CYBER SECURITY POLICY GUIDEBOOK

网络安全政策指南

[美] Jennifer L. Bayuk　Jason Healey
Paul Rohmeyer　Marcus H. Sachs
Jeffrey Schmidt　Joseph Weiss　著

张志勇　范科峰　向菲　译

国防工业出版社
National Defense Industry Press

WILEY

河南省科技创新人才计划杰出青年基金
(No. 134100510006)资助出版

网络安全政策指南

Cyber Security Policy Guidebook

[美] Jennifer L. Bayuk Jason Healey
Paul Rohmeyer Marcus H. Sachs
Jeffrey Schmidt Joseph Weiss 著

张志勇 范科峰 向菲 译

国防工业出版社

·北京·

著作权合同登记　图字：军－2014－060 号

图书在版编目(CIP)数据

网络安全政策指南/(美)贝尤克(Bayuk,J. L.)等著;张志勇,范科峰,向菲译. —北京:国防工业出版社,2014.11

书名原文:Cyber security policy guidebook

ISBN 978-7-118-09824－2

Ⅰ.①网…　Ⅱ.①贝…②张…③范…④向…　Ⅲ.①互联网络—安全技术—指南　Ⅳ.①TP393.08－62

中国版本图书馆 CIP 数据核字(2014)第 282272 号

※

國防工業出版社出版发行

(北京市海淀区紫竹院南路 23 号　邮政编码 100048)

北京奥鑫印刷厂印刷

新华书店经售

※

开本 787×1092　1/16　印张 12　字数 264 千字

2014 年 11 月第 1 版第 1 次印刷　印数 1—2000 册　定价 58.00 元

(本书如有印装错误,我社负责调换)

国防书店:(010)88540777　　发行邮购:(010)88540776

发行传真:(010)88540755　　发行业务:(010)88540717

译者序

作为从事网络信息安全领域的研究人员，我们从2012年WILEY出版社出版这本原著开始，就一直关注它。这是在网络空间安全政策与战略领域，非常高屋建瓴，极具参考价值的一本书。

党中央、国务院高度重视信息安全问题，党的“十八”大首次提出“健全信息安全保障体系”的目标，国务院国发〔2012〕23号文中提出“培育国家信息安全标准化专业力量，加快制定三网融合、云计算、物联网等领域安全标准”。2013年8月，国务院以国发〔2013〕32号印发《关于促进信息消费扩大内需的若干意见》，其中强调，加强信息基础设施建设，加快信息产业优化升级，大力丰富信息消费内容，提高信息网络安全保障能力。2014年2月，中央网络安全和信息化领导小组成立。该领导小组将着眼国家安全和长远发展，统筹协调涉及经济、政治、文化、社会及军事等各个领域的网络安全和信息化重大问题，研究制定网络安全和信息化发展战略、宏观规划和重大政策，推动国家网络安全和信息化法治建设，不断增强安全保障能力。据悉，截至2014年，全球已有40余个国家颁布了网络空间国家安全战略，并且在这项工作中，美国远远走在其他国家的前列。

本书所探讨的网络安全政策涉及行政、立法、司法、商业、军事和外交行动等众多领域，详细阐释了网络空间、网络安全和网络安全政策之间的关系，描述了网络安全演化历史以及衡量网络安全的方法。针对政策决策者所面临的复杂网络安全环境，全面地给出了不同组织和行业的网络安全政策列表，以及美国政府为调整网络安全战略与政策所做出的努力。因此，本书是在了解和掌握美国网络空间安全战略方面非常难得的一本参考手册和指南。

本译著的出版受到河南省科技创新人才计划杰出青年基金（No. 134100510006）资助。相关研究工作受到国家自然科学基金（No. 61370220，No. 61172053）、国家科技重大专项“新一代宽带无线移动通信网”（No. 2015ZX03003007）、国家242信息安全计划（No. 2014A104）、河南省科技攻关项目（No. 142102210425）、河南省教育厅科学技术研究重点项目基础研究计划（No. 13A520240，14A520048）等支持。

本译著的主要分工如下：河南科技大学计算机系主任张志勇教授、中国电子技术标准化研究院信息安全研究中心副主任范科峰博士负责本书的申请列选、论证和最终审定全稿。本书第1～5章由张志勇负责翻译，第6章由河南科技大学电子科学与技术系副主任向菲博士负责翻译，第7～8章由范科峰博士负责翻译。河南科技大学“多媒体内容安全”研究团队的研究生在本书的编辑、校对等方面给予了大力协助。本译著的

出版也得到了中国电子技术标准化研究院信息安全研究中心领导的关注和大力支持。他们的宝贵意见和建议，使得这本颇具价值的原著得以顺利译成并出版，和国内读者如期见面。

我们在本书翻译过程中，力求精益求精，期间翻阅和参考了大量的国外相关资料，但因能力有限，难免仍有疏漏之处，敬请读者批评指正。

张志勇　范科峰　向 菲

2014 年 8 月

序

不久前，我还是美国国土安全部（DHS）网络安全战略的负责人。在那个角色中，我主要负责和安全部的同事们一起实施维护网络安全行动。在一次例会上，当把焦点聚集在网络空间风险的管理和测量上时，我们观点交锋，互不相让。行动组一位资深员工透过桌子看着我问道："您真的认为政策应该推动行动吗？"

除这个问题背后显而易见的异常外，它指出了这本书要传达的核心主题：网络安全战略的重要性，战略和操作之间的关系，利益相关者和政策决策者这两个完全不同团体的直接关联性，以及由此引发的不可避免的争议与辩论。这些问题非常具有时代特征，并不是由于谨小慎微而提出的。

也许令我在 DHS 的同事懊恼的是，事实上，政策确实应当推动行动。正如作者明确指出的那样，政策必然推动许多不同层面的决策。我们中有多少人没有听过美国总统在演讲中说道："这是我的管理政策……"？他的工作是（和国会一起）制定国家政策，通过适当的实践行动实施政策，然后确保政策正确执行或根据情况进行调整。其他层面的执行者也有类似责任。

然而，在万事皆网络的发展过程中，政策并没有成为驱动力，反而成了马后炮。作者们用多种方式来说明这一点，并由此提出一个极其重要的问题：网络安全政策总是应该事后反应吗？显而易见，答案是否定的，否则，它推动的行动和标准将永远是被动的，这将导致一种本质上站不住脚的情况，即网络安全的工作总是落后于他们想要阻止的攻击。如果这种情况听起来太过熟悉，那是因为网络安全从业者在这个单调乏味的岗位上工作太久了，丝毫没有结束的迹象。

当然，很大的问题是，主动的网络安全政策设置是非常困难且耗时的工作。哪怕是最简单地详读本书第 6 章就足以告诉读者，几乎任何网络安全政策都是富有争议的，政策制定的基础本身实际上是模糊的。

作为一般规则，当一个人因为正确构建特定系统的复杂性而心烦意乱时，最好向后退一大步——然后提升自己更宏观地看待问题。只有这样，才能发现构筑本书的核心问题，"我正在建立正确的系统吗？"根据我的自身经历，这个问题的答案往往是：不。对于那些正在建立错误系统的人来说，如果构建方式是正确的，并因此加大投资，听到这样的答案将会痛苦得难以置信。

我相信，所有的这一切都能说明，《网络安全政策指南》这本书出现的理由。不论观点如何，如果毫无偏见地去读，这本书将帮助读者看到网络安全的全局及其关键政策的设置。这本书无疑是一个很好的助手。

本书的作者都是备受推崇的专业人士，都是各个领域的专家，他们将多年的经验汇集在本书中，这是非常令人愉快的。正如他们所指出的，标题惊人的广泛——这是一个自然

的结果，在今天的网络化世界中，“网络”无处不在。事实上，如果主题不是如此重要和具有重大意义，总是随身把这本书抱在怀里看上去很愚蠢。

但是，对我们大多数人来说，与国家安全、商业运营或互联网相关的任何事情都是非常重要的。为此，了解一些相关措施是至关重要的。因此，这本书非常之重要。

Andy Cutts

美国国土安全部前网络安全政策指挥官

前　言

当决定写这本书时，网络安全政策会议（SIT2010）恰好正在举行。会议议题的范围从风险资本家做出的安全技术投资决策到网络安全政策在个人隐私上的实现。尽管所有的演讲者都是各自领域的专家，并且被要求提出网络安全政策的演讲议题，许多人还是将焦点放在了战略或技术问题上。对于嘉宾和观众来说，即使对政策很清楚，也会因为阐述不清而无法参与知情讨论。因此，在会议上，评论变成了乱哄哄的嗡嗡声，对于与会者而言，这确实是一段难忘的经历。

这段经历使我们发现，网络安全政策对于不同的人意味着不同的事，甚至是那些在这一领域工作的人。这个发现促使我们想要写这样一本书，旨在引导读者通过个别简单的概念去吸收、理解网络安全及其政策。

我们很清楚，在网络安全领域，没有一个人有足够的经验以至于能够单独完成这本书。我们的团队能够保证，我们的经验覆盖了网络安全的主要领域。章节的每一部分都和我们的经验一一对应。而且，每个章节都被所有的作者仔细审阅过，以保证对于不同类型的读者，这本书都在做一个整体的陈述。政策是权威人士的领域。行政当局起源于由社会契约建立起来的政府或私人企业领域。虽然本书是以管理者的角度来写的，但并不仅仅是为他们而写。在立法时，为了从公共和私人两方面听到不同的声音，网络安全政策分析必须经过严格的审查，因此，本书的读者必须扩大到执行顾问、教育工作者、研究人员、立法人员和该领域的从业人员。虽然每位读者对这本书中所提到的内容，都有他们自身的知识背景和经验，但我们还是期望能够通过和同一领域内的同行们共同分享网络安全政策方面的一般框架和专业术语，从而丰富目前网络安全政策中的概念。同行们的专业经验使他们能够处理不断变化的网络安全问题。大多数关于网络安全的文献分为两类：技术和建议。谈到对网络安全政策的案例决策时，本书将避开技术术语和专业建议。尽管本书努力解释网络安全的技术问题，但完全是以外行人的口气。同时，本书强调对网络安全政策决策的评判和分析思考的重要性，使读者能够描述具体政策的选择所产生的影响，令读者自行决定将此影响看做积极的还是消极的。

这本指南整合了网络安全政策在行政、立法、司法、商业、军事和外交行动上可能的解释。这些学科的读者可透过本领域的专业视角审视这些内容，并由他人遇到的问题引导深入了解。对于外行来说，这是一本导论性的指南，同时，它又为网络安全领域的专家提供了全面参考。

起初，正如在会议上划分的那样，这本书被归类为政策领域，并且依此划分了章节，分给了每个作者。然而，写作刚开始，我们即对划分的方法产生了怀疑。会议上的一

些议题范围十分广泛，例如：法律的实施、隐私、公民权和人身自由；新兴技术、革新和商业成长；全球网络安全政策的影响。其他议题集中在系统的特定类型，如：下一代空中运输系统和电力分布。没有人认为，每章的政策内容简单组合就能组成一本书。本书的内容不能将一个行业的问题分成几个问题子集，但是它要能够达到启发外行人的目的。要使他们理解网络安全政策问题到底是什么。这一认识导致本书的行文布局使得全书更加完整统一。

第 1 章介绍网络空间、网络安全和网络安全政策之间的关系。第 2 章讲述了网络安全的简要历史。它提供了必要的背景知识，使外行也能够理解这个行业的当前状态，以及国家在网络空间领域建立安全控制的做法。本章并不是对网络犯罪或建立网络安全控制的立法尝试的事件记录，而是突出影响安全控制变革的重要事件。

第 3 章描述了衡量网络安全的通常做法。从安全的目的和目标的角度重温了第 2 章的历史；讨论了已被用来确定网络安全目标是否已经达到的各种方法；通过研究三个网络空间启用的案例来详细说明这些方法。这三个案例是：电子商务、工业控制系统和个人移动装置。

第 4 章为行政决策者提供指南，他们负责大的组织和选区，是网络安全利益相关者。本章强调网络安全管理与其他管理行为一样，成功的执行需要清晰明确的目标和相应的计划管理；提供了如何开始建立网络安全战略和有关网络安全政策的主要原则；建议在网络安全问题上，应当集成组织的使命和目的。

第 5 章介绍检查网络安全政策问题的编目方法。它将第 2 章和第 3 章的网络安全历史和指标放在网络空间操作环境中，从而将安全问题从责任问题中分离出来，在网络安全领域的“政策”适用于跨越多个组织和行业的不同层面的社会问题。因此，第 5 章描述了在不同的岗位上，决策者所面临问题的界定。也就是说，通信公司高管面临的政策决定与军事战略家所面临的政策决定是完全不同的。然而，由于它们之间存在重叠，因此在本章节中对这些界定特别进行了描述。界定是为了更清晰地说明，而不是为了介绍不存在的界限。

第 6 章在前 5 章介绍的概念和定义基础之上，解释了政策决策者所面临的网络安全环境。每个部分包括不同的组织和行业面临的网络安全政策问题的列表。

第 7 章按时间顺序记录了美国政府为调整网络安全战略与政策所做的努力，并评述了网络安全政策上历史性事件的影响。在本章的结束部分，提到了参众两院关于网络安全政策的建议。

第 8 章进行总结，并展示如何在每章就同一主题提出不同的观点；强调对于不同的网络空间利益相关者，网络安全政策的方法必然不同，并且在实现个人网络空间战略目标时，安全性措施必须针对有效性去衡量。

我们之间对彼此所从事领域的深度和广度深表欣赏。当我们在记录历史时，Marcus Sachs 在公共和私人政策领域的第一手经验是非常宝贵的。Jason Healey 在政府服务和私人研究政策分析上的丰富经验揭示了单一民族国家和全球外交的众多问题。Joe Weiss 在工业控制系统深入的专业知识防止我们对技术基础设施的关键属性失去焦点。Paul

Rohmeyer 在技术管理上不间断的学术研究和商业经验，确保我们的叙述不仅对决策者意义非凡，对实施战略目标的所有人都具有重要意义，很明显，那些人就是我们的目标读者群。Jeff Schmidt 的职业生涯长时间浸泡在互联网管理和软件工程问题上，这为本书提供了合理的完整性检查。Jennifer Bayuk 雄厚的技术背景和以外行人进行写作的行文技巧将本书巧妙组织，并完成了概念的陈述，且使之易于理解。

我们将本书献给网络安全政策的制定者，无论是台前的还是幕后的。愿你们在各自的领域取得成功。

Jennifer L. Bayuk
Jason Healey
Paul Rohmeyer
Marcus H. Sachs
Jeffrey Schmidt
Joseph Weiss

致　谢

本书的灵感来自于21世纪尊敬的空军部长Mike Wynne，他为空军的网络安全做了很大贡献，并在当时一手负责提高对于国家安全相关的网络安全政策问题的认识。在众多其他赞美和关键的任命中，Wynne先生担任过系统工程研究中心的顾问委员会主席和斯蒂文斯理工学院院长的高级顾问。

为了建立学术界的网络安全政策意识，Wynne先生主持了斯蒂文斯理工学院关于此主题的会议（SIT 2010），征询了网络空间多位专家的意见。他们在会议中发表了演讲或参与到讨论中。有些不能出席的专家也提供了其书面意见。我们感谢演讲者和其他给会议提供意见的专家。

非常感谢审查本书第一回完成稿的专家，他们的宝贵意见大大提升了这里所包含的网络安全政策内容的可理解性。我们非常感谢以下人的努力和意见：Warren Axelrod、Larry Clinton、Kevin Gronberg、Richard Menta、William Miller、Brian Peretti、Andy Purdy和Michael zur Muehlen。感谢以下人为本书提供材料：Michael Aisenberg、Edward Amoroso、Tom Arthur、Paige Atkins、James Arden Barnett、John Boardman、David M. Bowen、Christopher Calabrese、Ann Campbell、C. R. Collazo、Greg Crabb、William Crowell、Matthew D. Howard、John A. Davis、Christopher Day、James X. Dempsey、Edward C. Eichhorn、Robert Elder、Steve Elefant、Dan Geer、Charles Gephart、Gary Gong、Gail L. Graham、Kevin Harnett、Melissa Hathaway、Husin bin Hj Jazri、Erfan Ibrahim、Robert R. Jueneman、Jeffrey S. Katz、John Kefaliotis、Alan Kessler、George Korfiatis、Darren Lacey、Pascal Levensohn、Martin Libicki、Chan D. Lieu、Eric Luiijf、Pablo Martinez、Douglas Maughan、Ellen McCarthy、Dale Meyerrose、Gregory T. Nojeim、John Osterholz、James B. Peake、Jim Richberg、Robert D. Rodriguez、Tom Ruff、Brian Sauser、Ted Schlein、Agam Sinha、Ben Stewart、John N. Stewart、Eric Trapp、David Weild、John Weinschenck和Paul Winstanley。我们已经尽可能多地采纳了会议的意见，感谢这些分享他们见解的专家。我们期待有关网络安全政策方面更多的建设性意见，以确保网络安全向前发展的和平与繁荣。

目　录

第1章 引 言

1.1 什么是网络安全

网络安全通常是指网络系统具有控制接入和保障共所包含信息安全的能力。在网络安全有效控制的地方,网络空间被认为是一种可靠的、可恢复的且可信的数字基础设施。在网络安全控制缺失、不完整或是设计不合理的地方,网络空间被认为是数字时代尚未开垦的蛮荒之地。甚至那些工作在安全行业的人们,对于他们所置身其中的网络安全的认识也不尽相同。无论一个系统是物理设施或是网络空间组件的集合,被指派负责该系统安全的专业人员的角色都是为潜在攻击做计划,并且为攻击的后果做好准备。

虽然"网络"(Cyber)一词是主流术语,但是确切来说它到底指什么,却是难以清晰描述的。原本出自科幻小说,随后基于兴起的计算机控制与通信领域而闻名的"控制论"(Cybernetics)一词,现在通常指的却是电子自动化(Safire 1994)。相应的术语"网络空间"(Cyberspace)一词,其定义范围囊括从概念到技术,并且被一些人称做是第四领域,此外还有陆地、海洋和大气层空间等前三个领域(Kuehl 2009)。关于网络空间与网络安全,在文献中有很多种定义。我们的意图并不是为了在语义上对这些定义进行辩论,因此没有引入那些文献中的定义。进一步讲,这些辩论对于本书的目的是没有必要的,因为通常我们并不将"网络"(Cyber)一词用做一个名词,而是一个修饰其主语的形容词,它的属性是支持一组自动化电子系统通过网络进行接入访问。正如对应到词典编纂中,就认知语言学与约定俗成的大众文学之间对于语言的使用有争论一样(Zimmer 2009),因此我们请读者撇开容易引起困惑的两个术语"网络空间"(Cyberspace)与"网络安全"(Cyber Security),这两个词仅仅指代它们各自现实的概念。同时记住,我们通常将术语"网络"作为一个形容词,它的具体属性会随着所关注讨论的系统而变化。

在很大程度上,网络安全通常以下面一些三元组来解释,它们分别用来描述安全专业人员的目标与方法(Bayuk 2010)。这些三元组结合起来几乎包含了此术语的大多数用法,它们是:

预防,检测,响应;

人员,流程,技术;

保密性,完整性,可用性。

这些分别反映了网络安全的目标,达到网络安全的方法,以及实现网络安全目标所需要的机制。

预防、检测、响应通常是解决物理安全和网络安全的目标。传统上,安全计划的主要目标是阻止一个成功的敌手攻击。然而,所有的安全专业人员都意识到:根本不可能预防所有的攻击,所以最好在损失发生前,做好计划和准备,必须包括检测正在攻击的方法。

然而，无论检测步骤是否有效，一旦一个系统明显遭受威胁，安全就应包括响应此类事件的能力。在物理安全中，术语“应急人员”（First Responders）是指政策、火灾或者紧急医疗专业的“英勇”人士。典型的响应包含击退攻击、医治幸存伤员、保护受损的资产。在网络安全中，这个三元组中的第三个元素往往以比较乐观的形式阐明，如把“响应”替换为“恢复”或“更正”。对这个三元组动作的结果有一个更好的期望，那就是恢复而不是简单的响应，这反映在信息安全计划的文献中，建议安全管理应该包含对重要商业系统的还原与恢复。由于信息技术允许操作系统所需的数据和程序拥有多样性、冗余性和可恢复性，因此信息安全专业人员希望损害可以完全消除。无论发生什么情况，都希望从响应中所得到的经验教训能够反馈给预防计划，从而形成一个可持续的、安全不断完善的循环。

人员、流程、技术通常是解决一般的技术管理和作为一个专业领域的网络安全管理的方法。这个三元组遵守：系统需要操作者，操作者必须遵守为了使系统完成它们的任务而制定的规则。若应用到安全上，这个三元组更突出这样一个事实：安全不能由安全专业人员单独实现，也不能仅仅依靠技术来完成。要保护的系统或组织被公认为包含其他人员要素，这些人员的决策与行动，对安全程序的成功执行起着至关重要的作用。如果没有预先计划好的流程，即使这些人中的每个人都希望并且积极地执行安全操作，他们也不知道如何采取联合行动预防、检测和恢复受损的系统。所以安全专业人员需要将安全程序融合在已有的组织流程中，并在战略上采用技术实现网络安全目标。

保密性、完整性、可用性是解决特定信息的安全目标。保密性是指系统拥有限制信息分发和授权使用的能力；完整性是指维持所记录或报告信息的真实性、准确性和来源的能力；可用性是指系统的功能性实时可用。这些信息安全目标在没有用在计算机的时候，已经应用到信息上，但是网络空间的到来改变了这些目标实现的方法，也改变了目标实现的相应困难度。这些支持保密性、完整性和可用性的技术，经常彼此制约。例如，在网络空间中，为使信息达到一个高级别的可用性，经常会使保持信息的保密性变得更加困难。在一个给定系统中，针对每一类信息，安排好保密性、完整性和可用性方法，是一个网络安全专业人员应有的专业素质。网络安全通常是指使用三元组人员、流程、技术，去预防、检测和恢复受损系统，并在网络空间中保证信息保密性、完整性和可用性的方法。

1.2 什么是网络安全政策

网络使整个社会的生产力提高，并能够及时、有效地分发信息。无论网络被引入到什么样的产业或应用中，生产力的提高都是不争的事实。网络空间中信息的快速传送降低了整个系统的安全性。与技术专家致力于提高生产力相比，安全措施看似直接阻碍了进步，这是因为：预防措施减少、抑制或推迟用户进入；检查措施消耗重要的系统资源；响应需求会从系统特征中分散管理的注意力，而这些注意力本该集中在提供更加直接令人满意的系统功能上。网络安全政策解决了网络功能需求与安全需求之间的矛盾。

很多涉及网络安全的情况都会提及“政策”（policy）一词。它是指与信息发布有关的法律与规定、私企中信息保护的目标、控制技术中计算机操作方法以及在电子设备中的配置变量（Gallaher，Link，et al. 2008）。但是，在使用“网络安全政策”（Cyber Security Poli-

cy)这一短语的文献中也使用了大量其他方式。就“网络空间”(Cyberspace)这一术语而言,目前还没有一个定义。但是,当术语“网络安全”(Cybersecurity)作为一个形容词用在政策声明中时,这里却是一个普通的主题。这本指南旨在为读者提供足够多的背景去理解和领会其主题,以及所引申的内容。读完后,读者应该可以更有信心地去解读众多的网络安全政策。

一般来说,术语“网络安全政策”(Cyber Security Policy)是指直接用来维护网络安全的指令。网络安全政策如图 1.1 所示。为了有助于理解被称为“系统路线图”(Systemigram)的这些复杂主题,图中用一个建模工具来说明(Boardman and Sauser 2008)。“系统路线图”以一种介绍待定义事物的组成部分(所有名词)的方式,创造了一种简洁的、用做解释的定义,并且把它们之间所形成的活动(所有动词)结合起来。这个工具需要一条主干把所有的主要元素连接起来,这个“主干”连接被定义的概念(左上)及其目的或任务(右下)。这条主干是用来捕捉外行人对这个概念的看法。这个所定义的概念的其他观点可以用复杂概念上的补充观点来加以阐述。

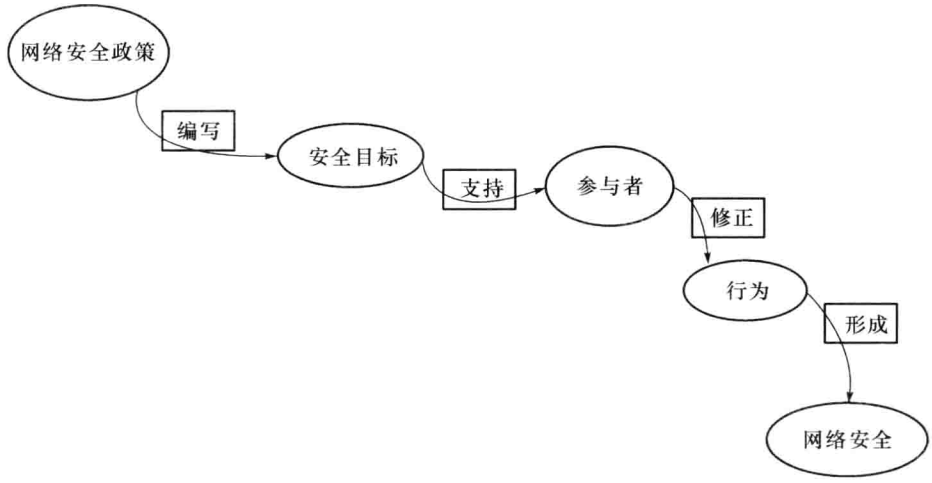

图 1.1　网络安全政策定义

在图 1.1 中,网络安全政策描述为编写网络安全目标,支持参与者遵照政策修正他们自己的行为,以实现网络安全。图 1.2 对概念做了补充,为网络安全政策中的不同观点添加了不同颜色。虽然不是所有的添加节点和连接都完全严格地包含在网络安全政策的定义范围内,但是却能够帮助理解图 1.1 中的主要定义。

在图 1.2 中,从“管理机构”节点进出的连接,说明了网络安全政策被管理机构作为一种实现安全目标的方法而采纳。此图是通用的,因为管理机构常常独立于它们领导的组织之外而存在。例如,单一民族国家可能是一个管理机构,也有人可能认为凌驾于多个独立业务单位之上的集中式企业安全办公室,也是一个管理机构。从“执行机构”节点辐射出去的连接,解释了政策执行机构的角色,即制定法律、规则和/或条例,这些不仅会影响参与者的行为,也会影响那些在决策过程中成为利益攸关的人。最左边的连接是说明标准的作用,这些标准是由受管理机构政策约束的管理组织所制定的。来自“供应商”节点的连接描述了供应商、参与者、管理者三方之间的关系,参与