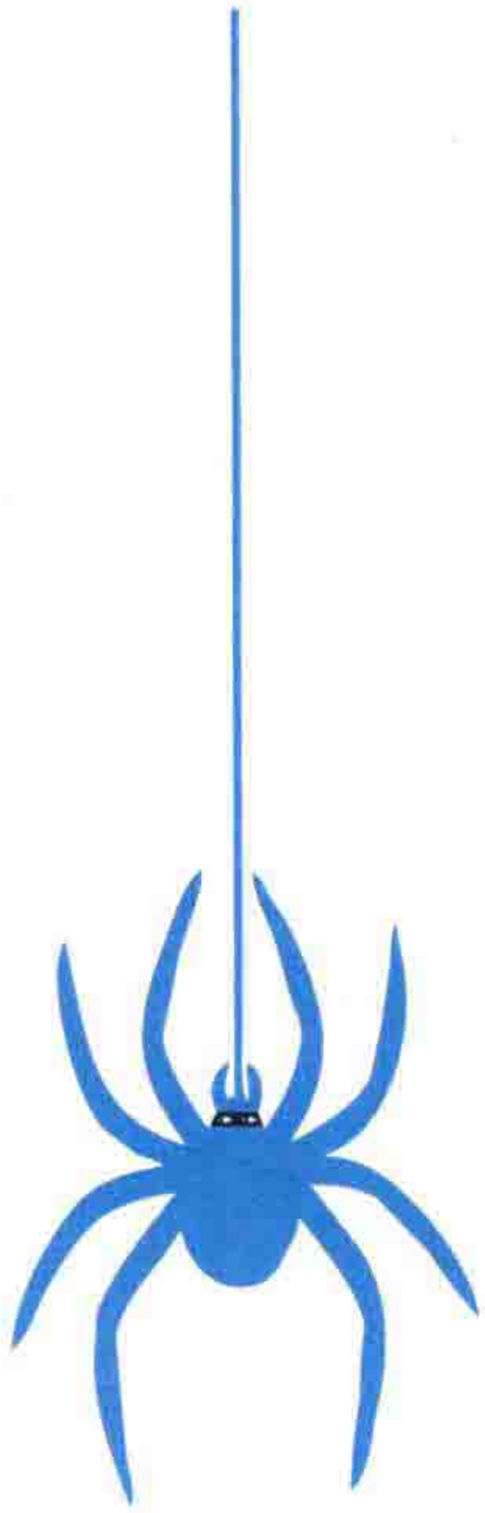
CYBERPHOBIA



Identity，Trust，Security and the Internet

网络恐惧症

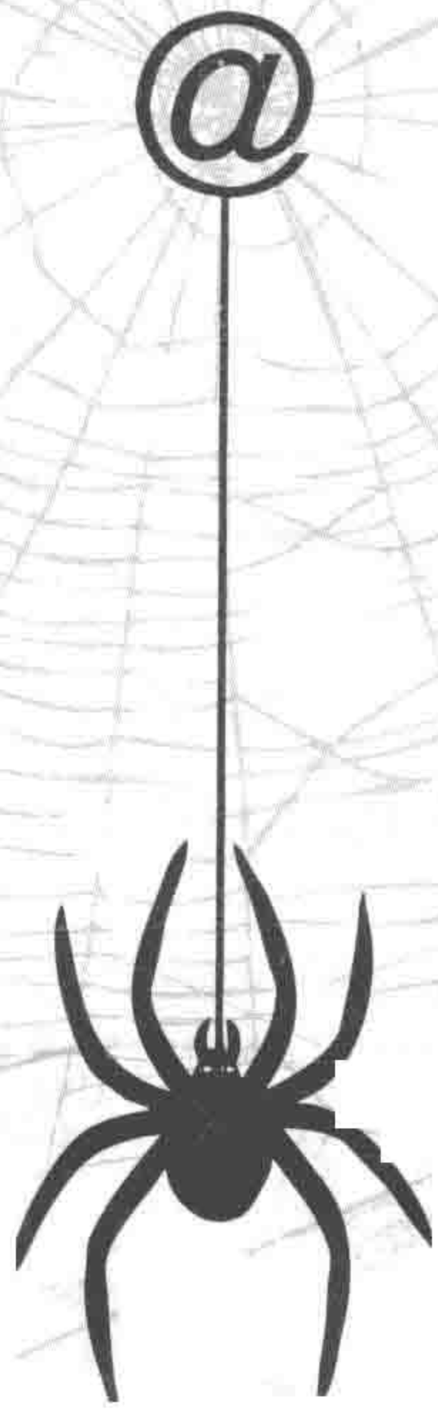
身份、信任、安全与互联网

［英］爱德华·卢卡斯（Edward Lucas） 著

王光林 译

九州出版社
JIUZHOUPRESS

CYBERPHOBIA



网络恐惧症

身份、信任、安全与互联网

[英] 爱德华·卢卡斯（Edward Lucas） 著

王光林 译

九州出版社
JIUZHOUPRESS

图书在版编目(CIP)数据

网络恐惧症 ： 身份、信任、安全与互联网 / (英)爱德华·卢卡斯著 ； 王光林译. -- 北京 ： 九州出版社, 2017.6

ISBN 978-7-5108-5467-5

Ⅰ. ①网… Ⅱ. ①爱… ②王… Ⅲ. ①计算机网络—安全技术 Ⅳ. ①TP393.08

中国版本图书馆CIP数据核字(2017)第145883号

著作权合同登记号：图字01-2016-2736号

网络恐惧症: 身份、信任、安全与互联网

作　　者	（英）爱德华·卢卡斯 著　王光林 译
出版发行	九州出版社
地　　址	北京市西城区阜外大街甲 35 号 (100037)
发行电话	(010)68992190/3/5/6
网　　址	www.jiuzhoupress.com
电子信箱	jiuzhou@jiuzhoupress.com
印　　刷	北京旭丰源印刷技术有限公司
开　　本	787 毫米 ×1092 毫米　16 开
印　　张	17
字　　数	220 千字
版　　次	2017 年 9 月第 1 版
印　　次	2017 年 9 月第 1 次印刷
书　　号	ISBN 978-7-5108-5467-5
定　　价	62.00 元

在阅读中展开，人生的可能

CONTENT

肯特文化

献给萨拉·卢卡斯

我的姨妈、教母和挚友

目　录

CONTENTS

序　言

查理·卓别林1940年完成的电影《大独裁者》激起了希特勒统治下德国人的愤怒，因为电影将纳粹领导人描绘得粗俗愚笨，盲目开展个人崇拜。[①] 在战时欧洲，所有德国控制的国家都禁播该片（尽管独裁者自己拿到了一份，看了两遍，还号啕大哭）。想象一下，第三帝国的情报部门肩负重任，受命打击报复查理·卓别林的工作室，而且还有发行该片的联美公司。希特勒的间谍或许会破门而入，盗走存放在办公室的电影正片。他们会扰乱经营活动，有时采取一些简单的犯罪行为，如到工作室纵火，有时安排一群鼓吹纳粹的暴徒到工作室外徘徊游荡（当时美国还未参战）。这些活动风险很高，而且还会徒劳无功。如果他们能想到利用电子通讯，任务就会容易多了。他们只需简单地干扰下电话总机，或者发送些假电报。不过，即便如此，这些也只会是些微不足道的干扰，他们更像是些恶作剧，而不是战争行为。

跟这种有限的选择幅度相比，针对索尼影视娱乐公司的攻击则十分有效，而且都是些匿名者。该公司制作了《刺杀金正恩》（*The Interview*），一部十足的喜剧电影。这一次的攻击不仅造成了一次迄今极具毁灭性的计算机网络破坏，而且也不知道究竟是谁犯下此罪，他们的作案手法和真正动机也不得而知。

---

① 查理·卓别林后来说道，他当时要是知道纳粹统治下大量犹太人被屠杀，就不会创作这部喜剧电影。

2014 年感恩节的周末，事态渐渐明了，袭击者使用了“恶意软件”，其中秘密安装了意图危害的电脑程序，能抹掉公司电脑上的数据。电子信箱停止工作，公司陷入瘫痪。这一切实施得干净利落，穿越了一系列的网络系统。这意味着袭击者知道到达公司的路径，并在袭击前几个月开始就一直在做侦察活动。抹掉数据杀伤力极强，这等于是在公司最重要的一幢大楼内放了一场严重的电子大火。不过这并不是最具破坏力的袭击。更糟糕的是被盗数据的质与量：据悉被盗的数据共达到了 100 个 TB。

要评估这一切难度很大，因为有太多的计算机被抹掉了。不过有一点很清楚，至少有五部未发行的电影被窃取并公布在互联网上。袭击者同时还复制公布了 47,000 条个人信息，涉及现职和离职员工，承包商和自由职业者（含诸多名人），此外还有大量电子邮件信息。所有这些都在不断制造破坏效果。丢失的影片直接影响到了公司的盈利空间：工作室不遗余力防止未授权的作品复制件在发布前流出，或在发布后被制作。由于雇员信息受到合法保护，因此雇员可因公司未妥善保管其个人信息而起诉公司。2014 年末，部分诉讼已经启动。

然而最糟糕的是公布那些本为私密的信件。尤其是高管间来往信函中包含的那些极其尴尬的交流信息。资深制片人斯科特·罗宾在写给公司董事长艾米·帕斯卡的邮件中将好莱坞影星、同时也是索尼最重要的演员之一安吉莉娜·朱莉描述成“她一定是疯了”和“一个天赋最差娇生惯养的小鬼”。在另一封邮件里，一位编剧解雇了一位有名的爱尔兰裔德国演员，理由是：“我不知道谁是迈克尔·法斯宾德，这世上的其他人也不会关心这个问题。”或许最糟的一封电子邮件是嘲笑总统贝拉克·奥巴马，暗示他只对黑人主演的电影感兴趣，很难说这样做不是种族歧视。

攻击索尼的细节一滴一滴地给挤了出来。这并未摧毁公司，也未阻

止《刺杀金正恩》一片的发行。在这场针对播放该片的所有影院的攻击中，索尼表现出一副俯首称臣的样子。不过，经过这次尴尬的大逆转，公司于 2014 年将这部针对朝鲜的喜剧放给了线上观众，并发行给一些有限的独立影院。该片赚了至少 1800 万美元，而制片预算则是 4400 万美元。

但已知的（未知的也许更重要）这段插曲例证了本书的主旨：计算机和网络对现代生活非常重要，同样重要的还有计算机与网络中隐而未现和不为人知的各种漏洞。

互联网是所有网络的总网，连接着地球上的大多数计算机。互联网不仅成为现代生活的中枢神经系统，还是现代生活最大的隐患。互联网变化的速度让人震惊。如果说在冷战时期，好莱坞制作了许多反苏电影，结果导致苏联意图攻击好莱坞，那么它会跟纳粹攻击卓别林一样，选择相当有限：实体入侵、破坏活动和政治施压。

直到 1989 年，苏联解体，蒂姆·伯纳斯·李发明了万维网，即计算机用户浏览互联网的方式。设计的初衷是帮助欧洲原子核委员会（CERN）量子物理实验室的科学家们。但实际上，这是一种在网络上标签数据的方式，以便不同的人在不同的地点可以同时查阅他们所需的文件。即使是最远见卓识的人也未料到，它会被用于破坏性目的，或会发展成为一项有数万亿美元价值的产业。

直到 20 世纪 90 年代中期才出现现代意义上的因特网，此后又过五年，公司才开始将其作为一项重要工具使用。1995 年，仅 1600 万人在使用因特网，而其中大多数是计算机发烧友。这些人仅占当时世界人口的 0.4%。尽管在当时，或许他们应当考虑安全性问题，但几乎没有人注意到这一点。因特网发展为连接学术网络的方式，其主要目的是促进研究人员合作。他们不会在自己的计算机上存储敏感的私人信息，或是用计算机办理银行业务和购物。十年后，使用因特网的人数超过了 10

亿，占人口数 15.7% 以上。如今这一人数超过了 30 亿，接近世界总人口的一半。在发达国家，使用互联网的水平达到了通用的程度——88% 的美国人已经联网。

互联网的重要性并不单单体现在使用人数上。它是世界上最重要的通信系统。2015 年，平均每天发送的电子邮件就超过 2000 亿封。这就意味着两天的电子邮件总量，就超过了世界邮政运输一年的总量。发送电子邮件的这 25 亿人中，鲜有人了解电子邮件是如何抵达目的地的，他们还误以为电子邮件能既可靠又隐秘地到达。也许更大的误区是，他们想当然地以为他们收到的电子邮件，就发自其所声称的发件人。

计算机存储也已经成为全世界存储数据的方式。一台单独的计算机就能运行拇指大小的存储器，里面包含了超过 5.28 亿打印页面的数据，大约是一个人的大脑能容纳的数据量。过去，电影工作室将作品存储在覆盖着银盐的胶片上。要想偷盗作品，就要把笨重的胶卷搬出戒备森严的存储设备，不但要突破人眼的看管，还要突破只能用实体钥匙打开的层层大门。如今这些影片，和大多数其他宝贵的知识产权一样，都存储在由计算机控制的电子媒介中。有正确的密码（有时也不需要密码），就能不知不觉，悄无声息地拷贝、删除和移动数据。

存储在计算机上的不仅仅是知识产权。我们把日复一日的生活点滴都存储在计算机上。从索尼影视娱乐公司盗取物中，单单一个文件夹里就包括如下数据：

至少 3000 多个社会保险号，姓名，联系方式，联系电话，生日，电子邮箱地址，员工福利，工伤赔偿明细，退休及停职计划，员工过往工作记录，管理层工资，医疗计划，牙科保健计划，性别，雇员编号，销售报表，护照信息复印件和差旅费发票。

公司存储在计算机上的信息有些是微不足道的。索尼影视娱乐公司在哪里买回形针重要么？但是，那些包含着私密或宝贵数据的网络有意无意之间都跟那些不太重要的数据网络连接起来了。

总之，互联网已经成为现代生活的舞台。它已经是我们通讯交流，休闲放松，保存回忆，查找信息和交友办公的场所。在未来的岁月里，互联网仍会变得更重要，因为它已经从一种连接人的方式转变为一种连接事物的方式。这就意味着我们家中的机器，如我们的电表、恒温器、冰箱和微波炉，将会共同运作，节约用电。在工业过程中，机器无需人工干预就能相互连接。超市收银台已经能提醒仓库注意需求的变化，提早准备所需运力。数十亿计的机器和设备将能联网，这一数量远大于联网的人数。

从个人层面来看，人类越来越依赖科技是有道理的。边际效益很明显：便利性、可靠性、机动性和安全性都在提高。如果你的对手和同伴在使用计算机和网络，而你不用，代价就很高昂。一个公司如果放弃了电子邮件就可能失去订单，一些拒绝携带移动电话的人可能会错过重要的消息。生活无情，时光飞逝，请保持更新，机会可能只有一次。

然而在整体层面上，这些个人决定产生了一个问题。一旦所有人都依赖科技，科技就最好是可靠的。就互联网来说，其可靠性是值得怀疑的。它的设计理念就是机动开放，并非安全可靠。

因特网的创始人是专业学者，不经证实就相信了用户的身份。当科研合作恰处于紧要关头时，这样做是合情合理的。然而，缺乏安全认证现在正阻碍着电子商务的发展和网络公共服务的供给。在日常生活中，从办理银行业务到约会，一旦你不了解跟你打交道的对象，你就很容易上当受骗，或屈从于缓慢烦琐的程序，诸如扫描并上传文件来证明自己究竟是谁。

相对现实世界来说，互联网有一定优势。由于互联网的升级方式，

它还没有用尽网络地址，不像某些大城市已经用尽了电话号码。互联网不会像交通系统那样，受糟糕天气的影响。确实，多亏互联网的设计方式，它本来就有自我修复力。与电话系统不同，互联网不是在人群间建立直接联系，而是将信息切碎成小数据“包”，以最便捷的方式使其到达目的地。一旦一条路径拥堵受阻，就会选择其他路径。数据包在另一端重新装配，再现原始的电子邮件，图片，文件或其他信息。

互联网更大的漏洞在于复杂性和混乱性。计算机和网络十分复杂。当我们使用时，我们不能确定自己究竟在做什么，究竟在和谁打交道。这为各种攻击者创造了一片天堂。这些人可以是间谍密探，士兵军人，流氓阿飞，搞怪专家，犯罪分子和商业对手，或是干脆就是这些人的大杂烩。在确保计算机和网络安全中，归因是唯一最棘手的问题，正是因为归因，使得如何回击这一问题十分难解。攻击索尼公司的罪魁祸首可能是朝鲜当局，他们因为心中崇拜的领导人遭到诋毁而心生不悦。但也可能是平壤方面买通了其他国家的黑客所为。也可能是激进分子，他们不喜欢索尼在数字作品版权问题上的立场，抑或如某些安全专家所述，是心存不满的公司员工所为。传说中的攻击者看着自己的杰作洋洋自得，虽然他们公布在网上的信息含混不清，但根据语言学分析，从其英文僵硬，错误频频来看，写程序的人可能以俄语为母语。美国联邦调查局（FBI）声称朝鲜应对此负责，但并没有发布任何确凿证据。圣诞节期间，朝鲜因特网和移动电话系统出现了两次崩溃数小时的情况：在这个世界上网络连接最不发达的国家，这不是什么稀罕事，不过未免太过巧合。这难道就是美国承诺中的以牙还牙？又或是别的原因？相同的手段能否用到其他国家身上？此类事件在计算机和网络世界里司空见惯，却并没有一个明确的答案。

线上生活的复杂与混乱已经超出了我们身心所能应对的程度。在我们家园之外，在更广阔的外部世界中，追求安全感是我们的本能反应。

我们知道有的邻居更靠谱，知道有些人要特别警惕。我们会在有的情形下，如旅游途中，保持低调。节假日里，在贫穷国家集市上逛街时，我们浏览商品、砍价和付钱的表现，与在富裕国家高档精品店里的表现截然不同。我们和信赖的人交易更快，通过外貌、行为和语气来评价陌生人，通过介绍人和亲友与之建立义务，分享权益。凌晨时分，一个体格健壮，衣衫褴褛，有点醉醺醺的年轻人来到我门前是种威胁，后来我儿子提醒我，他们不过是在等客人。

和我们的上几代人一样，我们在现实生活中的安全依赖锁和钥匙来保障，而且我们已经很好地认识到了它们的优势和劣势。我们不会用儿童挂锁来锁家里的大门。我们也不会用精密的防盗系统来确保花园小屋的安全。与他人共享钥匙时，我们会本能地平衡风险与便捷的关系：小孩子或许有家里大门的一把钥匙，但不会有一大串钥匙。在家里，我们或许还有保险箱来存储贵重物品和文件。我们还知道只有锁是不够的：我们在家里和办公室还会配备自动报警器，移动探测器，甚至闭路电视监控系统。此外我们还会配备人力：前台有接待人员当值，公寓楼里有门房当班。要是真有一个坏邻居，就是最坚固的锁也不能确保安全。在最安全的乡村地区，人们不用烦心去锁门，甚至为了方便起见还会把钥匙放在车里。

我们多多少少会去感谢那些设计、制造、安装和维护锁的人，认为他们十分专业。但几乎不会有人对细节有丁点儿兴趣。我们不需要当个锁匠才能开锁，正如我们不需要当个汽修工就能开车，不当医生也能保健一样。现代生活赋予了我们许多既不需要知识，也不需要灵敏就能完全掌握的能力。我们通过经验和本能，就能知道他们的优势和局限性。

简而言之，进化和教育赋予了我们大量的技能来平衡风险、安全和便利的关系。我们天生就是要相互信赖，相互帮助——原始人不可能单独生存，与此同时，我们也在从事一系列的观察和行动，而且大多是无

意识的。我们的眼睛、耳朵和鼻子会告诉我们是安全还是危险，该做什么，在哪里做，什么时候做。

一旦我们在网上冒险，上述一切都烟消云散。我们对真实世界的感知被抑制：所有我们要设法应对的是屏幕上的文字和图片，以及小喇叭里发出的细小声音。它是真实世界的拟象，但也是假象。我们做熟悉的日常活动时，也许会觉得信心满满，我们能购物、浏览网页、打网络电话、发电子邮件，但事实上，面对盗贼、操控手和敌手，我们感到无助，缺乏准备，容易受到攻击。我们看不到跟自己打交道的人，我们不能评价他们的语气，肢体语言或是面部表情。我们既闻不到也摸不到他们。我们无法将这些人定格在我们生活的历史和地理空间里。我们也不明白自己究竟在试图保护些什么。锁和钥匙只是作用有限的类比物。数据与实体资产不同：其价值取决于情境。一列姓名和地址本身并没有什么意义。一旦被标入秘密警察的线人目录，那么名单上的所有人员就会陷入危险。但我们不得不应对这个世界，并使用我们大多数人都弄不明白的技术。

此外，在真实世界中我们应对各种机构时，所采用的习以为常的保护措施，在网络上是不存在的。如果我们丢了钥匙，房子就陷入了被盗的危险。但如果我们丢了护照，我们不认为盗贼会因此而把我们的生活洗劫一空。例如，如果有一个人，长相、穿着和说话方式都像一位客户，他伪造签名，用盗取的护照提取了一些钱，蒙骗银行，那么，该支付这笔钱的依然是银行，而不是被偷盗的受害者。受害方只需证明并不是他本人来银行完成的交易即可免责。

但互联网改变了上述情形。电子安全将发现和防止诈骗的职责，由企业转嫁到客户身上。一旦你的密码和登录名被用于盗取你的钱，银行就会主张你要为未妥善保管而负责。然而，很可能是一台被篡改过的自动取款机，配备了能盗取卡号和个人识别码的智能设备，盗取了你的银

行卡详细信息。或许是因为盗贼在你的计算机上安装了什么，导致你登录网银的登录名和密码被复制了。但无论是哪种情况，证明无过错的责任都在你自己，不在银行。计算机将举证责任转嫁给了个人，而它转嫁的方式我们依然还没有清醒的认识。

网络安全曾是小众问题：复杂，无趣，边缘化。现在它却成了至关重要的问题，但理解起来仍旧困难。本书试图阐释的是计算机和连接计算机的各种网络安全问题。正如你无须当医生就能谈论医疗卫生，无需当汽车工程师就能谈论道路拥堵一样，你无须具备计算机科学的专业资格，就能理解你的计算机以及与之相连的他人计算机中的安全要素。

正如医学、法学、政治学和其他生活科学都被专业人才统领一样，这一课题也充满了缩略词、术语和语言的特殊用法。你们公司有没有雇“测电笔”用“社会工程学”来评估你的“攻击面”呢？这句话听起来太难了！然而实际上你是在花钱雇一个专业的欺诈魔术师，来看看你的安全性是否如你所想的那样好。一旦“白帽黑客”在攻击你的“粮仓”，另一个魔术师就会用纯电子手段，看看不同的信息是否会被合理地分开保存。

本书之所以题名为《网络恐惧症》（*Cyberphobia*），是因为技术语言复杂得多，使得许多人心生回避，没有意识到已经面临着的这些问题的重要性。关于该主题有许多书籍，详细地从技术细节上解释如何建立和防御所谓的安全性计算机网络。这些书更像是锁匠的技术手册：专家感兴趣，于外行却无用。

本书的中心思想是，我们对计算机的依赖变得越来越快，而我们预防攻击者的能力相对滞后。犯罪分子、流氓阿飞、激进分子和外国敌对势力，时常攻击个人、企业、组织和政府。他们获益颇丰，我们损失惨重。除非我们改变想法和行为，否则我们会变得越来越不安全，越来越不自由，越来越不健康，也越来越不幸福。我们首先应该理解到，网络