架构。

截至 2021 年 6 月 2 日，这篇论文在 Google Scholar 上的被引用次数为 12147 次。

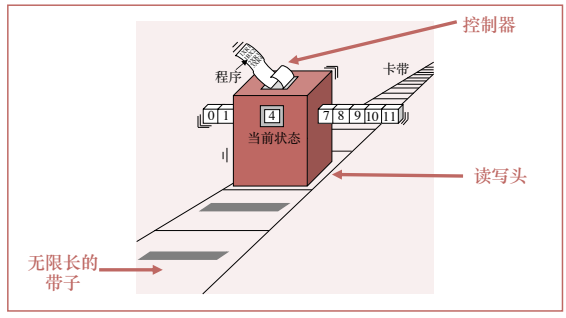


图 1.2 图灵机模型

无线电和摩尔斯电码的问世，开启了军事通讯的辉煌时代。为避免无线电通讯电文被敌方“一览无余”，加密看上去是唯一的解决方案。1918 年，德国发明家亚瑟·谢尔比乌斯（Arthur Scherbius）发明了史上最“坚不可摧”的加密系统之一——Enigma（恩格玛机）。Enigma 可以采用近一亿亿（10^{16}）种可能的组合对明文进行加密，想通过人工暴力进行破译无异于大海捞针。我们将在第 4 章详细介绍 Enigma 的工作原理。二战期间，德军陆续装备了三万台 Enigma 用于海、陆、空各大战场，Enigma 的复杂性导致盟军完全无法掌握德军的动态，只能在一次次作战中接连失利。1939 年，图灵和一大批数学家、语言学家、象棋冠军以及填字游戏高手集中到英国伦敦郊区的布莱切利庄园，开

Enigma 是人类进入机械化密码时代的开始。

这段尘封的往事通过传记电影《模仿游戏》被搬上了荧幕。

Bombe 意为半球形冻甜点、筒状高压气体容器、钢瓶、炸弹。

始为破译 Enigma 而努力。一开始采用的手工破译方法效率低下，破译工作一度陷入困境，往往德军的军事行动已经结束，电文中的大概意思才被参透。图灵决定另辟蹊径，他力排众议，在丘吉尔的支持下，继续了波兰密码学家马里安·亚当·雷耶夫斯基（Marian Adam Rejewski）的前期工作，最终制造了克制 Enigma 的天敌——Bombe 机。Bombe 机是盟军反败为胜的关键，据估计，Bombe 机的出现让战争至少缩短了两年，从而事实上挽救了无数人的生命。不过很可惜，因为其专用性及其机密性，二战后，Bombe 机就被拆除了，也导致其与“第一台电子计算机”之称失之交臂。

3. 第一台数字式电子计算机诞生

图灵不但是计算机科学的奠基人，也是人工智能之父。

在最初的图灵机模型中，程序是固定的，那么是否可以制造这样一台机器，能够模拟任意一台图灵机呢？答案是肯定的，我们称这样的图灵机为通用图灵机，图灵将其命名为 U（取自“Universal”一词）。通用图灵机可读取描述特定机器算法和输入的编码指令，并自动执行这些指令以完成任务。通用图灵机是一种对计算过程的模拟，另一位天才数学家约翰·冯·诺依曼（John von Neumann）将这一理论设想变为了现实[4]。

1944 年夏天，在阿伯丁火车站（英国苏格兰城市阿伯丁的主要火车站），冯·诺依曼邂逅了正在参与 ENIAC 计算机研制的科学家赫尔曼·戈德斯坦（Herman H. Goldstine）。彼时，美军的弹道研究实验室正在为大量投入使用的新型大炮和导弹计算射击表，每种型号的炮弹需要针对不同条件进行上千次弹道计算，其中还涉及复杂的微积分运算，实验室迫切需要一种自动化、高精度、高速的计算工具，ENIAC 的开发正是源于这一需求。由于当时的机械计算机难以达到要求，研究者们开始尝试使用电子管和电子电路搭建“全电子数字计算机”。在短暂交谈中，敏锐的冯·诺依曼被 ENIAC 计划所吸引，随后作为顾问加入了 ENIAC 研制组。1946 年，ENIAC 完工。尽管这时二战已经结束，ENIAC 没有实现帮助打赢战争的初衷，但仍然被军方继续应用于氢弹设计和随机数研究等各方面。ENIAC 的成功证明了电子计算机设计思想的可行性，至此，信息时代真正拉开了序幕。

由于 ENIAC 采用十进制的方式进行计算，且程序和计算分离，内部结构和编程的过程都极度复杂，如果想要执行一个新的计算任务，需要通过插头和开关对线路进行重新配置，这导致在 ENIAC 上运行一个应用程序往往需要耗费几周的时间，因此 ENIAC 在一段时间内通常只用于解决某一个问题，其通用性很差，利用率也不高。如果程序可以像数据一样通过某种介质长期存储在

机器内部，通过开关进行任务自动切换是不是就可以提高通用性呢？研究者们也想到了这一点。在 ENIAC 尚未完工之际，他们就着手研制一台可以存储程序的新机器，这台新机器被命名为“电子离散变量自动计算机”（EDVAC ）。EDVAC 采用二进制，并且增加了程序存储功能，以达到“动态”编程和自动配置的目的。当它开始处理一件任务时，程序指令和数据通过二进制编码读入机器的存储单元并执行。1946 年，冯 • 诺依曼基于 EDVAC 的设计和基础架构，扩展完成了长达 101 页、影响计算机历史走向的《EDVAC 报告书的第一份草案》（*First Draft of a Report on the EDVAC*）。该草案不仅详述了全球第一台通用数字电子计算机 EDVAC 的设计，还提出了著名的冯 • 诺依曼体系结构，其核心思想包括存储程序以及二进制编码等。存储程序思想可以说是由图灵等许多科学家的理论思想衍化而来的。通用图灵机能够根据纸带上的策略信息模拟任意图灵机的行为，纸带是存储器，策略信息就是程序，这正是存储程序最早的思想萌芽。

现在看来是理所当然的想法，在当时却闪耀着划时代的光芒。

如图1.3所示，冯 • 诺依曼体系结构包括运算器、控制器、存储器、输入设备、输出设备五大部件。它构造了一种基于中央处理单元、可编程、可存储的计算机。中央处理单元执行所有逻辑和算术运算。使用二进制表示数据，并将程序和数据一视同仁，将程序编码为数据，一同存放在存储器中。这种存储程序控制的设计解决了程序硬件化的弊端，使得硬件和软件分离，大大促进了计算机的发展。

冯 • 诺依曼体系结构也被称为普林斯顿结构，与之对应的还有哈佛结构。哈佛结构使用两个独立的存储器模块，分别存储指令和数据。

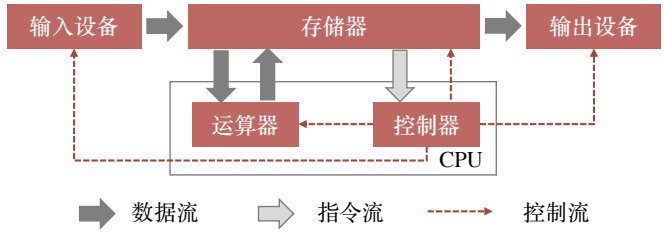


图 1.3　冯 · 诺依曼体系结构

4. 计算机系统

回顾历史，通常认为图灵赋予了计算机灵魂，冯 • 诺依曼搭建了计算机的骨架和血肉。时至今天，尽管硬件设备不断更新，但几乎所有的通用计算机都仍然遵循冯 • 诺依曼体系结构。1971 年，Intel 生产的 4004 微处理器将运算器和控制器集成在一个芯片上，CPU 由此诞生。如图1.3所示，冯 • 诺依曼体系

中的运算器和控制器就是 CPU 的主要组成部分，存储器主要对应为内存，输入和输出模块也被芯片化后集成到主板。它们发展成为计算机系统中的硬件系统。我们可以从文献 [5] 中了解计算机各个组件的基本工作原理。

CPU 是计算机系统的运算和控制核心，可谓是计算机系统的大脑。CPU 内部的功能实现由指令集具体完成，这些指令代码的底层实现并不开放，我们无法知道它们的安全性。一方面，它们可能集成了陷阱指令、病毒指令等，在潜伏中伺机而行。另一方面，CPU 可能本身存在技术缺陷，一旦这些底层的硬件设计漏洞和缺陷被攻击者发现和利用，就可能产生巨大危害[6]。1991 年海湾战争中，伊拉克防空雷达系统和各种通讯设施受到强烈的电子干扰，先后瘫痪；2007 年，以色列利用叙利亚预警雷达系统中的通用处理器后门突破防空系统，摧毁了隐藏在沙漠深处的一处核设施；2010 年，伊朗布什尔核电站在信息系统物理隔绝的情况下遭到“震网”病毒的攻击 …… 一系列血淋淋的现实告诉我们，只要存在国家和利益斗争，CPU 具有后门和被利用的风险就永远存在[7]。百万雄师在新型信息化综合作战场景下可能变得不堪一击。

除了硬件系统外，以操作系统为主体的软件系统则是计算机系统中的另一大组成部分。操作系统并不是与计算机硬件一起诞生的，它是在人们使用计算机的过程中，为了提高资源利用率以及增强计算机系统性能，伴随着计算机技术本身及其应用的日益发展，而逐步地形成和完善起来的。操作系统作为支撑软件，不但负责管理硬件系统，还支撑着其他应用程序的正常运行。一旦操作系统自身存在安全问题，譬如因开发设计不周而留下了可供利用的漏洞和破绽，无疑将给整个计算机系统带来巨大风险。我们将分别在第 6 章和第 7 章对计算机系统的硬件安全和操作系统安全进行详细讨论。

1.1.2 改变人类生活方式的互联网及其通信协议 TCP/IP

信息无处不在。信息理论首先把数学与电气工程学联系到了一起，随后又延伸到了计算领域[2]。信息理论推动着科技领域的前进，而各领域的发展也不断改变着信息传递的方式。从会说话的鼓到电报的发明，信息处理和编码方式不断取得进步，而计算机的发明和互联网的产生为信息编码和信息传递带来了翻天覆地的变化。

1. 互联网诞生

Sputnik 俄语意为“旅行伴侣”。

互联网的诞生始于人类第一颗人造地球卫星 Sputnik进入太空后发出的“哔

哔”信号声。1957 年 10 月 4 日，苏联将只有沙滩排球大小的 Sputnik 送入了近地轨道，这一事件传遍全球，美国国防部（United States Department of Defense，DoD）迅速做出响应，组建了高级研究计划局（Advanced Research Projects Agency，ARPA），开展科学技术在军事领域的应用研究。ARPA 的核心机构之一，信息处理处（Information Processing Techniques Office，IPTO），致力于解决网络通信等问题，并开展超级计算机等领域的研究。到了 20 世纪 60 年代，古巴核导弹危机发生，美苏进入冷战状态，越战爆发，“实验室冷战”开始，美国意识到需要一种不受核攻击影响的通信系统，避免集中军事指挥系统或电话系统可能被某一次核打击摧毁致瘫。

互联网的诞生，首要的驱动力，即互联的内在驱动力，来自于“冷战”这一特定的应用需求。

我们可以想象一下，在军事系统中，如果仅有一个集中的指挥中心，一旦被摧毁，那岂不是所有的军事指挥都会瘫痪了？设计一个分散的指挥系统太有必要了。这些分散的系统，不但需要保证在一个点或部分点被摧毁后整个系统能正常工作，还需要确保彼此之间能够通信。1962 年，IPTO 的第一位主任约瑟夫 • 利克莱德（Joseph C.R.Licklider）提出将当时被视为“大型计算器”的计算机连接到一起形成一个“星际”网络并进行相互对话和资源共享，以保证发生核攻击时即使部分节点被摧毁，美国通信网络仍然能够正常运行。

1967 年，ARPANET 之父拉里 • 罗伯茨（Lawrence G. Roberts）来到 ARPA，着手筹建这样一个“资源共享的分布式网络”，其核心思想即让 ARPA 的计算机互相连接，从而使大家分享彼此的研究成果，这就是 ARPANET 的起源。1969 年 9 月 2 日，在加州大学洛杉矶分校实验室，约 20 名研究人员完成了 UCLA（加州大学洛杉矶分校）与 SRI（斯坦福研究所）的两台计算机之间的连接，ARPANET 自此诞生。1969 年 10 月，ARPANET 完成了第一次通信。当然，ARPANET 早期面向的对象仅是彼此信任的研究机构或军事机构，通信过程的安全性并不在考虑范畴，这也一定程度上导致了现在互联网面对安全问题的困难局面。

ARPANET 的成功还得益于两项重要的技术发明：分组交换技术和 TCP/IP 协议，接下来分别介绍这两种技术。

2. 分组交换

实现计算机互连有一个重要的问题有待解决，即如何将数据信息传遍整个网络且只有接收方才能真正拆开这个信息。显然，让分布在各地的计算机彼此一对一相连进行数据传输是不现实的。

1948 年，克劳德 • 艾尔伍德 • 香农（Claude Elwood Shannon）在 *A Math-*

ematical Theory of Communication[8] 一文中提到通信的基本问题是在一个点上精确地或近似地再现在另一点上选择的消息。事实上，通信的本质即数据交换，数据交换的实现与数据线路的连通性息息相关。

“通信的数学理论”是信息论的奠基性论文，截至 2021 年 6 月 2 日，Google Scholar 引用已经达到 86863 次。

电路交换是早期的数据交换方式。电路交换首先需要建立连接，且在通信过程中该连接将被独占，因此实时性和稳定性都较好，但利用率较低。如何提高数据通信的效率成为构建网络的一大关键技术难点。

1961 年，麻省理工学院的伦纳德·克莱因洛克（Leonard Kleinrock）完成了自己的博士论文 *Information Flow in Large Communication Nets*[9]，这篇论文被认为是分组交换理论的首篇论文，为分组交换提供了数学理论，也奠定了互联网的技术理论基础。基于该论文，1964 年，克莱因洛克完成了第一本关于分布式通信理论的书《通信网络：随机的信息流动与延迟》（*Communication nets: stochastic message flow and delay*）[10]。无独有偶，事实上在同一时期提出“分组交换”思想的还有两批研究人员：1964 年，美国兰德公司的保罗·巴兰（Paul Baran) 提出了基于分组交换技术和分布式冗余的抗毁网络[11]；1965 年，英国国家物理实验室的唐纳德·戴维（Donald Davies）[12] 也提出了替代电路交换的分组交换概念。

这段历史详见参考文献 [13]。

分组交换，顾名思义，是一种拆分并发送数据的方法。信息被分解成一系列离散的“数据包”，单独发送到目的地，并在目的地重组。分组交换的方法增加了数据传输的可靠性，也不需要像电路交换一样独占专用链路，多个用户可以共享一条物理链路，因此也具有更高的利用率。

1969 年，军事承包商 Bolt Beranek & Newman 公司（即 BBN 科技公司）开发了一种新型的设备，称为接口消息处理器（Interface Message Processor，IMP），它可以部署到网络的任意位置，采用存储转发的方式协助进行数据包交换。现在网络中的核心路由器实现的就是当年 IMP 的主要功能。

3. TCP/IP 协议的产生

ARPANET 产生之前，连接每台远程计算机都需要一个专用的终端。例如，在办公室，你需要 3 台终端连接位于不同位置的 3 台计算机，而且这 3 台计算机因为使用的协议不同还无法相互通信。为了操作位于不同位置的计算机，你不得不将椅子滑来滑去，在不同的工作台之间来回切换。随着 ARPANET 向非军事部门开放，分组交换计算机网络规模不断增长，彼此不兼容的问题显得更为突出。如何将各种不同型号、不同操作系统、不同数据格式的计算机连在

一起实现通信并共享资源成为最大的难题，科学家们为此煞费苦心。显而易见，为了保持公平，最好的办法就是开发一种与硬件和软件无关、统一、通用的网络通信协议或数据处理规则，确保不同的计算机之间能按照规则自由“打招呼”和“握手”。1970 年 12 月，网络控制协议（Network Control Protocol，NCP）被提出，但其扩展性不足，对于节点和用户数量有限制，且缺少纠错功能，无法保证可靠性，因而没有被广泛接受。同一时期，也在开展相关研究的温顿·瑟夫（Vinton G. Cerf）和罗伯特·卡恩（Robert E. Kahn）意识到只有深入理解各种操作系统的细节才能建立一种对各种操作系统普适的协议。在分组交换理论的基础上，1972 年，瑟夫和卡恩提出开放的网络架构和 TCP/IP 协议，一方面它提供了端到端的数据传输控制，另一方面还提供了在网络间进行寻址和路由的机制，这为在不同的网络间进行数据交换提供了统一的标准，也促成了路由设备的出现。TCP/IP 就像邮件传递一样，通过 IP 唯一标识数据投递的地址，并将消息进行打包传递。其中，TCP 协议被称为传输控制协议，负责监督数据传输的过程，一旦发现问题则要求重新传输。1980 年，UNIX 操作系统发布了首个支持 TCP/IP 协议的版本 4BSD；1983 年，TCP/IP 成为 ARPANET 上的标准协议；1985 年，美国国家科学基金会（National Science Foundation，NSF）建设了覆盖全美主要大学和研究机构的国家科学基金会网络（The National Science Foundation Network，NSFNET）；1991 年，美国政府放开了对互联网的接入限制；1993 年，NSFNET 开始被若干商用互联网主干网替代；1995 年，NSFNET 宣布停止运作，从此，互联网正式进入普通大众的生活。

瑟夫和卡恩凭借 TCP/IP 通信协议的贡献获得 2004 年度图灵奖。

TCP/IP 协议至今仍然是全球互联网得以稳定运行的保证，开放分层的互联网体系结构成为互联网的基础和核心。如图1.4，尽管相比 OSI 模型，TCP/IP 协议族已经尽量简化，但仍然具有一定复杂性，在设计和实现过程中不可避免会存在漏洞或缺陷。解决 TCP/IP 协议栈的安全问题也成为解决网络空间安全问题的前提和基础。我们将在第 8 章对协议栈的安全进行详细讨论。

1.1.3 从 Web 开始的互联网应用大爆炸

互联网建设之初，尽管计算机可以彼此建立联系并交换信息，但使用并不方便。不同的计算机拥有不同的信息资源，如果你需要获取这些信息，就要连接到不同的计算机。如果能把信息共享出来，让所有的人都能看到多好。事实上，信息共享的想法早在互联网发明之前就有人提出过。

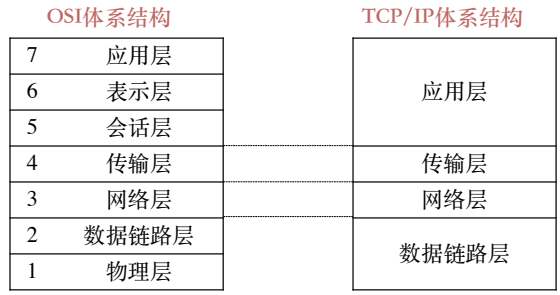


图 1.4 OSI 和 TCP/IP 体系结构

诚如所思，意即我们可以用机器来实现思维。

1945 年，二战即将结束，曼哈顿计划负责人范内瓦·布什（Vannevar Bush）在美国极有影响力的杂志 *Atlantic Monthly* 7 月号上发表了一篇名为 *As We May Think*[14] 的文章。在这篇论文中，他想表达这样一种思想：我们使用的信息是碎片化的，而大脑是通过联合协作来工作的，它可以从一个主体自动链接到下一个主体，那么如何通过机器来完成人类思维跳跃这样的操作呢？在该文中，他设计了一种机器，并将其命名为 Memex（如图1.5所示）。这是一个机械化的信息数据库，它可以模仿人类思维的关联过程，将一条信息链接到与之相关的信息，由此建立信息导航，并作为永久记录供后续读者使用。Memex 将传统图书馆的文献存储、查找机制与计算机结合起来，使得人类管理日益增长的信息成为可能。我们知道，1945 年，计算机还没有普及，布什的理论开创了超文本链接和 Web 浏览的雏形。到了 1965 年，美国的泰德·纳尔逊（Ted Nelson）正式提出超文本（Hypertext）的概念。

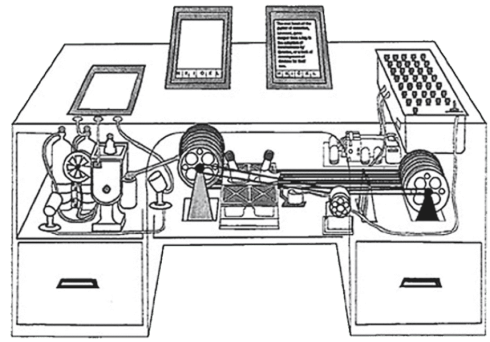


图 1.5 Memex

1980 年，英国计算机科学家蒂姆·伯纳斯-李发现使用超文本新技术可以使分布在各地的计算机分享和更新信息，他创建了用于存储信息的软件系统

“ENQUIRE”，并将该系统用于他当时就职的 CERN 内部，帮助大家进行文档和信息交流。这也成为 WWW 这一伟大工作的序曲。1990 年，伯纳斯-李提出了支撑 Web 的三种基础技术：一个统一资源定位系统（Uniform Resource Locator，URL）、一种通信协议 HTTP 和一种创建网页的语言 HTML，并以自己的 NeXT 计算机作为服务器，开发出世界上第一个网络服务器和第一个客户端浏览器编辑程序，建立了全球第一个 WWW（World Wide Web）网站 info.cern.ch，幸运的是，至今这个网站仍然运行正常。我们可以尝试登录一下，一睹它的风采。发展必然伴随着困难，事物前进的道路并不总是一帆风顺的。事实上，每天都使用 WWW 的你根本想不到，WWW 在开发之初并没有得到认可，我们可以从伊恩·瑞彻（Ian Ritchie）在 TED 的演讲中了解到这段历史[15]。

为防止 NeXT 被意外关闭，伯纳斯-李用红色墨水手写了一个标签：“这台机器是服务器。请勿关闭电源!!”

World Wide Web 中的 World Wide 颇具深意，正如伯纳斯-李的推文 *This is for everyone* 所指，开放和去中心化永远是伯纳斯-李的研究目标和准则。我们可以试着假设一下，如果没有 WWW，互联网可能还只是 IT 技术人员的专用工具。此外，Web 成功的原因还在于其良好的可扩展性，包括相对自由的组织方式、简单易操作（低门槛）的信息发布方式和分布式的架构。事实上在 Web 之前也有很多超文本的实践，但都因为复杂性并没有取得成功，对于大众而言，没人愿意在使用一个产品之前要先学一大堆专业的技能，伯纳斯-李改变了全球信息交流的模式，促进了互联网的飞速发展。当前的 Web 已经从 Web 1.0 发展到动态交互的 Web 2.0，以及面向人工智能、区块链等的 Web 3.0。当然，开放、共享、可扩展也就意味着数据的安全和隐私更容易发生泄露，从 2009 年至今，伯纳斯-李一直致力于解决数据的开放、安全和隐私问题。本书中，我们也将在第 5 章对网络空间中的隐私保护问题展开讨论。

伯纳斯-李因为发明了万维网、第一个浏览器和使得万维网得以扩展的基础协议及算法等贡献，于 2016 年获得了图灵奖。

1.1.4 网络战争的打响

互联网的设计源于彼此信任的团体或研究机构间的通信需求，因此 ARPANET 诞生之时并未考虑数据通信的安全问题。1969 年，一群高中生入侵了本该由五角大楼管理的封闭军事网络，网络的安全问题开始受到关注。1972 年，ARPANET 的一些用户惊讶地发现自己的计算机屏幕上显示了这样一条信息“I’M THE CREEPER: CATCH ME IF YOU CAN”，他们不知道这条消息从何而来。事实上，这条消息是 ARPANET 的一名研究员鲍勃·托马斯（Bob Thomas ）创建的。他意识到计算机程序可以在网络中移动，无论它走到哪里，都会留下一条痕迹。于是，他创建了一个名为“爬行者”（Creeper）的计算机程

序，在 ARPANET 的 Tenex 终端之间“旅行”并在途中留下自己的打印痕迹，当然这条消息并不是恶意的。电子邮件的发明人雷·汤姆林森（Ray Tomlinson）对此表示出了极大的兴趣，他进一步提升了 Creeper 的能力，使其能够自我复制，第一个计算机蠕虫由此产生。同时，他也编写了另一个名为 Reaper 的程序，用于追逐 Creeper并将其删除。这也是防病毒软件的第一个示例。

Creeper 揭示了网络存在安全缺陷，某些别有用心的人也意识到了这一点，他们开始寻求渗透网络并窃取重要数据的方法。

1978 年，温顿·瑟夫和罗伯特·卡恩建议在互联网的核心协议中内置加密功能以增加黑客入侵系统的难度。但这一建议受到美国情报部门的干预，并未被采纳。在当前的互联网上，为了确保日益增长的海量数据通信安全，用户不得不部署大量复杂的密码算法、采用各种认证系统，这对用户端设备和网络设备都提出了更高的要求。

没有保护的网络变得越来越脆弱，而病毒变得更加聪明，互联网病毒逐渐演变成为大流行病，扩散迅速，带来的危害也越来越大。它不再是学术上的恶作剧，而真正成为严重的威胁。网络开始被作为武器使用。1986 年，美国劳伦斯伯克利国家实验室的天文学博士、“网管”克利福德·斯托尔（Clifford Stoll）在就职的第 2 天就接受了一个艰巨的任务——调查是谁在当月蹭了 9 秒实验室的网，导致实验室少收入 0.75 美元。没过多久，斯托尔就追踪到了一位神秘的入侵者“Hunter”，但他是谁，又是如何成功蹭网的呢？在接下来的一年时间里，没有经费支持、没有前人经验的斯托尔顺藤摸瓜，发明并开启了入侵检测、数字识别、利用蜜罐钓鱼执法等多种技能，破获了黑客史上的第一件间谍大案，德国计算机黑客马库斯·赫斯（Marcus Hess）因此被抓捕。据估计，他入侵了包括五角大楼大型机在内的 400 多台军用计算机，并意图获取关于里根总统战略防御计划等大量机密情报以倒卖给苏联克格勃[16]。

那么，当时伯克利实验室网络的收费标准是每小时多少美元呢？

1988 年，信息产业迅猛发展，越来越多的大学、军事机构和政府与互联网建立了联系。这也意味着对安全措施的需求越来越大。这一年，无数大事件都没有一只小蠕虫来得令全世界震惊和难忘。就是这一年，康奈尔大学的研究生罗伯特·莫里斯（Robert Tappan Morris），利用 UNIX 系统的漏洞创造了一只蠕虫病毒，尽管这只蠕虫病毒创建的初衷并非要对网络实施破坏，但它在被感染的计算机上挤占了系统硬盘和内存空间，疯狂自我复制并传播，在 12 个小时内迅速感染了当时 10% 以上的互联网主机，使得网络陷入瘫痪。莫里斯病毒标志着首个具有主动攻击能力的网络蠕虫出现，催生了防病毒软件产业，也促使各系统开发商更加重视系统安全漏洞和网络安全。

莫里斯蠕虫的爆发使得莫里斯成为根据《计算机欺诈和滥用法》成功被起诉的第一人，催生了“计算机应急响应小组”CERT 的成立，推动美国总统里根签署了《计算机安全法令》。

2010 年 6 月，白俄罗斯安全公司 VirusBlokAda 受邀为伊朗的计算机进行故障检测，调查这些计算机反复崩溃、重启的原因。技术人员经过分析，发现了一

种复杂的网络数字武器，并根据代码中的关键字将其命名为“震网”（Stuxnet）病毒。随着对“震网”病毒的深入研究和分析，研究者们得到了惊人的发现，这一款病毒的精妙和复杂程度超乎想象。它利用了 5 个 Windows 漏洞，其中包括 4 个零日漏洞。此外，“震网”病毒还包含两个专门针对西门子工控软件 SIMATIC WinCC 的漏洞攻击，这种攻击方式在当时简直是闻所未闻。事实上，这是一款针对伊朗纳坦兹核工厂量身定做的数字武器。2006 年，伊朗重启核计划，在纳坦兹核工厂安装大批离心机，进行浓缩铀的生产，为进一步制造核武器准备原料[17]。出人意料的是，核工厂的运行极不稳定，出厂时质量合格的离心机，一旦投入运行故障率则居高不下。而导致这一问题的“罪魁祸首”正是“震网”病毒。如图1.6所示，“震网”病毒分三个阶段实施攻击。首先，它通过带有病毒的 U 盘感染存在快捷方式解析漏洞（MS10-046) 的计算机。然后，它将不断复制，并利用打印后台程序服务模拟漏洞（MS10-061）和远程代码执行漏洞（MS08-067）使其在局域网里扩散，并查找安装了西门子 WinCC 系统的服务器。最后，它利用 WinCC 系统中的 Step7 工程文件缺陷，接管西门子特定型号的可编程逻辑控制器（Programmable Logic Controller，PLC），让离心机表面上运转正常实际上却大幅提高转速，使其运行在临界速度以上，导致离心机迅速被毁坏。“震网”病毒的攻击过程之复杂令人瞠目结舌，这也让它摘得了业界的多个“桂冠”。它是第一个利用了多个零日漏洞的蠕虫攻击、第一个包含 PLC Rootkit 的计算机蠕虫、第一个盗用签名密钥和有效证书实施的攻击、第一个以关键工业基础设施为目标的蠕虫，它被认为是世界上第一款数字武器，也是最早导致实际物理损坏的已知数字攻击之一。“震网”病毒的里程碑意义并不在于其相对其他简单的网络攻击具有更高的复杂性和高级性，而在于它发出了这样一种信号：**通过网络空间手段进行攻击，可以达成与传统物理空间攻击（甚至是火力打击）等同甚至更好的效果**[18]。从此以后简单的数据窃取或信息收集不再是网络攻击的唯一目标，针对各种基础设施的网络安全对抗成为各国军事较量的新战场。

“零日漏洞”也被称为零时差漏洞，是指被发现后尚未得到修复即被攻击者恶意利用的安全漏洞，通常具有极大的突发性和破坏性。“震网”病毒中使用的 4 个零日漏洞分别为 MS10-046、MS10-061、MS10-073 和 MS10-092。

俄罗斯安全公司卡巴斯基实验室发布了一个声明，认为“震网”病毒“是一种十分有效并且可怕的网络武器原型，这种网络武器将导致世界上新的军备竞赛，一场网络军备竞赛时代的到来”，且“除非有国家和政府的支持和协助，否则很难发动如此规模的攻击。”

很显然，“震网”病毒为政府和其他组织建立了通过互联网实施重大破坏这一可能性的新认知。2013 年的斯诺登事件再次说明了这一点。自 2020 年 3 月以来，美国政府机构，包括其核武器试验室，陆续被黑客攻陷。黑客使用“供

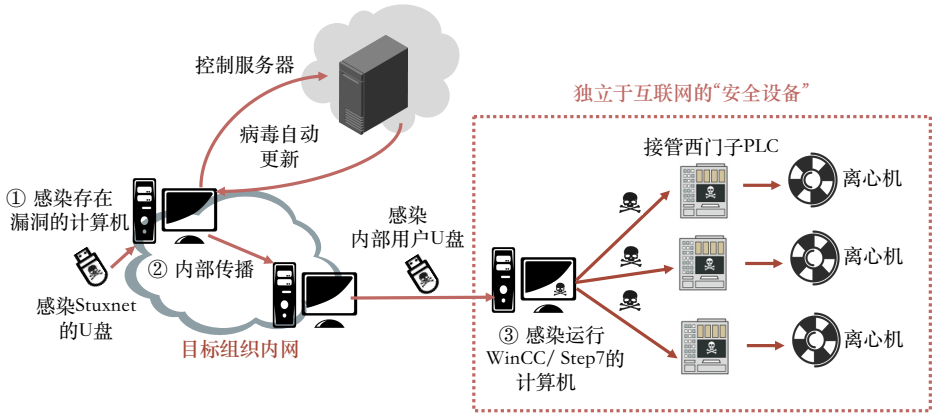


图 1.6 “震网”病毒传播过程

供应链攻击是一种面向软件开发人员和供应商的新兴威胁。黑客利用用户对厂商产品的信任，在应用下载安装或者更新时进行恶意软件植入。

C-Brain 诞生于 1987 年，由一对巴基斯坦兄弟编写，其初衷是惩罚那些非法复制他们软件的客户。C-Brain 利用病毒覆盖非法客户软盘上的引导扇区，它被认为是计算机病毒的始祖。

应链袭击”的手段，在 SolarWinds Orion 网络监控软件更新包中植入木马化后门（软件供应链攻击），并针对美国关键基础设施 OEM 制造商发起了产业供应链攻击，由此，以点带面辐射了数以万计的政府部门和企业，使得 SolarWinds 恶意软件成为美国关键基础设施迄今面临的最严峻的网络安全危机。这一攻击方式与“震网”病毒有异曲同工之效。

实际上，网络攻击每天都在发生，并且还在不断发展。从计算机蠕虫到数据泄露，从高中生制造的“小型黑客攻击”到影响总统选举的隐蔽攻击，网络攻击的形式和规模千变万化，网络攻击的破坏性、影响力和隐蔽性越来越强。如图1.7所示，梳理网络攻击的发展历程可以看出，早期网络攻击主要来源于病毒传播，例如，C-Brain。随后发展成为蠕虫及漏洞攻击。大量未经保护的基础设

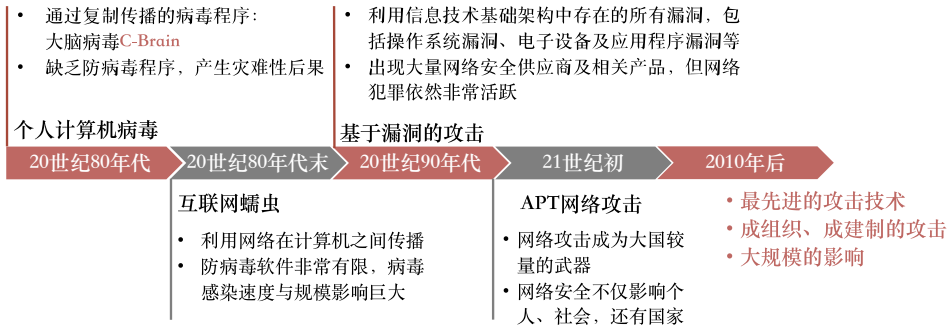


图 1.7 网络攻击的发展历程

施暴露在网络中，简单地使用在线提供的各种工具和技术寻找这些漏洞来开展

攻击对于黑客而言简直就是小菜一碟。犯罪分子可以利用网络间谍手段从银行窃取客户数据，或者通过精心策划的恶作剧造成严重破坏。到了 21 世纪，有计划、有组织地开展针对性强、持续时间长、隐蔽性好的攻击，即高级持续性威胁（Advanced Persistent Threat，APT）攻击成为高级新型攻击的代表，而频繁地使用网络攻击打击一系列军事甚至平民目标更成为各国军事部门的常用手段，网络空间安全已直接关系到国家安全。

1.2 网络空间及网络空间安全

互联网发展至今，应用规模持续增长，应用领域不断扩张，已经成为全球信息共享和交互的平台，并发展成为人类第五疆域：网络空间。伴随网络空间发展的是业已影响全球关键信息基础设施乃至国家安全的网络空间安全问题。本节，我们将介绍什么是网络空间和网络空间安全、网络空间安全的重要性及当前现状，并对全球网络空间安全战略进行简要介绍，最后重点介绍网络空间安全学科的体系架构。

1.2.1 网络空间定义及其特点

网络空间是伴随互联网技术的发展而来的。20 世纪 80 年代，作家威廉·吉布森（William Ford Gibson）在其短篇科幻小说《燃烧的铬》（*Burning Chrome*）中创造了“Cyberspace”一词用以描述虚拟的计算机信息空间，它将客观世界和数字世界交融在一起，彼此影响。Cyberspace 随着吉布森 1984 年出版的经典之作《神经漫游者》（*Neuromancer*）迅速风靡世界。据称，吉布森创造 Cyberspace 得益于 1948 年美籍奥地利数学家诺伯特·维纳（Nobert Wiener）首创的 Cybernetics 一词，该词源自希腊语 Kubernetes，意为“舵手、领航者、管理者”，中国学者把 Cybernetics 译为“控制论”，所以也有学者将 Cyberspace 理解为“控制空间”。事实上，Cybernetics 还强调了控制中的反馈，也就是隐含了通信的含义。

据不完全统计，从网络、信息、电磁等不同视角针对 Cyberspace 的正式定义近乎有 30 种。1991 年 9 月，《科学美国人》出版《通信、计算机和网络》专刊，就详细阐述了 Cyberspace 的概念，并谈到“Cyberspace 中的公民自由权”。国内对于 Cyberspace 的各类译文众多，有网络空间、信息空间、赛博空间、网络世界虚拟空间等。有关 Cyberspace 更多的译文和理解可以参考中国工程院戴浩院士的“赛博空间（cyberspace）概念的由来及译名探讨”[19] 一文。

戴浩院士是指挥与控制领域的著名专家，曾主持制订我军第一个中文微机接入计算机网络的标准规范，为我军指挥信息系统建设做出了重大贡献，被誉为我军指挥自动化网的“拓荒者”。

美国在 2001 年发布的《保护信息系统的国家计划》中首次提出 Cyberspace，即“网络空间”的表述，并在其国家安全 54 号总统令和国土安全 23 号总统令（这两项总统令通常缩写为 NSPD 54/HSPD 23）对 Cyberspace 进行了定义：“网络空间是连接各种信息技术基础设施的网络，包括互联网、各种电信网、各种计算机系统以及各类关键工业中的各种嵌入式处理器和控制器。在使用该术语时还应该涉及虚拟信息环境，以及人和人间的相互影响。”由此定义显而易见，**互联网是网络空间最重要的基础设施**[20]，**确保互联网的安全对于网络空间安全至关重要。**

从网络空间的要素出发，我们认为网络空间包含物理网络和在其上承载的数据及基于这些数据所做出的分析、决策和控制，代表了信息技术的最新发展状态和未来趋势。这个定义包含了网络空间的四个要素：计算机（硬件和软件）、数据资源、网络基础设施和通信链路，以及应用服务。这些要素相互关联、协作、融合，发展成为万物无限互联、数据无限积累、信息无限流动和应用无限扩展的网络空间，具体介绍如下。

（1）万物无限互联的网络空间：你是否曾经梦想过拥有一套最新款的钢铁侠战衣，它能够稳定飞行，进行目标扫描，提供全球定位等炫酷的功能。也许这个梦想并不遥远。事实上，可穿戴设备早在 1961 年就已经出现，彼时美国麻省理工学院数学教授爱德华·索普（Edward Thorp）和香农合作开发了一台可以放进鞋子的计时设备以帮助他们在轮盘游戏中获胜。今天，蓝牙耳机、健身腕带、谷歌眼镜，越来越多的可穿戴设备接入网络服务于人类。而随着移动设备的接入、社交网络和物联网的发展，网络空间已经容纳了物联网、车联网、工业互联网、空天地一体化网络、智慧城市、智慧医疗等数以亿计的新设备。信息网络连接和服务的对象从机器和人扩展到了万事万物，显然，万事万物互联带来的海量安全问题也不容小觑。

（2）数据无限积累的网络空间：当你在生活、学习和工作中碰到疑难杂症的时候，是不是首先想到的是找百度和谷歌？我们处在一个知识极大丰富的时代，能随时随地获取我们想要了解的一切，而这无疑归功于网络空间的海量数据积累。无限互联的各种事物、毫无时空限制的网络环境带来爆发性增长的海量数据产出和积累。这些数据规模庞大、复杂多样、增长迅速且可无限复制。文本、图像、多媒体等各种数据集合的规模从 GB 扩展到了 PB、ZB，而且仍然处于飞速增长中。国际数据公司 IDC（International Data Corporation ）在 *Data Age 2025* 白皮书中预测，到 2025 年，全球数据总量将达到 175ZB。当然，伴随着开放的网络，数据的隐私也荡然无存，大量软件和应用主动收集用

1GB=1024MB，1PB=1048576GB，1ZB=1048576PB。

户数据，小到个人兴趣偏好，大到国家经济状况等，这些信息积累与挖掘具有不可估量的价值，相应地，信息泄露和信息滥用问题也成为网络空间安全中的一个重要问题。

（3）信息无限流动的网络空间：互联网的本质是连通性，万物的互联、互通、互动带来的是信息在网络空间的无限流动。比尔·盖茨（Bill Gates）在1995 年出版的《未来之路》（*The Road Ahead*）一书中提到“信息高速公路将打破国界”。网络空间中的信息流动与传统社会中央向四周定向式的信息流动方式不同，信息流动超越了时空限制，呈现出一种去中心化的结构，从分散的任意点向网络空间任意点流动，具有更高的公平性和公开性，因此信息扩散也更加迅速和广泛。随着大容量、高带宽、长距离的新一代光纤接入网、卫星互联网等基础设施的发展，网络空间的信息流动将更加高效通畅。当然，确保这些基础设施的安全性对于网络空间安全而言也就尤为重要了。

（4）应用无限扩展的网络空间：伴随网络空间技术的发展和用户的增长，网络空间应用也在飞速发展，为适应更广泛的用户需求，应用服务提供商不断推陈出新。截至 2020 年 12 月，我国国内市场监测到的应用数量为 345 万款，这些应用涉及社交、教育、健康、购物、交通、医疗等各领域，改变着人们的生活和工作方式。丰富、复杂的应用由于设计、开发过程中存在诸多缺陷，也导致了大量应用漏洞的出现，甚至可能被恶意植入木马后门，成为网络空间攻防对抗的一大焦点。

极大丰富的数据资源，不断成熟的区块链和云计算等基础设施，不断发展的虚拟现实（Virtual Reality，VR）、增强现实（Augmented Reality，AR）、人工智能等技术，推进了网络空间的“智能化”和“虚拟化”，一个现实世界的数字版本，由现实世界投射而来且与现实世界融合的虚拟世界“元宇宙”（Metaverse）开始引起研究者们的关注。从字面上来看，Metaverse 中的 Meta 在计算机领域代表“元”，比如 Metadata 就是元数据，verse 则代表 universe（宇宙）的缩写。元宇宙一词最先出现于 1992 年 Neal Town Stephenson（尼尔·斯蒂芬森）的科幻小说《雪崩》（*Snow Crash*）中。斯蒂芬森在书中创造了一个与现实世界平行的三维数字空间，人们可以采用虚拟身份在其中自由活动。“头号玩家”的粉丝对“绿洲”一定不陌生，它拥有完整的、跨越实体世界和数字世界的经济系统，尽管“绿洲”的集中化特性与元宇宙的“去中心化”目标并不一致，但仍然被视为贴近元宇宙的一种展示。元宇宙实现了人工智能、机器学习、大数据分析、混合现实、区块链、物联网等多种技术的叠加和应用。2020 年疫情期间，诸如毕业典礼、演唱会等许多真实场景被搬到虚拟世界中，现实

Roblox、Epic、Genies 和 Zepeto 使用 Metaverse 来表示元宇宙，Facebook 曾使用 Live Maps，Nvidia 使用 Omniverse，Magic Leap 则使用 Magicverse 来表示这一全新的概念，也有称其为 AR 云、空间网络的。

与虚拟的世界被打通，人们开始将更多的时间和金钱投入虚拟世界，这成为网络空间发展的新趋势，也被视为元宇宙时代到来的前奏。

1.2.2 网络空间安全定义及其现状

由于网络空间内涵丰富，涉及领域广泛，网络空间安全目前也尚未有统一、标准的定义。这里，我们列出 ISO/IEC 27032:2012 和 ITU（国际电信联盟）对网络空间安全的定义，以分析网络空间安全的核心要素。在 ISO/IEC 27032:2012 中，网络空间安全定义为“网络空间中信息的机密性、完整性和可用性的维护”。国际电信联盟定义“网络空间安全致力于确保实现与维护组织和用户资产的安全属性，以抵御网络环境中的相关安全风险。其安全目标主要包括：可用性、完整性（包括真实性和不可否认性）以及保密性”。显而易见，这两种定义涉及的属性与信息系统安全一致，包括机密性、完整性和可用性。完整性确保信息不被未授权地修改或者即使被修改也能够被检测出来，它主要用于防御篡改、插入、重放等主动攻击。可用性保证资源的授权用户能够访问到应该享有的资源或服务，主要针对网络系统中路由交换设备、服务器、链路带宽等设备或资源的可用性攻击而言（如拒绝服务攻击）。保密性也称为机密性，用于保护信息内容不会被泄露给未授权的实体。当然，网络空间安全与信息安全并不等同。信息安全关注保护特定系统或组织内的信息（数据）的安全；网络空间安全侧重于保护网络基础设施及其构成的网络空间的整体安全。

网络空间所承载的信息已成为国家经济发展的战略资源，然而网络空间安全现状并不乐观，当前网络攻击方式越来越复杂，越来越智能，越来越隐蔽，针对网络空间的攻击领域不断扩张，网络空间中无论载体还是资源都成为被攻击对象。特别是物联网、云计算、大数据的发展，使隐私泄露问题日益凸显。从“震网”病毒到 2013 年的“棱镜门”，种种事件表明，网络空间在系统、网络、数据、应用等各方面均存在安全挑战。

媒介即信息表达的意思，即我们传输信息的方式与依赖的环境和信息本身一样重要。

加拿大传播学者赫伯特·马歇尔·麦克卢汉（Herbert Marshall McLuhan）在其1964 年出版的《理解媒体：论人的延伸》（*Understanding Media:The Extensions of Man*）[21] 一书中提到“The Medium is the Message ”（媒介即信息），这一名言改变着人们对网络空间安全的理解，甚至影响了美国空军在网络空间安全上的举措。事实上，在早期，政府和军队将网络空间等同于计算机、路由设备等网络通信基础设施，针对网络空间安全的注意力也就主要集中在对网络中基础设施的打击上，通过各种渗透手段，实现对基础设施的控制和破坏。

后来，人们进一步意识到网络空间不只包含网络中的通信设施，更包括网络之间的数据传输方式，它们是各种基础设施的关联者。网络中数据产生、传输的方式及其依赖的环境等与基础设施在网络空间安全中具有相同的地位。随着我们对“媒介即信息”的进一步深入理解，可以发现网络空间安全不仅有基础设施和数据信息的安全性，还包括网络空间涉及的所有媒介和要素，例如协议栈、操作系统、应用等。

根据各类全球互联网安全威胁报告归纳，我们总结网络空间安全现状如下：

（1）国家关键基础设施和网络关键设备面临瘫痪风险： 受到大规模分布式拒绝服务攻击、漏洞后门及病毒泛滥的影响，网络中大量主机和服务器、骨干路由器和交换机都可能成为被攻击目标。如图1.8所示，全球关键基础设施始终是黑客攻击的目标。据美国国土安全部报告，2005 年针对美国政府或私营部门的网络攻击就有 4095 起，到 2008 年已增至 72000 起。《2019 年中国互联网网络安全报告》统计结果显示，2019 年涉及我国政府机构、重要信息系统等关键信息基础设施安全漏洞的事件约 2.9 万起，同比大幅增长 42.1%。

图 1.8 关键基础设施受攻击概览

（2）网络数据面临泄露或被窃取的风险： 网络空间是存储、处理、交换和传输各种数据信息的载体，而互联网对于数据传输缺乏有效的安全保障。随着云计算、物联网、大数据、人工智能的发展，网络空间向工业、能源、军事及金融领域扩展和延伸，海量敏感数据被监听、窃取和滥用的风险越来越高。2016 年 9 月 22 日，全球互联网巨头雅虎证实，至少 5 亿用户账户信息在 2014 年遭人窃取，其中包括用户名及密码等敏感信息；2020 年，网络安全公司 Cyble 发现，53 万 Zoom 账号以及 2.67 亿 Facebook 账号在暗网上被低价叫卖。事实上，通过暗网或黑客论坛进行数据售卖的事件已经频繁发生，用户隐私受到严重威胁。

（3）网络应用服务可信性得不到保证： 网络通过各种各样的应用向用户提供服务，而利用应用漏洞发起的网络攻击比比皆是。除了应用自身的安全漏洞外，第三方的开发工具、软件模块中的安全漏洞同样会带来巨大的危害，前面提到的供应链安全攻击即是如此。2015 年引起轰动的 XCodeGhost 事件就是

由非官方渠道下载的自带后门的 Xcode 造成的。UNIX 之父肯 • 汤普森（Ken Thompson）在其图灵奖演讲 *Reflections of Trusting Trust* 中就提出过一种通过修改的 tcc 编译器产生后门的思路。

针对网络空间发起的攻击涉及网络设备、网络资源各层面。其中，还有一个特别值得注意的问题就是：网络源地址伪造。在互联网中，所有传输的数据包都会根据目的地址进行路由选择，然而整个转发过程并不对源地址进行认证。既然没人检查，那攻击者就可以随心所欲假冒源地址隐蔽身份，这也使得地址伪造成为众多攻击成功的一个基本条件。换句话说，如果互联网能解决好地址假冒问题，可以说网络空间安全问题就解决了一大半。我们将在第 10 章中详细讨论源地址伪造问题的解决方案。

1.2.3 网络空间安全战略

各国网络政策的调整和网络军事力量的加速建设使得网络空间弥漫的“火药味”日益浓烈，网络空间战略化、军事化和政治化引发网络空间的国际战略博弈、军备竞赛和国际秩序之争，网络空间安全战略成为新的国际竞争领域。

美国对网络空间安全的关注可以追溯到 1996 年成立的关键基础设施委员会。事实上，美国各届执政党都对网络空间安全给予了极大关注，并将加强网络中心战列为“核心能力”。2008 年 1 月，布什签署两份涉及网络空间安全的机密总统令，即前面提到的 NSPD 54 和 HSPD 23，主题为“网络空间安全与监控”；2009 年美国发布《网络空间政策评估报告》，对网络的国家战略资源地位和确保其安全的重要性进行了明确；2011 年 5 月，美国又发布了《网络空间国际战略》，指出“网络空间安全具有与军事安全和经济安全同等重要的地位”，同时提出七大政策，其中最“强硬”的一条规定是，“美国保留对网络攻击进行军事报复的权利，并正在努力提高追踪任何攻击来源的能力”；2015 年，奥巴马政府先后发布《网络威胁制裁令》和《网络威慑战略》；2016 年 2 月 9 日，美国白宫发布《网络空间安全国家行动计划》，提出全面提高美国数字空间安全的目标；2020 年 3 月，美国网络空间日光浴委员会发布具有“向前防御”（defend forward）概念的《分层网络威慑战略》，这份网络空间的综合性战略提出了六项政策、七十五条行动建议以支撑塑造行为（Shape behavior)、获益拒止（Deny benefits)、施加成本（Impose costs）三种战略手段，以期遏制大国崛起；2021 年 3 月 3 日，拜登新政府发布《临时国家安全战略指南》，分析了美国面临的国家安全威胁以及应对策略，提出将把网络安全放在首位。从

美国网络空间安全战略的发展可以发现，从早期的“全面防御”发展到“攻防结合”和“主动进攻”，其网络空间战略的主动性、进攻性不断增强。

俄罗斯自 20 世纪 90 年代独立以来，通过了《信息、信息化和信息保护法》《俄联邦国家安全构想》等一系列国家战略规划文件和法律法规，奠定了网络空间安全战略形成的基础。2000 年，俄罗斯颁布首份维护信息安全的国家战略文件《俄罗斯联邦信息安全学说》，随后几年先后出台了《俄联邦网络安全战略构想（草案）》《俄联邦国家安全战略》《关键信息基础设施安全保障法案》等一系列战略规划文件，从军事、外交等各角度建立了网络空间安全框架，明确了网络空间安全战略原则及行动方向。2017 年 2 月俄国防部长谢尔盖·绍伊古公开宣布了俄网络战军事力量的存在。

自 1992 年发布《信息安全框架决议》以来，欧盟在网络空间安全方面也发布了一系列政策法规，其网络空间安全战略日益成熟。2013 年欧盟发布《欧盟网络安全战略》，对网络空间安全的威胁来源及应对措施做了明确阐述。2017 年，欧盟通过修订后的《欧盟网络安全战略》，加强了盟友之间在网络安全领域的合作。2020 年，欧盟委员会发布《欧洲数据战略》，强调了网络空间技术主权意识。

我国也高度重视网络空间安全，自 20 世纪 80 年代开始进行信息化领导管理体制建设，以 1994 年颁布的《中华人民共和国计算机信息系统安全保护条例》为开端，形成了《国家信息化发展战略纲要》《网络安全法》等一系列网络安全法规体系。2014 年 2 月，党中央成立了网络安全和信息化领导小组，习近平总书记指出“没有网络安全就没有国家安全，没有信息化就没有现代化。网络安全和信息化是事关国家安全和国家发展、事关广大人民群众工作生活的重大战略问题。”2016 年 12 月，我国首次发布《国家网络空间安全战略》，对网络空间进行了界定，并强调了网络空间主权要点。

从各国网络空间安全战略的发展来看，全球网络空间安全战略呈现从被动监控防御到积极主动出击的转变，在网络空间战略向军事战略演变的同时，突出了网络空间在防御力、威慑力和进攻力方面的能力建设。

1.2.4 网络空间安全学科体系架构

随着网络空间安全问题成为全球关注的焦点，网络安全已经成为国家安全的一部分。继 2001 年教育部批准设立信息安全专业之后，2015 年 6 月，**教育部正式批准“网络空间安全”为一级学科**，以推动和普及信息安全全民教育水

自从教育部批准设立“网络空间安全”一级学科以来，很多专家学者已经开设了一批高水平的课程，编写了多本高质量的教材，比如 [22–25]，感兴趣的读者可以自行参考。

平，提升国家网络空间安全的整体实力。

互联网的规模越来越大，网络空间安全面临的挑战也越来越明显。吴建平院士对网络空间安全问题的特点进行了总结[20]，具体来说包括：

（1）网络空间安全是整体性的，不可分割的： 许多网络威胁涉及网络空间的各个方面，如计算系统、物理网络、应用等，其复杂性也增加了安全问题的隐蔽性。

（2）网络空间安全是动态而非静态的： 网络空间安全事件常常是动态发生的，导致很多网络故障无法重现，增加了问题分析的难度。

（3）网络是开放而非封闭的： 网络规模越大越开放，其应用价值就越高，而从安全问题的解决来说，越小越封闭的网络安全问题越好解决。然而网络安全事件一定是发生在开放环境下，这更增加了跟踪和溯源的难度。

（4）网络安全是相对的不是绝对的： 网络安全事件时刻在发生，但网络安全保障要有高成本的投入，且任何解决方案都是相对的，在成本一定的情况下，如何尽可能确保网络安全，是另外一个需要平衡的问题。

这里的相对指的是，解决方案是否有效，要看攻击者投入多大的攻击成本。

（5）网络安全问题是联系的不是孤立的： 许多网络安全问题具有共同性、国际性和关联性，它们不是孤立的，多实体、多国家协同解决网络空间安全问题成为一种趋势。

网络空间安全涉及领域广泛，问题错综复杂，但并非无迹可寻。网络空间面临从系统到数据、网络、应用各层面的安全挑战，国内外学者纷纷从不同的角度探讨网络空间安全内涵，构建网络空间安全研究体系[26]。本书中，我们将阐述吴建平院士提出的网络空间安全学科体系，该体系从计算机科学的视角，基于网络空间的定义，即物理网络等资源载体及其承载的信息对象出发，从基础理论、机制与算法、系统安全、网络安全及分布式系统与应用安全着手构建网络空间安全学科体系，如图1.9所示。其中，基础理论和算法是网络空间安全学科的基石，它们支撑系统、网络及应用安全的研究，我们将在第 2 章到第 5 章介绍这些基础理论、机制和算法。其中，第 2 章将详细介绍网络空间安全技术涉及的基础理论，包括图论、控制论、博弈论、最优化理论以及概率论等，并对如何使用这些基础理论来分析网络空间安全的问题进行探讨。第 3 章将围绕当前网络空间的代表性安全机制展开讨论，如沙箱、入侵容忍、可信计算、类免疫防御、移动目标防御、拟态防御、零信任网络等。第 4 章和第 5 章分别从数据加密和隐私保护的历史谈起，对公钥密码、对称密码、摘要与签名等数据加密技术以及匿名化、差分隐私、同态加密、安全多方计算等隐私保护技术进行概述。

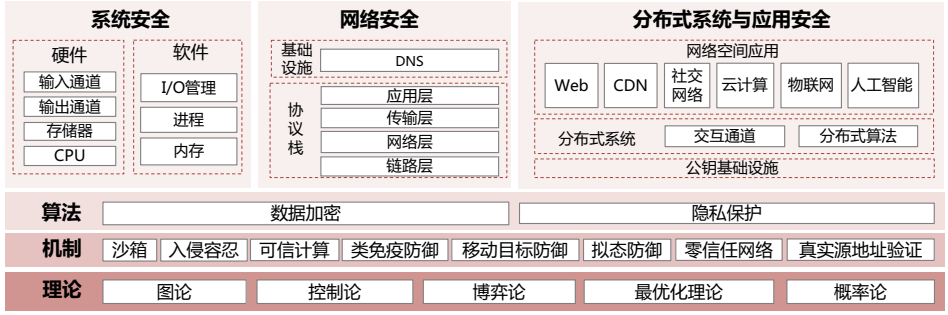


图 1.9　网络空间安全学科体系架构

（1）系统安全：计算机系统安全是网络空间安全的基础单元。计算机是网络空间的承载主体，计算机设备在硬件系统和软件系统的协同工作下实现“计算”功能。因此，通常我们从硬件安全和软件安全两个方面讨论系统安全的问题。硬件安全包括芯片等硬件和物理环境的安全，系统软件的安全则主要包括操作系统安全。本书第 6 章，我们将从计算机系统的主要硬件模块及其工作方式谈起，梳理硬件系统面临的主要安全威胁，剖析造成这些威胁的本质原因，并给出一些常用的硬件防护措施。第 7 章，我们将从攻击和防御两个角度分析与操作系统相关的安全问题。

（2）网络安全：网络空间中的各种物理设备通过网络连接起来进行信息传递，网络安全是网络空间可靠、安全运行的保障。具体来说，网络包括连接系统的中间设备、链路等基础设施以及相关的服务系统和管理系统。这其中，互联网是网络空间通信的基础，网络基础设施的安全和互联网体系结构都决定着网络空间的安全。如何保证接入网络的用户、设备和数据的安全可信，如何保证网络和其承载的信息基础设施可以向用户提供真实可信的服务是网络空间安全要解决的核心问题。我们将在第 8～10 章介绍网络层的典型安全问题，并挖掘这些安全问题后面的共性特征。第 8 章着重就 TCP/IP 协议栈的安全问题进行分析讲解，剖析导致协议栈安全问题的本质并给出基本的防御原理。第 9 章围绕 DNS 安全问题，对 DNS 缓存中毒攻击、恶意 DNS 服务器的回复伪造攻击和拒绝服务攻击等进行分析，探讨相应的防御对策。第 10 章从互联网体系结构的安全缺陷出发，探讨如何构建真实源地址验证体系结构，以阻断基于 IP 地址欺骗的攻击发生。

（3）分布式系统与应用安全：应用是网络空间中建立在互联网之上的应用或服务系统。以 Web 为首，物联网、大数据、人工智能等领域丰富的应用

是推动互联网发展到网络空间的重要原因。这些应用通常基于分布式系统实现，且由于复杂性等原因会带来一系列的安全漏洞，不完善的身份验证和访问控制措施、不当的数据库使用、存在漏洞的算法等都可能造成信息泄露的发生，第 11～14 章将围绕各种应用安全问题展开讨论。其中，第 11 章概述公钥基础设施及其安全问题。第 12 章就分布式系统的安全问题展开讨论，并对如何解决分布式系统中的安全协作及信任问题给出了建议。针对物联网、移动应用、CDN、云计算、社交网络等具体网络应用的安全问题将在第 13 章进行探讨。第 14 章将重点关注人工智能算法面临的主要安全问题、核心挑战，以及可能的解决方案。

1.3 网络空间基础理论之网络科学

要进行网络空间安全的研究，我们首先需要了解网络空间的特性，包括其结构特性及用户行为的规律等，例如，互联网是怎样“链接”的，流量拥塞是怎样产生的，病毒是如何在网络中传播的等等。随着互联网向网络空间发展，网络结构呈现出越来越多的层次化，网络资源不断扩张，形成异构、多层、跨域的互联，用户行为更加动态化，而在复杂交错的结构和行为中，网络空间又表现出一定的规律性。复杂的网络空间，需要运用复杂网络的理论和方法进行研究。本节，我们将探讨复杂网络与网络空间之间的联系，以及如何借助复杂网络的研究成果开展网络空间安全研究。

1.3.1 网络科学概述

我们的生活中有形形色色的网络，电话通信网、邮政网、物流网络、有线电视网络、互联网、万维网；还有社会关系网、产品供销网、金融借贷网等，这些网络都是由大量主体组成的复杂系统，尽管它们存在差异，但其结构彼此相似，究其根本实则为不同的“事物”实体，通过一定的“联系”关联在一起。我们将这些数量庞大的事物称为网络中的节点，用边来表示节点之间错综复杂的关联关系，并将这些网络称为复杂网络。在计算机领域，网络就是用物理链路将各个孤立的计算机相连在一起，组成数据链路，从而达到资源共享和通信的目的。**复杂网络呈现高度的复杂性和不确定性，很难用简单的方法进行分析，网络科学从字面上理解就是研究复杂网络的新兴学科。**

美国国家科学研究委员会（National Research Council，NRC）定义网络科学是利用网络来描述物理、生物和社会现象，并建立这些现象的预测模型，即

研究各种复杂网络的共性特征的学科。这一描述非常形象，毫无疑问，网络科学是一种用于分析复杂关系的有效手段。

维基百科也将网络科学定义为研究复杂网络的学术领域，这些复杂网络包括信息技术网络、计算机网络、生物圈网络、学习和认知网络等，它们主要由节点（顶点）表示不同元素或参与者，由连边表示元素或参与者之间的联系。该领域借鉴了数学中的图论、物理学中的统计力学、计算机科学中的数据挖掘和信息可视化、统计学中的推理建模、社会学中的社会结构等理论和方法。

1.3.2 复杂网络的性质

复杂网络呈现出高度的复杂性，包括结构复杂、连接多样、节点多样、节点状态动态变迁等，研究复杂网络通常从复杂网络的刻画和性质分析入手。

1. 复杂网络的特征参数

复杂网络包含社会中物理意义截然不同的多种网络，那么这些网络具有什么共同属性和特征呢？通常在刻画复杂网络的特征时，使用如下几个参数：度分布、平均路径长度、聚合系数、介数等。

（1）度分布：网络中某个节点拥有相邻节点的数目，即节点关联边的数目为该节点的度。如图1.10所示，节点 3 的度为 5。度分布 $P(k)$ 表示网络中度为 k 的节点出现的概率。我们后面会讲到，复杂网络中节点的度分布具有幂律特性。一般而言，**度越大的节点在网络中就越“重要”**，那也就意味着度大的节点被攻击产生的危害可能更大。

这一结论是否绝对成立呢？

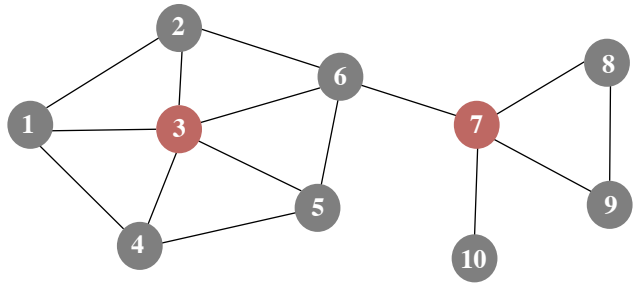


图 1.10 网络示意图

（2）平均路径长度：我们在网络中任意选择两个节点，那么连通这两个节点的最短路径就是这两个节点之间的路径长度。在图1.10中，节点 1 和节点 7

的路径长度为 3。网络中所有任意两个节点之间路径长度的平均值就是网络的平均路径长度，它反映了网络的全局特征。事实上，尽管多数网络规模很大且复杂，但其平均路径长度都相对较小。

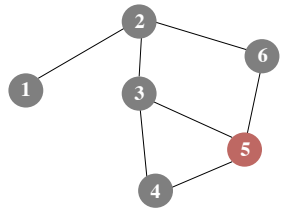
（3）聚合系数：节点的聚合系数定义为某节点的所有相邻节点之间连边的数目占可能的最大连边数目的比例。在图1.10中，节点 7 的 4 个相邻节点之间的实际连边数为 1，而其连边的最大可能数量为 6，则节点 7 的聚合系统为 1/6。网络的聚合系数为网络中所有节点聚合系数的平均值，网络聚合系数为 0 表示所有节点都是孤立点，为 1 表示网络中任意节点间都有边相连。聚合系数反映了一个节点的邻接点之间相互连接的程度，即节点间联系的紧密程度。比如在社交网络中，聚合系数表示你的朋友之间有多少是彼此认识的。

（4）介数：前面提到度的值是衡量一个节点重要性的参考指标，但也存在一些特殊情况，例如在某个网络中，有的节点度虽然小，但它可能是联系某些重要组织的关键点，如果该节点发生意外或崩溃，可能影响网络的连通性。为了衡量这种情况，复杂网络又引入了“介数”这一参数。点介数即为网络中经过某个节点的最短路径的数目占网络中所有最短路径数的比例。假设图 $G=(V,E)$ 中有某个节点 v，则节点 v 的介数可以表示为：

通常，我们利用编程来计算介数。那么，图1.10中各节点的介数各是多少呢？

$$B_v=\sum_{s\neq v\neq t\in V}\frac{\sigma_{st}(v)}{\sigma_{st}}$$

其中，σ_{st} 表示节点 s 和节点 t 之间的最短路径总数，其中经过节点 v 的路径条数表示为 $\sigma_{st}(v)$。例如图1.11中，节点 2 的介数为 4。边介数即为网络中经过某条边的最短路径的数目占网络中所有最短路径数的比例。介数的大小反映了节点的吞吐量、访问量、通行能力以及节点在复杂网络中的活跃程度，即某个节点的介数越大，在信息传递过程中该节点越容易发生拥塞。



节点	介数
1，4	0
2	4
3	3
5	1.5
6	1

图 1.11 介数示例

2. 复杂网络的性质

对于连接复杂多样的网络而言，使用什么样的拓扑结构来描述它比较合适呢？1959 年，两位匈牙利数学家保罗 • 埃尔德什（Paul Erdős）和阿尔弗雷德 • 瑞利（Alfréd Rényi）建立了著名的随机图理论（Random graph theory），用相对简单的随机图来描述网络。在随机图中，节点和边都以一定的概率由随机过程产生。随机图理论统治图论研究领域长达 40 年之久，也一度成为研究互联网拓扑结构的经典模型。它被用于描述一种病毒可能的感染途径、互联网的结构以及论文之间的引用关系等。

你应该有过这样的经历，你添加了一个微信好友，一天这位好友发了一条朋友圈，你赫然发现在这条朋友圈下点赞的除了你还有一个老熟人，原来你们拥有共同好友。或者你还会发现对你来说“遥不可及”的一些人，实际离你并不“远”，我们不得不感叹“原来世界这么小”。那么对于世界上任意两个人来说，借助第三者、第四者这样的间接关系来建立起两人的联系，平均来说最少要通过多少人呢？这是一个有趣的问题。1929 年，匈牙利作家弗里杰斯 • 凯伦斯（Frigyes Karinthy）撰写了一篇短篇小说，名为《链条》（*Láncszemek*，英语翻译为 *Chains* 或 *Chain-Links*），其中提到，随着交通与信息传播技术的进步，人际关系的亲密度将打破地域限制，他大胆假设，两个陌生人之间最多只需要 5 层关系就能联系起来，这就是“六度分隔”概念的最早表述。在 20 世纪 50 年代，伊赛尔 • 德索拉 • 普尔（Ithiel de Sola Pool）和曼弗雷德 • 科兴（Manfred Kochen）在撰写的一份手稿 *de Sola Pool and Kochen* 中，阐明了社交网络中的重要思想，其中包括通过连接链量化人与人之间距离的讨论。1967 年，美国社会心理学家斯坦利 • 米拉格（Stanley Milgram）招募了一批志愿者，选定了一名目标人物，以检验人与人之间社交联系的短路径的存在，以此研究社交网络的结构。这项具有里程碑意义的社会科学实验被称为“小世界实验”。在这项实验中，他获得了一个惊人的结论：**社交网络中，最多通过 5.5 个人（四舍五入，即为 6）你就能够关联到任何一个陌生人，这就是著名的“六度分隔”理论。**那么，“六度分隔”的理论是否在其他网络中也存在呢？

20 世纪 90 年代，美国影迷和大学生中流行一个有趣的游戏——找“贝肯数”，以确定某一个好莱坞演员与凯文 • 贝肯（Kevin Bacon）的“合作距离”。如果一个演员与贝肯曾合作出演过电影，那么他（她）的“贝肯数”就是 1。如果一个演员没有与贝肯合作过，但与某个“贝肯数”为 1 的演员合作演出过，那么他（她）的“贝肯数”就是 2，以此类推。通过对超过 133 万名世界各地

猜一猜任意两个网页之间的平均间隔是多少呢？两个 Facebook 用户之间的平均距离又是多少呢？

演员的统计得出，他们平均的“贝肯数”是 2.981，最大的也仅仅是 8。事实上，数学家们很早就开展了类似的研究，他们试图找到自己到图论先驱之一的保罗·埃尔德什（Paul Erdős）之间的“最短路径。埃尔德什发表的论文数高达 1500 篇，有 507 个共同作者。与“贝肯数”相似，如果一个数学家与埃尔德什合作过论文，则他的“埃尔德什数”就是 1，如果一个数学家至少要通过 k 个中间人（合作论文的关系）才能与埃尔德什有关联，则他的“埃尔德什数”就是 $k+1$。据统计，美国数学学会的数据库中记录了超过 40 万名数学家，他们的“埃尔德什数”平均是 4.65，其中最大的是 13，而大多数数学家的埃尔德什数都很小，只有 2~5。从这些数据中你是否发现了一些有趣的现象？它们后面是否隐藏一些特定的规律？事实上，科学家们针对电子邮件、MSN、Facebook 都进行了实验，尽管距离不同，但结论依然成立，现在我们知道，社交网络并不是仅有的“小世界”。

1998 年，美国的邓肯·瓦茨（Duncan J. Watts）和他的老师史蒂芬·斯托加茨（Steven Strogatz）在 *Nature* 上发表了 *Collective dynamics of 'small-world' networks*[27] 一文，指出许多具有泊松分布的复杂网络也具有“小世界”特性，由此解释了“六度分隔”的科学现象，同时提出了小世界网络模型。1999 年 10 月，*Science* 上发表了一篇由艾伯特-拉斯洛·巴拉巴西（Albert-László Barabási）和雷卡·阿尔伯特（Réka Albert ）撰写的论文 *Emergence of scaling in random networks*[28]，提出无标度网络模型，指出许多现实复杂网络节点的度分布具有幂律分布规律。这两个重大发现从根本上改变了人们对复杂网络的认识，结束了随机模型对于互联网拓扑结构分析的主导作用，更对现实网络及网络空间安全的研究产生了深远的影响，宣告了网络科学领域的正式形成。这之后，针对复杂网络的研究如雨后春笋，层出不穷。

（1）小世界特性

小世界特性也称为六度空间理论或者是六度分割理论（Six degrees of separation）。小世界特性指出，社交网络中的任何一个成员和任何一个陌生人之间所间隔的人不会超过六个。小世界特性的关键并不在于网络中两个成员的间隔数值具体是多少，实际在于：**由成千上万节点组成的大型网络，实际上是“小世界”，尽管其大部分节点彼此并不相连，但绝大部分节点之间只需要经过很短的路径就可以到达，且该网络具有较大的聚合系数。**

瓦茨和斯托加茨提出的小世界模型将真实世界的聚合特性、规则网络的规律性和随机网络的偶然性进行了统一。如图1.12所示，对于规则网络，平均路径长度较长，但聚合系数高。对于随机网络，平均路径长度较短，同时其聚合

系数也低。而小世界网络，平均路径接近随机网络，而聚合系数却依旧相当高，接近规则网络。这就为我们许多研究和分析带来了便利。

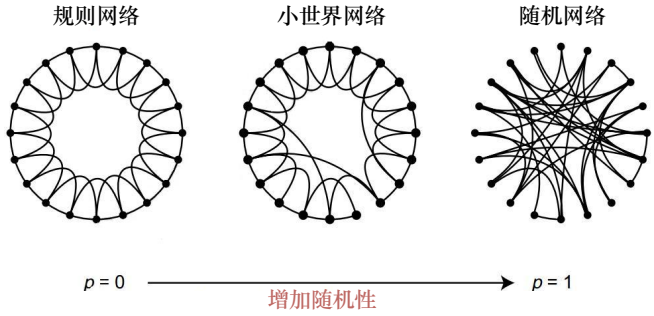


图 1.12　三种网络类型

复杂网络的小世界特性是分析网络空间中信息传播、病毒传播，以及“排兵布阵”的有力工具。通过网络结构和拓扑分析，我们可以发现只要少量改变几个连接，就可以显著提高传输性能。当然，这种特性毫无疑问也可以用于我们分析病毒的传播并快速切断传播途径，将损失降至最低。学完第 2 章，我们将会对此有更深刻的理解。

（2）无标度特性

在瓦茨提出小世界网络模型之后，巴拉巴西[28–31] 获取了他们的实验数据。在拿到数据后，他没有急于验证小世界模型的正确性，而是分析了网络中每个网站与其他站点链接数（也就是度）的分布情况以及网页的点击率。巴拉巴西在对几十万个节点进行统计后发现：网页上的链接分布和点击率呈现**幂律特性**，绝大多数网站的链接数或点击率很少，而有极少数网站（“中心节点”）却拥有异乎寻常多的链接数或点击率。这一结果为网络科学的发展做出了巨大的贡献。此外，巴拉巴西和他的学生们也对万维网中任意两个网页之间的平均距离进行了统计分析，1999 年 9 月，他们在 *Nature* 上发表论文 *Diameter of the world-wide web*[31]，指出万维网中任意两个网页之间的平均距离为 19。

改变分析问题的角度，可能带来新的突破！

总而言之，现实世界的网络大部分都不是随机网络，少数节点往往拥有大量的连接，而大部分节点连接却很少，比如抖音中普通用户的粉丝数量仅为个位或十位数，而一些明星的粉丝数量则达到上千万。网络中节点的度分布符合幂律分布，也被称为网络的无标度特性（Scale-free）。度分布符合幂律分布的复杂网络则被称为无标度网络。

我们可以从巴拉巴西撰写的《链接》和《爆发》这两本书中看到，世界由两个法则构成，一个是高斯法则，也就是正态分布。另一个正是幂律法则，也可以理解为二八法则。

无标度特性实际上反映了复杂网络中节点重要程度各异，复杂网络整体上

具有严重的分布不均匀性，可以说少数节点对无标度网络的运行起着主导的作用。这种特性在我们丰富多彩的世界中无处不在：芸芸众生中，像图灵、巴拉巴西这样的天才人物毕竟是少数；同样，在自然界中，像鲨鱼、老虎这样的食物链顶端生物也不多。

复杂网络的无标度特性对于理解网络的健壮性和脆弱性具有重要的作用。我们可以思考下面两个问题，针对度数非常高的节点进行攻击是否能够大大降低网络的健壮性呢？在等概率情况下，是否遭受攻击的节点越多，就越能使网络迅速瘫痪呢？实验结论是令人惊讶的，一方面，少量中心节点的破坏，即可导致网络迅速四分五裂为多个“孤岛”[32]；另一方面，互联网这样的无标度网络也同时具有相当的稳健性，能够承受相当比例的节点失效。

1.3.3 复杂网络与网络空间安全

在各行各业对互联网依赖增加的同时，网络攻击的方式更日趋复杂、隐蔽。我们都知道网络中已经部署了大量防火墙和入侵检测设备，但网络攻击事件却屡增不减，病毒传播也经久不绝。数理学家们在研究网络中的传播行为时，往往并不对其研究对象进行具体区分，无论是计算机病毒的传播还是自然界疾病的传播，抑或谣言的传播，都可以通过点和边来表示。这也就意味着自然界的一些传播规律也可以被应用于网络空间安全的分析和研究中，对应地，网络中的分析结果也可以用于解释和研究一些自然界的现象。

通过1.3.2节对复杂网络性质的学习，我们已经知道网络空间是具有小世界和无标度性质的，通过网络结构分析和网络行为推理来开展网络空间安全研究成为新的趋势。我们来思考一下，如果能够提前摸排网络系统的脆弱点，把一些关键节点重点保护起来，是不是可以有效对抗攻击呢？或者在攻击发生时，如果可以迅速发现攻击或病毒传播的规律或路径，定位关键环节，开展协同防御是不是可以有效抑制攻击扩散从而及时止损呢？网络科学的方法为我们从思维方式和模型方法上揭示网络行为规律，探索网络安全破解之道开辟了新思路。

1. 网络结构分析

互联网中的攻击往往难以预测，具有不确定性，而通过已有的攻击和特征，我们可以发现，一些攻击事件的效果往往取决于这个攻击事件带来的雪崩效应。这时候，如果可以结合复杂网络的结构特性，分析网络空间的全局组织，发现重点保护对象或资源，进而构建整个网络的健壮性和稳定性模型，是否可以避

免雪崩效应的发生呢？答案当然是肯定的。文献 [33] 通过分析度分布与病毒传播的关系确定了病毒抑制的步骤。文献 [34] 通过网络的拓扑结构分析来确定网络不同粒度上的保护对象并确定受保护区域的边界。文献 [35] 通过计算动态删除节点后网络平均最短路径变化的情况实现对脆弱点的发现和防御。

2. 网络行为推理

巴拉巴西的研究告诉我们网络中充斥着各种各样的幂律分布：用户发送邮件的时间间隔符合幂律分布，用户访问某网站连续点击链接的时间间隔符合幂律分布 …… 事实上，这些网络行为可能与网络空间安全密切相关，我们可以通过分析网络行为特性，研究攻击或病毒传播的行为规律，从而抑制病毒扩散。文献 [34] 对利用网络上的行为特性抑制病毒传播的方法进行了探讨。

总结

飞速发展壮大的互联网发展成为网络空间的同时，不断改变着人类生产、生活和经济的秩序[36, 37]。本章，我们回顾了计算机理论模型、计算机系统和互联网的发展历程，从图灵机的产生、冯 • 诺依曼体系架构的出现、TCP/IP 协议的创建和 Web 的发明中体会应用需求和开放共享对互联网发展的推动作用。从莫里斯蠕虫、“震网”病毒和 SolarWinds 攻击事件中了解到网络空间安全的严峻形势。我们概述了网络空间的定义和当前网络空间的安全现状以及各国安全战略，并介绍了基于基础理论、机制与算法、系统安全、网络安全、分布式系统及应用安全的网络空间安全学科体系，在接下来的各章中，我们将围绕这一体系进行详细讨论。在本章的最后，我们还探究了网络空间的复杂特性，为从网络科学的观点研究网络空间安全问题提供了新思路。

参考文献

[1] Babbage C. On the application of machinery to the computation of astronomical and mathematical tables[M]. Offprint from Memoirs of the Astronomical Society of London 1 (1822). London: Richard Taylor, 1824.

[2] 詹姆斯 • 格雷克. 信息简史 [M]. 高博, 译. 北京: 人民邮电出版社, 2013.

[3] Turing A M. On Computable Numbers, with an Application to the

Entscheidungsproblem[J]. Proceedings of the London Mathematical Society, 1937, 2-42(1) : 230–265.

[4] 迈克尔 • 斯韦因, 保罗 • 弗赖伯格. 硅谷之火: 个人计算机的诞生与衰落 [M]. 陈少芸, 成小留, 朱少容, 译. 3 版. 北京: 人民邮电出版社, 2019.

[5] 查尔斯 • 佩措尔德. 编码 • 隐匿在计算机软硬件背后的语言 [M]. 左飞，薛佟佟，译. 北京: 电子工业出版社, 2012.

[6] 魏强, 李锡星，武泽慧，等. X86 中央处理器安全问题综述 [J]. 通信学报，2018，39(z2): 151-163.

[7] 芯片中的硬件木马:X86 CPU 到底存在哪些安全风险 [EB/OL]. 2016-06-30 [2021-01-13] https://www.leiphone.com/news/201606/axsOSvKWy2ZZdzs9.html.

[8] Shannon C E. A mathematical theory of communication[J]. The Bell System Technical Journal, 1948,27(3):379-423.

[9] Kleinrock L. Information Flow in Large Communication Nets[D]. Cambridge: Massachusetts Institute of Technology, 1961.

[10] Kleinrock L. Communication Nets: Stochastic Message Flow and Delay[M]. San Francisco：McGraw-Hill, 1964.

[11] Baran P . On Distributed Communications Networks[J]. IEEE Transactions on Communications Systems, 1964, 12(1):1-9.

[12] Davies D W, Bartlett K A, Scantlebury R A, et al. A digital communications network for computers giving rapid response at remote terminals[C]. Proceedings of the first ACM symposium on Operating System Principles，January 1967.

[13] Roberts L G . The evolution of packet switching[J]. Proceedings of the IEEE, 1978, 66(11):1307-1313.

[14] Bush V. As We May Think[J]. Atlantic Monthly, 1945,176: 101-108.

[15] 伊恩 • 瑞彻：我拒绝蒂姆 • 伯纳斯-李的那一天 [EB/OL]. 2011-07[2021-01-13]. https://www.ted.com/talks/ian_ritchie_the_day_i_turned_down_tim_berners_lee/up-next?language=zh-cn.

[16] Cliff S. The cuckoo's egg: tracking a spy through the maze of computer espionage[M]. New York: Simon and Schuster, 2005.

[17]《骇客交锋》背后看不见的交锋：解密中美伊以新型国家网战 [EB/OL]. 2015-03-05 [2021-01-13]. https://www.tmtpost.com/199533.html/1-1040.

[18] 震网事件的九年再复盘与思考 [EB/OL]. 2019-09-30 [2021-01-13]. https://www.freebuf.com/vuls/215817.html.

[19] 戴浩. 赛博空间 (cyberspace) 概念的由来及译名探讨 [EB/OL].2016-01-15 [2021-01-13].http://www.360doc.com/content/16/0115/19/21966267_528220372.shtml.

[20] 吴建平. 网络空间安全的挑战和机遇 [EB/OL]. 2016-11-30 [2021-12-09]. https://www.edu.cn/xxh/media/zcjd/fmbd/201605/t20160512_1397332.shtml

[21] McLuhan M, Terrence Gordon W. Understanding Media: The Extensions of Man[M]. California: Gingko Press, 2003.

[22] 石文昌. 网络空间系统安全概论 [M]. 3 版. 北京: 电子工业出版社, 2017.

[23] 蔡晶晶, 李炜. 网络空间安全导论 [M]. 北京: 机械工业出版社, 2017.

[24] 沈昌祥, 左晓栋. 网络空间安全导论 [M]. 北京: 电子工业出版社, 2018.

[25] 刘建伟. 网络空间安全导论 [M]. 北京: 清华大学出版社, 2020.

[26] 罗军舟, 杨明, 凌振，等. 网络空间安全体系与关键技术 [J]. 中国科学：信息科学, 2016, 46(8): 939-968.

[27] Watts D J, Strogatz S H. Collective dynamics of 'small-world' networks[J]. Nature, 1998, 393(6684): 440-442.

[28] Barabási AL, Albert R. Emergence of scaling in random networks[J] . Science, 1999, 286(5439): 509-512.

[29] 艾伯特-拉斯洛 • 巴拉巴西. 爆发: 大数据时代预见未来的新思维 [M]. 马慧，译. 北京: 中国人民大学出版社, 2012.

[30] 艾伯特-拉斯洛 • 巴拉巴西. 巴拉巴西网络科学 [M]. 沈华伟，黄俊铭，译. 郑州：河南科学技术出版社，2020.

[31] Albert R, Jeong H, Barabási, AL. Diameter of the World-Wide Web [J]. Nature,1999, 401:130–131.

[32] 艾伯特-拉斯洛 • 巴拉巴西. 链接网络新科学 [M]. 长沙：湖南科学技术出版社, 2007.

[33] 王林, 戴冠中. 复杂网络的度分布研究 [J]. 西北工业大学学报, 2006, 24(4)：45-49.

[34] 李德毅, 韩明畅, 孙岩. 复杂网络与网络安全 [J]. 军队指挥自动化, 2005(06):15-20.

[35] 赵小林, 徐浩, 薛静峰, 等. 基于复杂网络的网络系统脆弱点发现方法研究 [J]. 信息安全学报, 2019, 4(1)：39-52.

[36] 徐恪, 王勇, 李沁. 赛博新经济: “互联网 +” 的新经济时代 [M]. 北京：清华大学出版社, 2016.

[37] 徐恪, 李沁. 算法统治世界——智能经济的隐形秩序 [M]. 北京：清华大学出版社, 2017.

习题

1. 计算机由哪五大部件组成？
2. 请描述图灵机的主要组成部件及其功能。
3. TCP/IP 协议分为几层，每一层的作用是什么？
4. Web 的三种基础技术是什么？

5. 简述“震网”病毒的传播过程。
6. 网络空间有哪些主要特征？
7. 网络空间安全面临哪些挑战？
8. 什么是网络科学？
9. 复杂网络有哪些典型特征参数？
10. 简述小世界特性和无标度特性。