



# 自由与互联网的未来

[澳]朱利安·阿桑奇——著  
Gavroche——译

## CYPHERPUNKS

FREEDOM AND THE FUTURE  
OF THE INTERNET



自由与互联网的  
未来

# 密码朋克

CYPHERPUNKS

[澳] 朱利安·阿桑奇——著

Gavroche——译

中信出版集团·北京

图书在版编目 ( CIP ) 数据

密码朋克: 自由与互联网的未来 / (澳) 朱利安·阿桑奇著, Gavroche 译. -- 北京: 中信出版社, 2017.10

书名原文: Cypherpunks: Freedom and the Future of the Internet

ISBN 978-7-5086-7624-1

I. ①密… II. ①朱… ②G… III. ①密码-加密技术-研究 IV. ①TN918.4

中国版本图书馆CIP数据核字 (2017) 第 108263 号

Cypherpunks: Freedom and the Future of the Internet  
Rights arranged through Peony Literary Agency Limited  
© 2017 Julian Assange. Published by arrangement with OR Books, New York  
Simplified Chinese translation copyright © 2017 by CITIC Press Corporation  
All Rights Reserved.  
本书仅限中国大陆地区发行销售

密码朋克: 自由与互联网的未来

著 者: [澳]朱利安·阿桑奇

译 者: Gavroche

出版发行: 中信出版集团股份有限公司

(北京市朝阳区惠新东街甲4号富盛大厦2座 邮编 100029)

承印者: 北京通州皇家印刷厂

开 本: 880mm×1230mm 1/32

印 张: 8 字 数: 121千字

版 次: 2017年10月第1版

印 次: 2017年10月第1次印刷

京权图字: 01-2017-1513

广告经营许可证: 京朝工商广字第 8087 号

书 号: ISBN 978-7-5086-7624-1

定 价: 42.00元

版权所有·侵权必究

如有印刷、装订问题, 本公司负责调换。

服务热线: 400-600-8099

投稿邮箱: author@citicpub.com

## 什么是密码朋克？

密码朋克提倡通过使用密码术及其类似手段来实现社会和政治改革。<sup>①</sup>该运动形成于 20 世纪 90 年代早期，在 90 年代的“密码战争”（cryptowars）和 2011 年的互联网之春时期最为活跃。“密码朋克”（cypherpunk）这个术语来自“cipher”（密码）和“punk”（朋克），在 2006 年被收入《牛津英语词典》。<sup>②</sup>

---

① 简单地说，密码学（cryptography）这个术语来自希腊语的“密写术”（secret writing），是一种通信编码措施。

② “Oxford English Dictionary Updates Some Entries & Adds New Words;Bada-Bing, Cypherpunk,and Wi-Fi Now in the OED”，载于 ResourceShelf，2006 年 9 月 16 日，<http://web.resourceshelf.com/go/resourceblog/43743>（访问于 2012 年 10 月 24 日）。

## 对密码武器的一个呼吁

本书并非宣言，这已为时太晚。本书是一则警告。

世界已经不是在滑向，而是在奔向一个新型的跨国反乌托邦。这种发展尚未被国家安全领域之外的人正确认知。它被隐藏在秘密、复杂性和小尺度之中。互联网——我们最伟大的解放工具——已经转变成前所未见的极权主义的最危险的推进器。互联网正在威胁人类文明。

这些转变是悄然而至的，因为正在全球监控产业中展开工作的那些人没有说出真相的动机。如果任其在先前轨道上继续发展，数年之内，全球文明将会变成一个后现代

的监控型反乌托邦，除了具备最好技术的那些人，其他所有人都无处可逃。事实上，我们已经置身于此了。

很多作者思考过互联网对全球文明的意义，然而他们错了。他们错了，是因为他们不具备亲身体验而获得的视角和敏感；他们错了，是因为他们从未遭遇敌人。

我们遭遇过敌人。

六年来，维基解密与几乎所有大国作战。我们学会了从一个局内人的视角来观察这种新型监控型国家，因为我们揭露了它的秘密。我们从参战者的视角来看待它，因为我们不得不保护我们的人员、我们的资金以及我们的信息源；我们从全球视角来看待它，因为我们的人员、资产和信息几乎来自所有国家；我们从一个时代的视角来看待它，因为我们已经与之斗争多年，并一次又一次地见证了它的倍增和蔓延。这是一种看不见的寄生虫，从社会中长大，越长越肥，并嵌入了互联网。它正在颠覆这个星球，正在传染每一个国家，甚至每一个人。

我们需要做什么？

过去，在现已不复存在的一个地方，我们，年轻的互联网的建设者和公民们，讨论着新世界的未来。

我们看到，我们的新世界将改善所有人之间的关系，而由人们交流信息、经济和权力的方式定义的国家性质也将被改变。

我们看到，现存的国家结构和互联网的结合将引发国家性质的改变。

首先，要记住，国家是强制性权力在其中流动的系统。国家内的各个派别也许相互竞争以谋求支持，但这只是导致了一种民主的表象，而国家的基础是系统性地运用或规避暴力。土地所有权、财产权、租金、股息、税收、法院罚款、审查、版权以及商标，这一切，都是由国家的暴力威胁来强制执行的。

大多数时候，我们都不会注意到暴力离我们有多近，因为我们所有人都为了免遭暴力而让渡了权利。就像水手嗅到微风，我们很少思考我们眼前的世界是如何被表面之下的黑暗支撑起来的。

在互联网的新空间中，强制性权力的调节器将是什么？

提出这样一个问题真的有意义吗？在这个非现实的空间里，在这个理念和信息似乎自由流动的柏拉图国度里，也会存在强制性权力的概念吗？一种能够修改历史的权力，

一种能够窃听电话的权力，一种能够分裂人民的权力，一种能够将复杂性分解并筑起高墙的权力，就像一支占领军一样的权力？

互联网的柏拉图本性，即理念和信息的流动，被它的物质起源玷污了。互联网的基础是跨越大洋海底的光缆，是在我们头上旋转的卫星，是安置在从纽约到内罗毕的城市建筑物中的计算机服务器。就像用三尺之剑杀死阿基米德的士兵，同样，一个武装的民兵也能威胁西方文明发展的巅峰、我们的柏拉图国度。

互联网的新世界，从粗暴的原子构成的旧世界脱胎而出，渴望着独立。但是，国家及其盟友行动起来，通过控制互联网的物质基础，夺取了对我们新世界的控制权。国家，就像油井周围的一支军队，或者边界上的关税代理人，向我们索取贿赂，他们将很快学会利用其对物质空间的控制，夺取对我们柏拉图国度的控制，这将阻碍我们梦寐以求的独立。进而，通过控制光纤线路、绕地卫星和地面接收站，大规模拦截我们新世界的信息流——这个新世界的本质——即便每个人、每一种经济和政治关系都欢迎这个新世界。国家将渗入我们新社会的经脉，吞噬每一种表达



和交流的关系，吞没人们阅读的每一个网页、发送的每一条信息以及搜索的每一个概念，每天拦截数十亿条信息，然后将这些权力梦寐以求的信息，永久地存储在一个巨大的机密仓库里。再然后，国家会一次又一次开采这些宝藏、这些搜集到的人类个体的智力创造，利用前所未有的复杂搜索和模式发现算法，充实这些宝藏，将拦截者与被拦截的世界之间的不平衡不断扩大。最后，国家会将他们从中所学到的运用到现实世界，去发动战争，去发动无人机攻击，去操纵贸易和联合国的委员会，去为产业界、局内人和朋党亲信的巨大关系网牟利。

但是，我们发现了一个工具，我们抵抗全面统治的一个希望，一个结合勇气、洞见和团结的希望，让我们可以利用它来进行抵抗。一项来自我们所生活的物质宇宙的奇异的属性。

宇宙相信加密。

加密容易，解解难。

我们发现，我们可以利用这项属性去创建新世界的法律。让我们的新柏拉图国度从它的卫星、海底电缆和控制器中脱身而出。让我们的空间在密码之幕背后得以加固。

让我们创造一片新的国土，将那些物质现实的控制者阻拦在外；为了跟随我们，进入我们的领土，他们将耗尽无穷资源。

以这种方式，我们宣示独立。

曼哈顿计划的科学家们发现，宇宙允许原子弹的制造。这并非一个显而易见的结论。核武器也许并不属于物理定律的范畴。然而，宇宙相信原子弹和核反应堆。它们是宇宙所赐福的现象，就像盐、海洋或星辰。

与之类似，我们这个物理宇宙的一种属性，使得个人或团体能够可靠地、自动地对事物进行加密，即便是地球上最强大的超级霸权以最强烈的政治意愿动用所有的资源，也无法解密。人们之间的加密通道能够联结在一起，创造出免受外在国家强制性力量干扰的区域，免于大规模拦截，免于国家控制。

通过这种方式，人们可以用自己的意志反抗一个充分动员的超级霸权的意志，并且赢得胜利。加密的是这种物理定律的一个体现，它不听从国家的咆哮，甚至也不听从于跨国监控型反乌托邦。

世界必须如此运作，这并非显而易见。但宇宙以某种

方式向加密微笑。

密码术是非暴力直接行动的终极形式。

有核国家可以对数百万人施加无限暴力，然而强大的密码术意味着一个国家——即便是能够施加无限暴力的国家——也无法打破个人保守秘密的意志。

强大的密码术能够抵抗无限施加的暴力。任何暴力都无法解决一道数学问题。

但是，我们能否利用关于世界的这个奇异事实，将它建造成互联网的柏拉图国度的基石，使人类在此得到独立和解放？随着社会与互联网的融合，这种自由能否反作用于物理现实，从而重新定义国家？

我们要记住，国家是决定强制性权力如何持久运用，以及用在何处的系统。

这种强制性权力能够在多大程度上从物理世界渗透到互联网的柏拉图国度，这个问题将由密码术和赛博朋克的理想来解答。

随着国家与互联网的融合，我们文明的未来将成为互联网的未来，我们必须重新定义权力关系。

如果我们不这么做，互联网的普世性将让全球人类逐

渐消失在一个大规模监控的天罗地网中。

我们必须发出警告。本书就是守夜人在黑夜中的一声呐喊。

2012年3月20日，在等待引渡的软禁中，我在英国与三位朋友，也是志同道合的守夜人同伴会面，或许我们的齐声呐喊能够唤醒这座城镇。我们必须就我们所知交换意见，而这也给予你——读者——一个机会，去理解正在发生的事，并对此采取行动。

是时候了，拿起我们新世界的武器，为我们自己，为我们所爱之人而战。

我们的任务是在可能的地方争取自决，在不可能的地方阻止乌托邦的到来，如果这些都失败了，那就去加速它的自我毁灭。

朱利安·阿桑奇

2012年10月于伦敦

## 讨论参与者

朱利安·阿桑奇 ( Julian Assange )，维基解密<sup>1</sup>的主编和创始人。作为密码朋克邮件列表的最初贡献者，朱利安·阿桑奇是当今世界最著名的密码朋克哲学倡导者之一。他通过维基解密所做的工作为密码朋克的传统信条“弱者要隐私，强者要透明” ( Privacy for the weak, transparency for the powerful ) 增添了政治砝码。尽管他最耀眼的工作是对言论自由的强力实践和推动权力机构的透明和问责，但他同时也是对国家和公司侵犯个人隐私的尖锐抨击者。阿桑奇创建了众多遵循密码朋克哲学的软件项目，包

括最早的TCP/IP端口扫描器strobe.c，可拒绝加密文件系统rubberhose，以及维基解密的原始代码。<sup>2</sup>阿桑奇少年时代就已是一名早期的计算机和网络安全研究员，那时，某些黑客行为还没有被法律认定为犯罪活动。之后的（20世纪）90年代，他成为澳大利亚的活动家和互联网服务提供商，同时还与赛利特·德累福斯（Sulette Dreyfus）合著了关于国际黑客运动历史的《地下》（*Underground*）<sup>①</sup>一书，电影《地下：朱利安·阿桑奇的故事》（*Underground: The Julian Assange Story*）据此改编。<sup>3</sup>

雅各布·阿佩尔鲍姆（Jacob Appelbaum），位于旧金山的创客空间“噪声桥”（Noisebridge）的创办者，柏林混沌计算机俱乐部（Chaos Computer Club，CCC）的成员和开发者之一。<sup>4</sup>雅各布还是Tor项目的推广者和研究员，这是一个旨在帮助所有人抵抗监控和规避互联网审查的匿名上网系统。<sup>5</sup>过去十年，他的主要活动是推动环境保护和人权运动。为了这个目标，他已经在从计算机取证到医用大麻的多个领域发表了有关新型安全、隐私和匿名的研究。

---

① 中译本名为《维基大战前传I：阿桑奇和他的黑客战友》（世界图书出版公司，2011年出版）。

雅各布相信毫无例外每个人都有自由阅读和自由发言的权利。2010年，当朱利安·阿桑奇无法到纽约发表一个讲话时，雅各布代其发言。从此以后，他以及他的朋友和家人便遭到美国政府的骚扰：在机场遭受执法官员的盘问、侵犯性搜身，并被暗中威胁即将遭受监狱强奸，他的设备被没收，他的在线服务项目受到秘密传讯。这些措施没能让雅各布屈服，他继续进行法律斗争，同时仍是言论自由的公开倡导者和维基解密的积极支持者。

**安迪·米勒-马贡 (Andy Müller-Maguhn)**，是位于德国的混沌计算机俱乐部的长期成员、前董事会成员兼发言人。<sup>6</sup>他是欧洲数字权利组织 (EDRI) 的联合创始人之一，这是一家旨在加强数字时代人权的非营利性组织。<sup>7</sup>2000年到2003年，他被欧洲互联网用户推选为互联网名称与数字地址分配机构 (ICANN) 的欧洲地区总监，该机构负责为全世界互联网的“名字和数字”运行制定政策。<sup>8</sup>他还是一位电信和其他类型监控方面的专家，通过他的维基项目 [buggedplanet.info](http://buggedplanet.info)<sup>9</sup> 对监控产业进行专业调查。安迪在密码通信领域展开工作，并与其他人共同创办了加密电话 (Cryptophone) 公司，该公司向商业客户销售安全语音通信

设备，并在网络架构环境中提供战略咨询服务。<sup>10</sup>

热雷米·齐默尔曼 ( Jérémie Zimmermann )，公民诉求团体 La Quadrature du Net 的联合创始人和发言人，该组织是欧洲地区捍卫在线匿名权的最著名的组织，同时也致力于促进人民对互联网自由的管制和攻击的认识。<sup>11</sup> 热雷米致力于为公众参与公共辩论以及推动改革开发工具。他投身于版权战争 ( copyright wars )，这场论战围绕网络中立性和其他对自由互联网的将来有关键影响的监管议题展开。最近，他的组织 La Quadrature du Net 在欧洲政治中取得了一项历史性胜利，他们召集的公众运动在欧洲议会上成功击败了《反假冒贸易协定》( ACTA )。参与作为本书基础材料的讨论后不久，热雷米在离开美国时遭到两名 FBI ( 美国联邦调查局 ) 官员的阻拦，并被盘问与维基解密有关的问题。

## 注 释

1. 维基解密：<http://wikileaks.org>。

2. 更多关于 rubberhose 文件的信息，参见赛利特·德雷福斯：“The Idiot Savants’ Guide to Rubberhose”，<http://marutukku.org/>



current/src/doc/maruguide/t1.html (访问于 2012 年 10 月 14 日)。

3. 更多关于图书《地下》的信息, 参见: <http://www.under-ground-book.net>; 更多关于电影《地下: 朱利安·阿桑奇的故事》的信息, 参见: Internet Movie Database: <http://www.imdb.com/title/tt2357453/> (访问于 2012 年 10 月 21 日)。

4. “噪声桥”是一个位于旧金山的黑客空间, 为技术创意产品提供基础设施, 由其成员联合运营: <https://www.noisebridge.net/wiki/Noisebridge>; 柏林混沌计算机俱乐部是混沌计算机俱乐部的柏林分支机构, 参见: [https://berlin.ccc.de/wiki/Chaos\\_Computer\\_Club\\_Berlin](https://berlin.ccc.de/wiki/Chaos_Computer_Club_Berlin)。

5. Tor 项目: <https://www.torproject.org>。

6. 混沌计算机俱乐部是欧洲最大的黑客协会, 其活动包括技术研究和开发、政治竞选运动、集会活动、出版活动以及政策建议: <http://www.ccc.de>。

7. 欧洲数字权利组织: <http://www.edri.org>。

8. 互联网名称与数字地址分配机构 (ICANN): <http://www.icann.org>。

9. 窃听行星 (buggedplanet): <http://buggedplanet.info>。

10. 加密电话: <http://www.cryptophone.de>。

11. La Quadrature du Net: <http://www.laquadrature.net>。