paloalto NETWORKS

全球IT高管网络安全秘籍

THE DEFINITIVE CYBERSECURITY GUIDE FOR DIRECTORS AND OFFICERS

遨游数字时代

NAVIGATING THE DIGITAL AGE

[美] Palo Alto Networks 编

中国水利水电出版社
www.waterpub.com.cn

遨游数字时代——全球 IT 高管网络安全秘籍

[美] Palo Alto Networks 编

中国水利水电出版社
www.waterpub.com.cn
·北京·

内 容 提 要

数字技术已全面渗入我们生活的各个方面，但我们在数字时代的生活方式面临着方方面面的挑战，尤其网络安全方面最为直接和突出。因此，致力于网络安全技术及相关事业的 Palo Alto Networks 公司组织编写了本书。

本书汇集了全球商业、科学、技术、政府、学术、网络安全和执法领域 50 多位具有重大影响力的领导者和预言家的观点，其中的很多观点对一般企业的网络安全建设极具参考价值。

本书适合企业的高管尤其是负责网络安全的高管借鉴参考，同时也适合对网络安全有兴趣的人阅读参考。

图书在版编目（CIP）数据

遨游数字时代 ：全球IT高管网络安全秘籍 / 美国派拓网络编. -- 北京 ：中国水利水电出版社，2019.6
ISBN 978-7-5170-7706-0

Ⅰ. ①遨… Ⅱ. ①美… Ⅲ. ①计算机网络－网络安全
Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字(2019)第093044号

责任编辑：周春元　加工编辑：王开云　封面设计：李　佳

书　名	遨游数字时代——全球 IT 高管网络安全秘籍 AOYOU SHUZI SHIDAI——QUANQIU IT GAOGUAN WANGLUO ANQUAN MIJI
作　者	[美] Palo Alto Networks　编
出版发行	中国水利水电出版社 （北京市海淀区玉渊潭南路 1 号 D 座　100038） 网址：www.waterpub.com.cn E-mail：mchannel@263.net（万水） sales@waterpub.com.cn 电话：（010）68367658（营销中心）、82562819（万水）
经　售	全国各地新华书店和相关出版物销售网点
排　版	北京万水电子信息有限公司
印　刷	三河市鑫金马印装有限公司
规　格	184mm×240mm　16 开本　16 印张　370 千字
版　次	2019 年 6 月第 1 版　2019 年 6 月第 1 次印刷
印　数	0001—2000 册
定　价	88.00 元

前　言

欢迎阅读全新的《遨游数字时代——全球 IT 高管网络安全秘籍》。之所以强调“全新”，是因为本版没有任何内容与我们之前的版本的内容有重复。前一版是在三年前出版的，三年对于数字时代，如同一千年。

本书汇集了商业、科学、技术、政府、学术、网络安全和执法领域近 50 位领导者和预言家的观点。每人撰写一个章节，旨在让我们深入思考我们正在创造的这个数字世界的影响。

本书的一个焦点是，在数字时代开展业务，尤其需要在技术与非技术高管之间就围绕网络安全存在的问题培育共识。

本书分为三个部分：第一部分着重介绍未来的威胁与风险；第二部分强调从当今世界吸取的教训；第三部分旨在帮助你确保自己在目前得到安全保护。每个部分都有反映其目标和目的的特点。第一部分偏向未来，第二部分偏重经验，第三部分更为实用，您会发现每个部分都发人深省且极具价值。

在编辑这些章节时，我们发现的一个惊喜是作者始终都能把网络安全的业务和技术挑战与整个世界所面临的更广泛问题无缝、完美地联系起来。

但是，回想起来，或许我们不应惊讶。毕竟，使本书如此必要和如此引人关注的原因，是数字技术已全面渗入我们生活的各个方面这一事实。正如您会在后面发现的一样，我们目前仍然仅仅处在遨游数字时代这一旅程的开端。

除非另有说明，否则所有金额均以美元为单位。

目　　录

人

流程

技术

结论

第一部分

威胁与风险的未来

1

序

Tom Farley——纽约证券交易所前总裁

“如今，没有任何其他问题在公司高管和董事会中引起的担忧超过网络安全风险。”

我就是这样介绍上一版《遨游数字时代》的，三年后的今天，这种情绪甚至更深刻、更紧迫。当时，我们就已经看到对网络数字技术的严重依赖以及我们为防止网络安全攻击而必须保持的警醒程度。

我们见证了数据隐私与基础架构攻击、选举干扰、勒索软件的出现，以及网络攻击对全球企业的潜在连锁效应。我们通过痛苦的经历了解到，随着我们继续加快数字时代的创新节奏，网络安全现状并未提供我们所希望感受到的信任和信心。

我们可以做许多工作来解决网络安全挑战，而且还有更多工作必须完成。这就是本书的切入点。本版以“网络安全登月”概念开篇，然后是近 50 位专家撰写的文章，意在努力让读者更好地了解我们在“遨游数字时代”中所面临的挑战，以及现在和将来保护与赋能数字生活方式所必须采取的措施。

你会看到有几个主题在以下篇幅中反复引起共鸣：

- 网络数字技术是我们生活方方面面的根基，不仅包括我们的业务基础架构，也包括我们的电网、供水、空中交通系统、选举系统和国家安全机构，这里不再一一列举。
- 我们仍然处在数字时代旅程的早期阶段。未来几年，物联网、人工智能和其他“指数性”技术的扩展将会极大地推动创新，同时扩大我们的受攻击面和风险。
- 由于我们处于这种数据与技术快速扩展的前沿，因此必须快速、全面进步，以抢先解决网络安全挑战，避免局面失控。许多作者的高度紧迫感通过时间得到了检验，并且再次出现在后面的章节中。
- 有效的网络安全集人、流程和技术于一体。我们的业务和技术领导者必须意见一致，发出相同的声音，并坚持最佳监管实践。我们必须利用先进的

自动化技术来创造与对手的公平竞争环境，以机器对抗机器。

- 我们能够采取网络安全措施。这需要协调、集中的行动，需要跨行业和政府的合作，需要培训、教育、试验、创新和发明，而且还需要更多措施，但这是可以完成的。

作为商业、技术、网络安全、政府和学术领域的领导者，我们的职责就是在可能的情况下，确保更多任务得以完成。有几位作者指出网络安全是我们这个时代最重要的问题，确实如此。如果我们在网络安全方面失败了，那么我们所有的数字时代梦想和志向都将面临风险。

如果能够从这些文章中所分享的集体智慧中汲取一个结论的话，那就是：说到网络安全，我们只能成功。我们必须成功，而且必须集体成功，因为不管怎样，最终我们都会在数字时代连成一体。

在纽约证券交易所，我们致力于完成手边的任务。我们大力鼓励上市客户尽其所能解决企业内的网络安全挑战，并参与本书讨论的一些更广泛计划。由于我们都愈加互相关联，因此越来越依赖我们的外部关系，包括合伙伙伴、供应商、监管机构等。网络安全是我们的集体责任，不仅对我们的雇员和股东，对整个社会也是如此。我们越能协作行动，就越能有效地降低我们所有人的风险。整个世界不仅在拭目以待，而且正期待我们竭尽全力。

2

要保护我们在数字时代的生活方式，就必须实现网络安全登月

Mark McLaughlin——Palo Alto Networks 副董事长

数字时代为我们所有人提供了站在可能提升和塑造全球未来几代人生活的前沿的特权。无论是来自商业、工业、学术还是政府部门，作为肩负重托的领导者，我们都有既定的责任在这个日益依赖网络数字技术的世界保护我们的生活方式。

如果我们做好自己的工作，就能帮助解决这个时代的一些最大的问题：气候变化、饥饿、贫穷、人口大爆炸和疾病。我们能够以数以千计的方式（无论大小）让个人的生活变得更好——改善他们的医疗、沟通方式、学习方式、所做的工作方式、生活方式、娱乐方式以及实现梦想的方式。

但是与我们的特权相伴的是责任。为了看到我们自己的希望和梦想成真，为了确保我们的工作在切实改善生活而非相反，我们必须克服有可能迟滞或阻止这一进展的一个巨大障碍，这个障碍就是网络安全。未来依赖于做好网络安全。

历史将会如何评判我们？

我们时代的挑战：网络安全登月

我认为，如果要得到有利的评判，我们就必须登月。之所以有意使用“登月”这个术语，是因为它不仅是我们手边任务的一个象征，而且在某些方面也是模式和使命声明的体现。在我们一生中，甚至在我们许多人出生之前，人类已经进行了登月尝试，并且取得了成功。而且登月改变了世界。

1962 年 9 月 12 日，美国总统约翰·肯尼迪在莱斯大学的一次演说中许诺要在未来 10 年内把一个人送上月球。他承认这是一个可能会在国内外受到怀疑的大胆目标。但他也知道这是一次值得且必要的努力，而且他相信这是可以做到的。他也非常有远见地知道协力完成一个清楚阐明的目标将会带来有形、巨大和持久的好处。正如他在其标志性演说中所述：“这个目标将有助于组织和衡量我们的最佳精力和技能。”

现在，我们的处境类似。数字时代的网络安全给这一承诺带来的现实威胁要求我们现在支持、宣传和采取努力：围绕解决世界网络安全挑战的愿景组织和衡量我们的努力和技能。

我们的目标必须远大、简单和直接。实际登月有着清楚和明确的目标，例如肯尼迪总统的目标是把一个人送上月球并安全带回。我认为我们的“网络安全登月”应当拥有同样简单而强大的目标：在 10 年内确保互联网的安全。

我知道这有些大胆。我也知道将会有反对者、怀疑者和吹毛求疵的人：“这太大胆了。”“‘安全’意味着什么？”“我们如何跨全球网络安全生态系统展开合作？”

这些问题的提出在许多方面体现了申明这一目标的目的。这些问题为我们呈现了需要解决和克服的一些最艰巨的障碍。我们相信，回答这些问题和克服这些障碍是我们一生的最大挑战之一，尤其是对有责任践行变革的我们而言。

了解紧迫性

在说出如何组织和凝聚我们的努力与技能来实现网络安全登月的具体想法之前，我们都应当明确了解手边任务的紧迫性。网络安全不仅关乎我们的未来，也关乎我们的现在。如今，安全和经济的基本支撑依赖于数字网络技术：电网，金融市场，军事系统，水、食物、通信基础设施，以及我们生活所需的所有其他东西。

虽然数字网络技术使得我们能够打破障碍和实现最初被认为不可能的目标，但如今的现实是它们也在受到攻击——持续、复杂、坚定和无情的攻击。如今，黑客、罪犯和国家能够并且的确在攻击医院、阻止业务运营和制造全球政治动荡。

商业互联网已有 20 多年的历史，事实是我们从未采取根本性措施来确保其基本的长期的安全性。作为全球社区，作为各个国家，作为各个行业（包括网络安全行业），作为科学家、教育工作者、政府官员、企业领导者或活动家，我们还未完成这件事。你可以说打破系统，但是从一开始就打破某个从未真正存在的东西很难。

这不是因为缺乏努力或兴趣。我们绝望地希望互联网是安全的，但庆幸和遗憾的是，技术很久以来一直以闪电般的速度前进，很难跟上。就本质而言，政府和私营行业针对连锁攻击通常采取的紧急措施是短期、弥补和不够的。甚至我们目前认为最先进的一些安全技术也可能会在下一年过时。

坦率地说，我们处于悬崖边上。发生灾难性事件或一连串事件的可能性很高。目前我们事后解决网络安全威胁的零碎方法根本不可持续。如果听任不管，网络攻击越来越具破坏性的特点将会削弱我们的数字生活方式根基，威胁新技术已帮助我们实现的社会和经济增长。如果我们不在 10 年内实现目标，就将太晚了。哪怕仅从宏观思考我们就能取得显著和持久的成果。

了解挑战

拟议的网络安全登月有两个要素。第一个是：确保互联网的安全性。其核心是安全和信任，人们在上网时必须感觉安全，不担忧他们正在参与对他们具有任何实际个人危险的活动——无论是如临大敌还是心里总在惦记。

我们不应一开始就过于陷入对“确保互联网的安全性”这个定义的纠结。相反，我们应当让流程来定义它，发挥我们的最佳精力和技能来确定使人们在使用互联网时感到安全所需的特征。我几乎可以保证，当我们做到时，我

们就会知道。

网络安全登月的第二个要素是：在 10 年内实现。为什么要为我们的努力设一个时限呢？首先是我们前面讨论的紧迫性。我们无力承受对解决数字时代网络安全挑战持满足态度的代价。使世界变得更美好的潜力太重要，且风险太大。没有安全互联网的每一天都可能发生导致损害的事件。而且每次发生此类事件时，都会给我们的信心、心灵和愿望造成更大伤害。

10 年时限的第二个原因来自我们从最初登月吸取的经验。当时肯尼迪总统曾说目标是把一个人送上月球，他说得非常清楚、非常具体："10 年内完成"。这就是曾使登月使命如此大胆和引发怀疑的原因："10 年？这怎么可能？"

但这个时限成为了动力。它使美国得以把空前的资源、智囊、激情和献身精神集结在这个目标下。为了实现这个 10 年时限，美国必须团结和激发各部门的最佳精力和技能，包括政府、教育、技术、科学和私营行业。

而且此举凑效了。不仅美国把一个人送上月球并带回地球，而且此举背后的精力和努力也创造了一波改变世界的创新。因最初登月而出现的创新包括太阳能电池板、心脏监护仪和起搏器、防火材料、无线仪器和数十种其他创新。这些创新改善了我们日常生活的方方面面，从医疗和安全到替代能源和娱乐。

我们现在可以采取的行动

就像我们不应排斥今天用"确保互联网的安全性"来表达我们的用意一样，我们不应排斥能够借以实现网络安全登月的各种模式。最初的登月模式证明这可以通过由国家提供领导、愿景和资源来完成。这可能是一个成功的网络安全登月模式，或许我们将会发现其他模式。

不过，虽然我们不希望预先确定一个具体的网络安全登月模式，但我们的确知道这需要横跨多方的、集中、协作和协调的行动来实现，包括整个过程中的许多"关注者"。政府、私营行业和学术机构都有发挥作用的机会。作为领域的领导者，我们能够提供愿景、激情、领导和献身精神。我们有这个机会，就像肯尼迪总统所说："组织和衡量我们的最佳精力和技能。"

我们每个人无论身处私营行业、政府还是学术领域都能立即采取行动。而且我们可以放心，我们所采取的每个措施都将使我们逐步接近最终目标。我们必须开始把它当成一个共同旅程，发挥我们自己的专长，探索现在和将来我们所能给予的帮助。我们应当关注的领域是什么？我们能够设定什么类型的目标？以下是对网络安全登月的成功至关重要的五个关键学科：

1. **技术**：让我们面对它。我们目前的网络安全消费模式根本就是支离破碎的。我们必须开发一种保护数字资产和互动的新模式。我们必须从愈加利用人来对抗机器的传统模式演进。我们必须推广和宣传基于预防导向方法的渐进替代模式，这种方法可使我们在数字世界保持信任。这个新模式的关键要素包括：
   - **自动化与调合**：我们需要软件来对抗软件。面对机器，人类几乎无工具可用。
   - **共享情报**：共享信息对我们的共同未来至关重要。我们可以通过一个自动化的全球信息共享生态系统来实现这一点。
   - **灵活的安全模式**：我们需要选择最

佳解决方案和在需要时使用它们的能力，从而利用易于部署且经济实惠的云计算和其他模式。

2. **隐私**：隐私性与安全性相互强化。说到信任——让用户放心互联网是安全的，隐私性必须放在首位考虑。如果人们认为其财务或医疗记录面临曝光风险或者被人以可能给他们造成损害的方式使用，用户就会拒绝使用技术。同时，也可能存在能够通过信息的战略共享来实现更大好处的环境，而不会曝光个人的私人记录。我们能够阻止恐怖攻击或防止将会影响数百万人生活的重大安全漏洞吗？在便利、安全和隐私问题之间达到正确的平衡是保护数字时代生活方式的一个基本要素。
3. **教育**：教育不只是指塑造下一代网络安全专家，虽然这实际上就是一个基本要素。教育也涉及建立一个对 21 世纪数字技术使用的挑战、机遇和风险更加警醒的社会。我们的孩子开始在更小的年龄使用技术，这提供了一个在他们幼小时教育他们的机会。我们需要颠覆性思考孩子的教育方式，把所有层次的技术和网络安全整合起来。我们也必须更好地把 STEM 教育（科学、技术、工程和数学）整合到我们的课程中。我们也必须确保学校能够使用现代技术，包括宽带。而且我们必须认识到教育不只面向青少年。我们必须确保政府和企业领导者具有更高的网络感知能力，而且必须建立和培养一支更具网络感知能力的工作者队伍。
4. **国家安全**：网络攻击是一种威胁，目标并不总是可见的，而且并不总是可识别的。它们的目标不只是政府。针对金融系统、医疗和能源系统的攻击能够对任何国家的安全造成灾难性影响。把国家安全严格视为政府的权限范围大大扩大了风险。政府并不完全负责或完全能够确保互联网的安全性。事实上，很难证明政府处在任何技术领域的前沿。因此，网络安全要求私营和公共部门采取协调、合作和联合行动，来解决所有国家的安全问题。
5. **外交**：数字时代的基本事实是我们都能通过所使用的任何技术联系起来，而无论我们身处何地。网络世界的内在力量是惊人的，但也是可怕的。并非每个国家都有相同的利益。如何解决这些挑战？如何确保通信协议的全球标准化？如何在这个勇敢的新世界指导国家在某种层面的规则？正如我前面所说，这并不容易，但应对艰难挑战正是我们必须登月的原因。

迈出下一步

庆幸的是，这些不只是无聊的想法。它们反映了企业、政府、机构和个人目前已经采取的旨在解决数字时代网络安全挑战的行动。

从全球层面看，参加诸如世界经济论坛之类的活动是我们回应在这个破碎的世界加强合作的呼吁所能采取的一个关键和重要的措施。从国家层面看，各国政府都在前进。在美国，我被特许共同主持总统国家安全通讯咨询委员会下的一个分委员会，任务是进一步定义网络安全登月愿景，为政府、学术部门和私营行业联合操作此事推荐一个战略框架。NSTAC 工作