<<2020，世界网络大战>>

图书基本信息

书名：<<2020，世界网络大战>>

13位ISBN编号：9787543879881

10位ISBN编号：7543879883

出版时间：2012-1

出版时间：湖南人民出版社

作者：东鸟

页数：382

前言

网络战争的“零日威胁” 11年前，美国哥伦比亚广播公司“60分钟”栏目组曾到五角大楼录制网络战争的节目。
当时，网络战争还只是停留在理论上。
今天，网络战争不再是理论上的假想，而是每天发生在我们身边，成为真实的“零日威胁”。
2020年中美将爆发网络大战 斯托弗·布隆克，是美国前外交官、莱斯大学信息技术和公共政策专家。
2011年3月，他在美国空军刊物《战略研究季刊》发表题为“炸毁：中国的网络战争（2020年8—9月）”的文章。
他极尽想象，假想未来美国及其同盟国和中国之间爆发网络战争的景象。
布隆克假设未来10年，中国以“挑战者”身份，引爆中美网络大战。
届时，美国以台湾问题或其他事情为由，拒偿中国债务；美印在印度洋扩大军事存在，令中国担心石油及波斯湾和非洲原材料运输航道安全，日本海上力量持续壮大，具备制衡中国崛起的实力，新加坡成为中美争夺的焦点，因为新加坡对马六甲海峡有着重要影响。
因此，中国很可能在2020年夏末，在网络空间击败美国，并控制马六甲海峡。
2020年8月，崛起的中国希望将新加坡揽入怀抱，就像香港、澳门和台北。
在对新加坡发动攻击前几周，中国就已发起大规模网络战，目的是破坏美国、日本和其他盟国的通信能力。
解放军6万网络部队渗透到美国军队、政府和企业的网络系统，并实现系统控制。
2020年9月，当解放军首次在南中国海袭击新加坡的导弹驱逐舰时，美军发现通信能力骤降。
计算机、无线电、卫星通信以及战地通信设施全部陷入瘫痪。
军方网络和服务器受到攻击，向陆地指挥官和海上舰船提供错误情报，以致五角大楼未能及时调动常规部队行动。
美军国防信息系统局发出警告：不明计算机代码正试图绕过国防部绝密电脑网络的高低二极管，进入未加密主机，目标是宾夕法尼亚的陆军军械库。
美军网络专家立即进行反击。
55天后，随着中美两军陷入僵局，这场亚太冲突结束，没有达成任何公约或协议，甚至没有进行国际交涉。
由于两国希望规避风险，只需从网络战场撤退即可，一场全面战争得以避免。
新加坡依然保持独立。
但是，中美双方都有潜艇被击沉，航空母舰舰队始终在对峙。
上面这个场景，可能与许多人的预想完全不同。
尤其是对谁首先发起网络战争这个问题，多数人的观点会与布隆克完全相反。
实际上，从2008年起，美中经济与安全审查委员会、美国智库战略与国际研究中心和国防部，就陆续推出应对网络战争的报告。
奥巴马上任不到4个月，就将网络战争视为“最严重的经济和国家安全挑战之一”，承认网络战争“从理论走向实战”。
五角大楼甚至提出“网络威慑”概念。
国务卿希拉里发表“网络自由”演讲，大力推行网络外交，组建网络司令部，社交网站助推西亚北非动荡…… 2011年6月，美国国防部长盖茨在新加坡演讲时首次表明，在确认遭到来自他国的网络攻击时，将“视为战争行为并以武力还击”。
美国成为网络战争的先行者。
全球已进入网络战争时代 2009年11月，网络安全公司迈克菲（McAfee）发布报告《近在眼前：走进网络大战的时代》，称美法等大国正积蓄力量警惕网络冷战爆发，他们积聚网战武器、搞间谍活动等，以利用网络控制战争。
报告作者是美国国土安全局前顾问保罗·库尔特，他对20多位国际关系、国家安全以及网络安全专家

进行采访后完成了这份报告。
报告认为，备战网络战争的国家，以美国、以色列、俄罗斯和法国最积极。
报告称，“事实证明，网络战争随时可能爆发，全球进入网络冷战时代。
”比如，2009年7月，美国和韩国网站遭到大规模攻击，黑客试图切断韩美军与五角大楼及夏威夷太平洋司令部的网络通信。
还有许多网络攻击事件也带有战争意味，比如爱沙尼亚、格鲁吉亚分别在2007年和2008年遭到网络攻击。
美国国家安全局前副局长威廉·康沃尔说：“20到30年之内，网络战争将成为未来战争的重要组成部分。
我唯一不能预测的，是网络大战可能会对未来社会造成的影响。
” 2010年初，美国战略与国际研究中心完成《交火：网络战争时代的关键基础设施报告》，对14个国家600家IT和基础设施企业进行调查。
报告称，56%的受访者认为，网络攻击的首要目标是金融信息，然后是能源，如电力、石油、天然气部门，其中一半以上网络攻击是针对计算机操控系统的。
如，广泛用于电力系统的数据采集与监控系统（SCADA系统）几乎没有安全措施。
白宫前反恐顾问、国防部前部长助理理查德·克拉克，曾描述过一场世界末日式的可怕情景：由于病毒和其他网络武器令飞机无法起飞，并引发核爆炸，美国在几天之内就回到了石器时代。
这就像施瓦辛格主演的《终结者3：歼灭者》的情节，由病毒控制的“天网”系统引发全球核爆炸，毁灭了人类文明。
这不是危言耸听。
2011年初，南加州一家大型供水企业计划探测工业控制系统的漏洞，便雇用洛杉矶著名黑客马克·迈弗雷特进行测试。
仅一天时间，迈弗雷特就控制了对饮用水进行化学处理的设备。
他只需轻点几下鼠标，就能让数百万家庭的饮用水不能饮用。
被迈弗雷特攻占的工业控制系统，同样应用在电力网、输油管道、化工厂等基础设施上。
工业控制系统一旦遭到攻击，将导致街区爆炸、银行数据丢失、飞机坠毁，以及大面积停电。
2006年，在美国举行的一次测试中，黑客竟能远程摧毁一台重达27吨、价值100万美元的发电机。
发电机会失控旋转，必须强行关闭。
如今，网络战争已是一种现实威胁。
2011年6月，国际货币基金组织（IMF）爆出内部网络系统遭黑客袭击的消息。
黑客先是盗取大量文件，然后又下载各种信息。
事发后，一街之隔的世界银行，切断了与其的网络连接。
这次事件触动了世界神经。
因为IMF正忙于处理对葡萄牙、希腊和爱尔兰的金融援助问题，掌握三国“敏感数据”。
IMF作为应对金融危机的重要国际组织，握有各国财政绝密信息，以及各国领导人的有关秘密协商材料。
一旦泄露，将引发维基解密效应，不仅会引发金融市场波动，对世界经济复苏造成负面影响，还可能引发部分国家社会政治动荡。
强大之争的中美国网络空间冲突 2010年5月，首届世界网络安全峰会在美国达拉斯举行。
各国代表认为，网络攻击将导致新一轮国际矛盾，激发中国、印度、俄罗斯、美国等之间相互防卫、相互猜疑，甚至引发网络战争。
当前，国际形势正经历“冷战”结束以来最为深刻复杂的变化。
金融危机以来的世界情势，如同20世纪初一样，出现新一轮的动荡不安，全球经济复苏缓慢，西亚北非政局动荡，军备竞赛愈演愈烈。
在现实世界，美国作为唯一超级大国，始终谋求世界与区域霸权和领导地位；中国作为最大的发展中国家和社会主义国家，追求的是多极化与独立自主。
在网络空间，美国是第一强国，掌控全球计算机和互联网的核心技术和重要应用；中国则是第一大国

，拥有最多的网民数量和最大的产业市场，与美国的市场竞争和文化对抗更加直接。
哈佛大学教授弗格森和柏林自由大学教授石里克，曾共同创造新词“中美国”，强调中美经济关系。
西方舆论借机鼓吹“中美国共同体”和“中美G2时代”，鼓噪“中美共管世界”。
这完全不切合实际。
因为美国绝对不会让中国同它一起演奏“二重奏”。
面对中国的发展壮大，美国心态十分复杂，可谓“羡慕、嫉妒、恨”。
其从骨子里就把中国视为霸权挑战者和政治异类，戒备防范与歧视偏见始终深重。
现在，美国已把这种心态带到网络空间，视之为“传统和非传统冲突的主要阵地”，决意在网络空间与中国一较高低，并竭力保持绝对优势。
美国政界和军界都十分看重网络空间的跨国属性和战略价值，大肆渲染中国、俄罗斯等国家的网络威胁。
他们炮制“中国网络威胁论”，指责中国黑客对美国军事和商业部门进行攻击，同时制定《网络空间安全政策评估》、《网络空间作战能力构想》等报告，把防范重点对准中国。
美国还试图以打击全球网络犯罪、网络恐怖主义为由，发展先发制人的网络攻击能力，并对他国发展网络战力进行约束。
2010年8月，国防部还向国会递交《中国网络战争执行能力报告》，指责中国政府和军队“指使”民间黑客集团向美国政府和商业部门发动网络攻击，不仅抹黑中国形象，还为对中国进行网络制裁制造口实。
现在，美国已经把网络议题作为中美外交的新摩擦点。
奥巴马、希拉里都把网络空间作为全球外交和传播西方价值观的主战场和主渠道，利用优兔、脸谱、推特等社交网站和谷歌博客等，插手中国经济社会热点问题；鼓噪谷歌退出中国大陆市场事件，两次发表“网络自由”演说，点名道姓指责中国；西亚北非多国出现政局动荡后，又企图把动荡祸水通过互联网引向伊朗、中国等国家。
2011年8月，迈克菲发布《隐蔽远端存取木马行动》报告，强烈暗示中国是全球黑客袭击的源头，是美国最需要防范的网络敌人。
可以预见，美中两国在网络领域的矛盾必将日益加剧。
不是“擦枪走火”的意外事件　再回到布隆克的那篇假想文章。
因为他对中美网络空间必有一战，还有着更深的解读。
布隆克认为，中国在网络空间与美国发生冲突，不可能是“意外擦枪走火”。
1991年海湾战争伊拉克的惨败，解放军对美军不可思议地运用信息技术指挥战争，多次在战争关键时刻发挥压倒性优势充满敬畏。
中国至少要拥有致瘫美国亚洲盟友的能力。
他还绘声绘色地描述：2020年，解放军将建成数字行动指挥部，负责指挥6万多网络士兵。
7大军区各建超过4000人的网络战团。
在上海之外，中国成立了一支整编网络战师，专门针对美国政府及军队网络。
但是，美国最担心的是北京郊外的“信息与通信作战研究所”，其专门进行网络战争战略、战术和技术研究，直接向中央军委汇报，与中国科学院有密切联系，工作人员至少有1.5万人。
外界对这个“国家黑客实验室”知之甚少。
直到2018年7月，一个化名“万路”的工作人员借口续签旅游签证，走进澳大利亚驻东京使馆并叛逃，外界才获悉这些情报。
布隆克的上述假想，意在突出中美网络冲突是一种必然。
他还假想，中国网络部队蓄谋已久，早已渗透进美国在华企业网络。
中美冲突爆发后，他们就利用从这些网络搜集到的信息制造混乱。
各种错误信息被混入美国企业的网络系统。
联邦快递和联合包裹服务公司等被迫停止所有业务，因为网络系统会将包裹发送到除正确目的地以外的任何地方。

对五角大楼来说，届时将很难知道美军在干什么，更不用说敌人。
航行在太平洋上的舰船，将遇到种种航行和数据链接问题。
他还假想，中国的网络攻势极具破坏力，不仅仅瞄向高度安全和机密的美国网络，还渗透进许多军民部门的非保密性网络，以获取相对低级别的信息。
这对中国了解美国的部署和战略也非常有用。
如，可以详细了解美军调动、对燃料及其他基本物资的需求等情况。
布隆克认为，为了应对中国的网络攻击，美国必须从国家安全局、国土安全部、国防部信息系统局、中央情报局、国务院、司法部及其他机构调动一切可调动的资源。
高级理论专家、工程师甚至是语言学家及私营部门专家也要参与。
尽管这样，还是要好几周才能瓦解中国的网络进攻，并实施网络防御，然后重新恢复美国网络系统。

<<2020，世界网络大战>>

内容概要

谁控制了互联网，谁就控制了世界。

自世界各国接入互联网以来，一场以键盘、鼠标为武器的新形态战争便悄然拉开了序幕。
2010年，美国网络司令部全面运作，英、俄、印、日、韩等国紧随其后。
2011年，美国公布《网络空间国际战略》，将网络战略提升到国家战略的高度，吹响了在网络世界攻城略地的号角。

今天，网络战争已经直接影响到国家安全和社会生活的每一个领域。
政治上，无论是西亚北非，还是东欧拉美，网络舆论正催生着一场场现实世界的“颜色革命”；经济上，西方网络公司巨头正在全球各地渗透势力，攫取巨额利益；军事上，高端网络武器能够轻易侵入他国网络系统，使其全面瘫痪……网络战争已足以操纵全球信息流动和世界经济命脉，改变国家力量对比和世界政治格局。

本书以全球视野和国家维度，从现实威胁和战略高度，披露了世界各国的网络战争情势，分析了各国在网络空间的国家战略和生死较量，揭示了以美国为首的西方国家正在网络空间发起新一轮攻势，昭示了东西方阵营的世界网络大战一触即发！

作者简介

东鸟，网络战争研究专家，现供职于某研究机构，著有《网络战争：互联网改变世界简史》《中国输不起的网络战争》《维基解密：阿桑奇和他的解密王国》等。

<<2020，世界网络大战>>

书籍目录

章节摘录

 推特塑造特别代表影响穆斯林世界 2010年夏，罗斯和科恩在华盛顿会见法拉·潘迪思（一个新设职位的负责人，国务院穆斯林团体的特别代表）。
潘迪思出生在克什米尔，很小时就移民美国。
她40岁出头，精力充沛，口齿清晰，富有吸引力，负责与持续怀疑美国动机的多样化群体进行对话，为美国利益服务。
她在2009年9月上任以来，一直都很活跃，去过25个国家，致力于扩展美国和穆斯林团体的互动范围。
刚从印度、荷兰等国返回的她，与副手凯伦·钱德勒等着罗斯和科恩帮她出招。
在会见中，科恩和罗斯致力于让技术帮潘迪思作出比徒劳无功的洲际飞行更多的业绩。
“我们要解决这个问题，”罗斯说，“一个部门用满天飞的方法，要顾及地球上14亿人，这在物理空间上是不可能的。
我们应该跟你合作，搞出一个连接技术的战略来。
这就是我们正在解决的问题。
”“不管你去哪里，”科恩说，“你身后都要留下你支持穆斯林的雪泥鸿爪。
这叫‘BOF计划’。
”接下来，罗斯和科恩用了半小时谈“BOF计划”。
重点是如何利用这个无可争议的资产——潘迪思，一个代表美国政府的女士，一位伶牙俐齿的迷人女性，跟一个庞大而多元化且继续怀疑美国动机的人群对话；以及如何利用网络信息技术来提升她的形象和影响。
这将带来比无休止的洲际飞行要好得多的效果。
科恩说：“我们需要一个真正好的#号标签，比如‘#支持穆斯林’。
”但是，大家都认为“#支持穆斯林”这个标签太长了。
标签不一定要当场定下来。
罗斯说：“你有一大堆好材料。
我们要有人去看一遍，抓到重点。
在这过程中，要明白不管你说了些什么，都要能够压缩成140个字，或者更少。
比如说有10件事情，我们就把它翻译成普什图语、达里语、乌尔都语、阿拉伯语、斯瓦西里语等。
下一步就是我们要在推特、脸谱和其他社交网站上找到‘有影响’的穆斯林人物。
简单地说，我们用适当的、柔和的网络外交手段，接触到他们。
”这样，国务院就可以向穆斯林发送消息，并向他们表明：“这是与你们价值观一致的信息。
这些虽然是来自美国的声音，但我想你们愿意听到这些信息，所以我们将其放在这些社交网站上……”于是，美国就得到了穆斯林群体中的“青年领袖”，再让这些“青年领袖”负责在推特上发微博信息，号召人们跟随她（潘迪思）。
比如，可以把“#关注这个女人”（暗指潘迪思）的标签放到他们使用的主流社交网站上去。

后记

有人曾讲过：互联网是美好的，因为我们的现实世界是美好的；互联网是丑恶的，因为我们的现实世界是丑恶的。
其实，发生在网络世界的一切，美好的或丑恶的，都是我们这个现实世界的写照和延伸。
一年以来，网络世界与我们的现实世界一样，发生了许许多多的事情，既有美好的，也有丑恶的。
网络世界大事件的波及范围，遍及世界每个角落，对当今世界政治格局产生着深远影响。
在网络世界版图之中，不论是西亚北非，还是拉美北美，不论是东欧南欧，还是东亚中亚，都上演着与现实世界一样的硝烟战事。
只不过，这些战事更加隐蔽，常人难以察觉。
就从伊朗与美国的争端看，虽然两国在现实世界战事未起，但是在网络世界的战争却早已开始。
伊朗核电站遭受病毒攻击、军火库无端爆炸，以及破获美国间谍网络、建立“清洁内联网”等，无一不是美伊两国在网络世界的较量。
这些无疑给我们敲响了战争的警钟。
今天，人类社会从来没有像现在这样高度依赖于互联网这种科技发明。
互联网似乎在超越其他一切人类伟大科技发明，改变和重塑着我们的现实世界。
但是随着网络信息技术的快速发展和普及应用，很快就出现了一个悖论：依赖性和脆弱性的矛盾，即人类社会对互联网的依赖性越强，经济社会运行的脆弱性也就越强。
现在，各国的关键部门、重要产业等经济社会领域，正在被互联网联成一体，形成各个国家的“关键性基础设施”，包括政务、电力、交通、能源、通信、航空、金融、传媒、军事等领域的网络系统。
由于技术水平和人为因素，互联网存在着先天不足的硬件“缺陷”和后天不备的软件“漏洞”，其日益暴露出严重的安全威胁。
这不是危言耸听。
实际上，谷歌退出中国内地和紧随其后的希拉里“网络自由”宣言，都预示着一个难以预知的历史阶段来临。
21世纪的国家安全已经超越了传统安全领域，成为一个涵括国防安全、金融安全、信息安全、环境安全、公共安全、能源安全等领域的全方位、多层次的国家安全体系。
众多安全领域，无不涉及网络安全的范畴。
最近，俄罗斯爆发反普京抗议示威游行。
这背后不难看到西方国家的身影，如美国国务卿希拉里乘机批评杜马选举不自由、不公正，欧盟也声称点票过程出现违规，大喊“俄罗斯之冬”到了。
美国资助的选举监察组织Golos网站，成为揭发选举舞弊的重要平台，也是激发示威的重要导火线。
很多俄罗斯民众通过脸谱网站获得相关资讯，受到推特信息鼓动。
美国共和党参议员约翰·麦凯恩也加入批评俄罗斯的行列，甚至在社交网站上给普京留言称：“亲爱的普京，阿拉伯之春正在你家附近上演。
” 以前我们讲，弱国无外交，现在是弱国无信息自由。
2009年6月，伊朗总统大选发生骚乱，美国国务院官员让推特网站推迟网站的维护时间。
因为网站维护会影响信息传播，影响美国帮助伊朗反对派传递信息。
这充分表明，美国在利用技术优势控制网络话语权，为美国的利益服务。
美国意识到，电子邮件、聊天工具和社交网络都是“强大的工具”。
2011年11月，美国2012年总统竞选候选人、前驻华大使洪博培在竞选辩论对华政策时宣称，要利用美国政府在中国内部的年轻网民来搞垮中国。
这位可能的未来美国总统是这样说的：“……必须依靠我们在中国内部的盟友和支持者，他们被称为‘年轻一代’，或是‘互联网一代’。
要知道在中国一共有5亿网民，8000万人在玩博客。
这一代网民将给中国带来巨大的变化，而这些变化将削弱中国的实力。

” 本书要努力说明的是，西方国家正在网络世界发起征服中国乃至世界的战略总攻，中华民族再度“到了最危险的时候”。
本书要向国人敲响警钟，让社会大众和高层领导更好地认识和理解当今网络世界的战争对峙状态，在现在和未来的生活工作中做出正确的判断和决策。
我们每一个人都必须认识到，这是一场全方位的较量，政治、经济、文化、科技等一切领域的较量。
作者 2011年12月于北京

媒体关注与评论

开辟一个网络战场，目标就是用西方价值观统治世界，实现思想的征服。
——美国 《国家信息基础结构行动计划》 网络战争已经从理论走向实战，是最严重的国家安全挑战之一。
——美国总统 奥巴马 美国要扳倒中国，就必须依靠我们在中国内部的盟友和支持者，他们被称为“年轻一代”，或是“互联网一代”。
——美国前驻华大使、下一届总统候选人 洪博培 互联网用户影响着信息主流的形成，每一位用户都有机会向公众发出一条可能改变世界的新闻。
——俄国总统 梅德韦杰夫 互联网可能被用来反对国家利益。
——俄罗斯总理、下一届总统候选人 普京 信息的自由流通可以用来行善，也可以用来作恶。如果有人策划暴力和骚乱，我们会阻止他们通过社交网站进行联络。
——英国首相 卡梅伦 工业时代的“战略战”是核战争，而信息时代的“战略战”就是网络战。
——中国 《南方周末》

<<2020，世界网络大战>>

编辑推荐

《2020,世界网络大战》是网络战争研究专家东鸟力作！
网络空间的国家阴谋与较量。
先发制人的网络威慑，愈演愈烈的网络暗战。
运筹帷幄的网络外交，双重标准的网络自由。
下一个十年，网络大战决定国家命运！
谁控制了互联网，谁就控制了世界！

名人推荐

网络战争已经从理论走向实战，是最严重的国家安全挑战之一。
——美国总统 奥巴马 美国要扳倒中国，就必须依靠我们在中国内部的盟友和支持者，他们被称为“年轻一代”，或是“互联网一代”。
——美国前驻华大使、下一届总统候选人 洪博培 互联网用户影响着信息主流的形成，每一位用户都有机会向公众发出一条可能改变世界的新闻。
——俄国总统 梅德韦杰夫 互联网可能被用来反对国家利益。
——俄罗斯总理、下一届总统候选人 普京 信息的自由流通可以用来行善，也可以用来作恶。如果有人策划暴力和骚乱，我们会阻止他们通过社交网站进行联络。
——英国首相 卡梅伦

<<2020，世界网络大战>>

版权说明