暗网的真相

暗网的初衷是保护异见人士，但它同时也掩盖了诸多非法活动

阿迪蒂·库马尔、埃里克·罗森巴赫

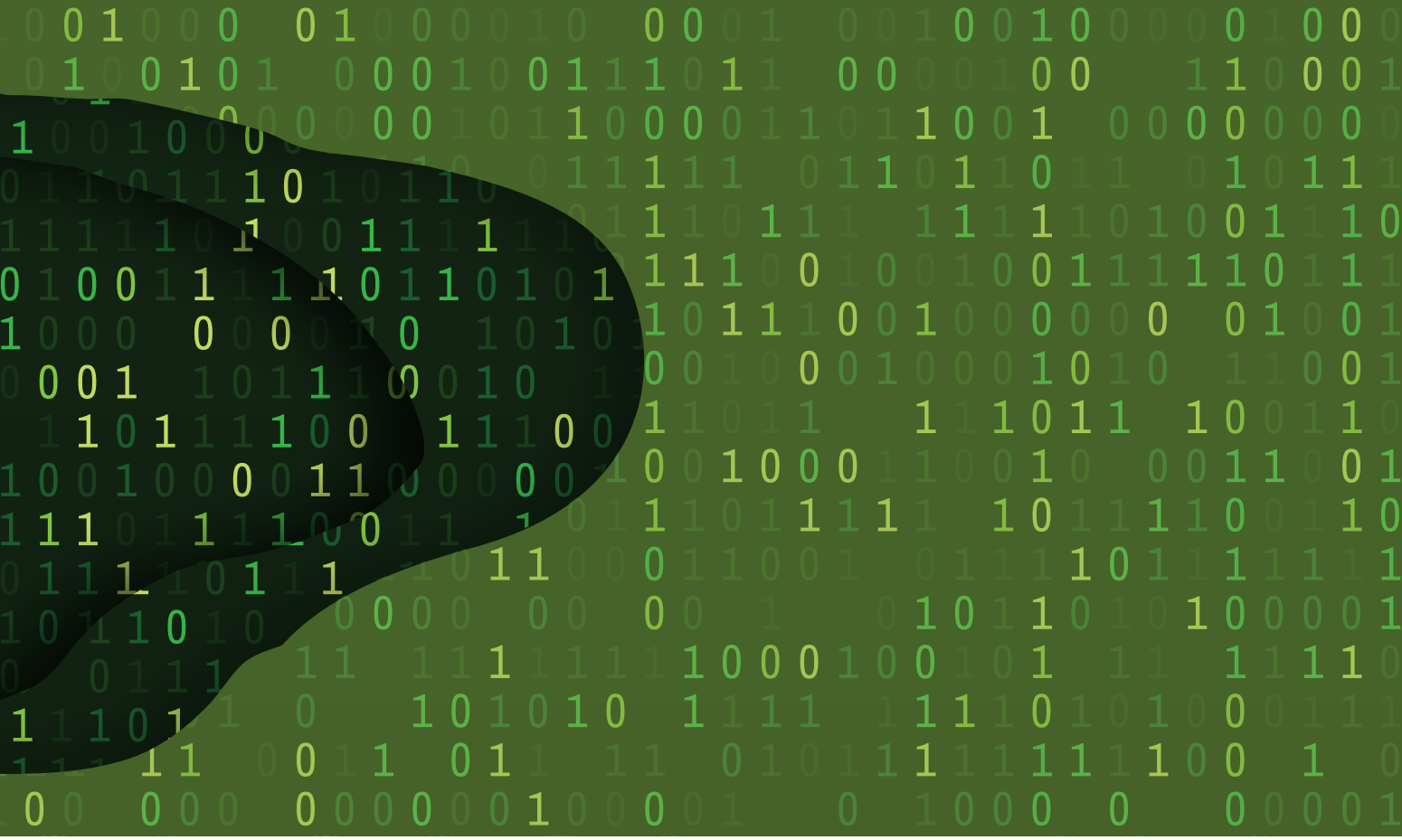
20 世纪 90 年代末期，美国国防部的两家研究机构开发了一种匿名的加密网络，以保护美国间谍在交流时收发的敏感信息。普通的互联网用户无法知晓或访问这个秘密网络。尽管我们没办法充分理解这其中不可告人的初衷，但有些研究人员却从中发现了不同的价值主张——组建非营利组织，专注于以匿名形式保护人权和隐私活动。

考虑到保护流动信息的多层加密，需要登录 Tor（全称“洋葱路由”）网络。Tor 处于互联网的边缘，是暗网的底层技术。这里的暗网是指普通浏览器无法访问、谷歌等搜索引擎无法索引的一些隐秘网站。要解开网络中这个专注于隐私的秘密角落，唯一的方法是免费下载 Tor 浏览器。然而，完全匿名会产生长远的影响。

事实上，暗网除了能高度保护隐私，以摆脱独裁政府的监视之外，还催生了一个日益庞大的地下市场，在那里，惯犯可以进行贩毒、盗用身份、儿童色情以及提供非法产品和服务等犯罪活动。由于无法追踪的加密货币是主要的支付方式，要想加强对犯罪活动的管控，全球执法机关、金融机构和监管机关需要紧密合作。

灰色地带

如今，Tor 网络上存在 65000 多个以 .onion 结尾的独特的 URL（统一资源定位符）。2018 年，计算机安全公司 Hyperion Gray 开展了一项研究，对其中 10% 的网址进行了编目，发现其中最常见的功能都是通过论坛、聊天室、文件和图贴（image hosts），以及依托市场的商务活动来推动的。这些功能性角色——尤其是与交流有关的角色——在自由社会中有诸多合理且合法的用途。而且，2016 年，一家名为 Terbium Labs 的研究公司在其研究中



对随机选择的 400 个 .onion 网址进行了分析。这项研究表明，暗网中超过一半的网址都是合法的。

对于生活在压制性政权下的普通民众而言，由于这一政权屏蔽了许多互联网网址，或迫害持不同政见者，因此暗网便成为他们的一丝希望，让他们能够获得信息并免遭迫害。在更为自由的社会，暗网可能是重要的举报和沟通工具，使人们在职场或社区不会遭到惩罚或评判。或者，对于那些担心企业和政府跟踪、使用并有可能买卖个人数据的人而言，暗网能够确保隐私和匿名性。如今，许多组织在 Tor 都有隐藏的网址，比如几乎所有的主流报刊机构、脸书，甚至美国中情局 (CIA)。这是因为 Tor 网站体现了对隐私的尊重，虽然有时只是象征性的。例如，《纽约时报》和中情局都希望更加有效地推动与虚拟的且能提供敏感信息的不速之客之间的交流。

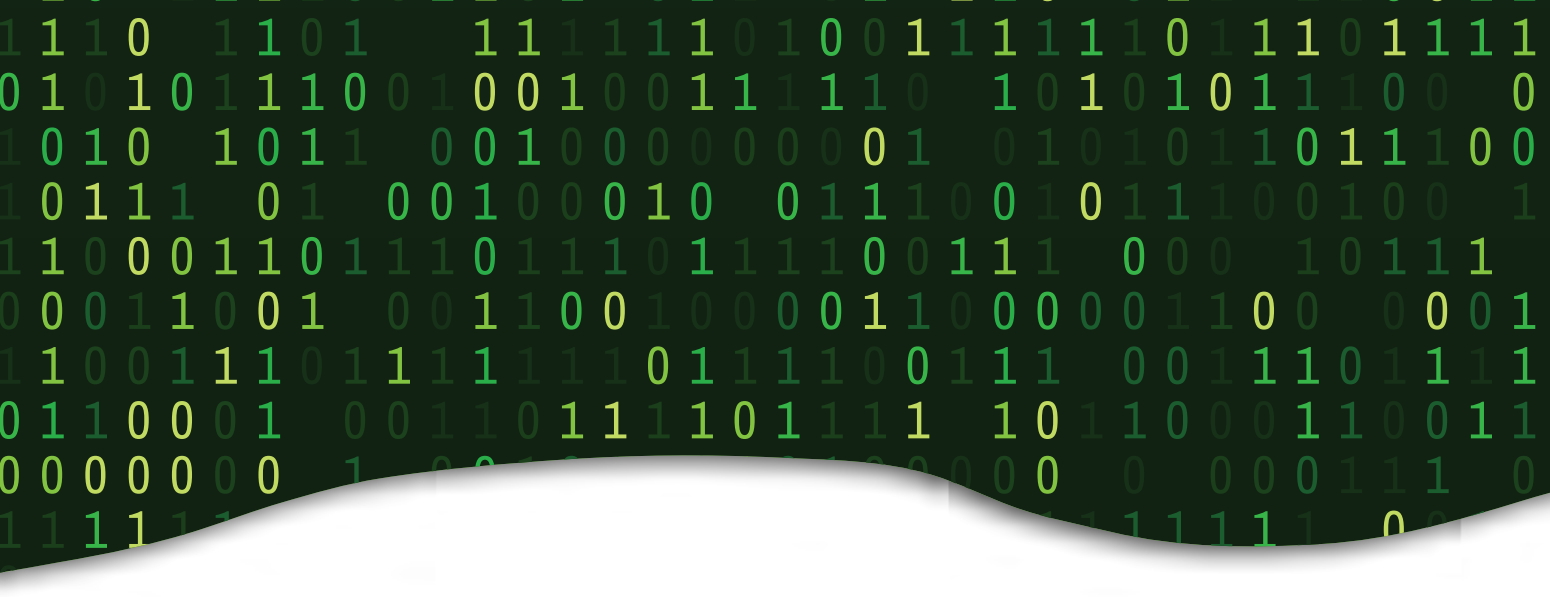
另一方面，隐私和匿名性可保护人们不受暴政和精准广告的影响，这也使得暗网成为犯罪的跳板。一些比较普遍的非法活动包括武器走私、毒品交易、剥削性内容的分享，而且经常会涉及儿童，例如色情和暴力图片以及其他虐待儿童的事件。这些网站还支持新纳粹分子、白人至上主义者及其他极端团体的言论。

对于生活在压制性政权下的普通民众而言，由于这一政权屏蔽了许多互联网网址，或迫害持不同政见者，因此暗网便成为他们的一丝希望。

一旦暗网服务与虚拟货币勾结起来，预计犯罪活动将大幅增加。十年前，一位化名中本聪的密码学专家（他在破解密码方面很有一套）开发了世界上首个不受国家政府监管的货币和支付网络：比特币。最初，比特币仅是科技界内使用的交换媒介。2011 年，比特币成为在“丝绸之路”这个暗网上从事非法交易的毒品贩子使用的货币。过去五年间，那些隐藏在大多数人视线之外的加密网络与执法官员几乎无法追踪的交易货币相互勾连，最终形成了一个规模小但影响大的市场——非法商人销售非法商品的市场。

在 Terbium Labs 列明的近 200 个非法域名中，75% 以上是交易市场。在比特币和其他加密货币

设计：ISTOCK/TETIANALAZUNOVA



当今社会所面临的诸多破坏性威胁均受到Tor网络的保护，国际监管机构、金融机构和执法机关应给予关注。

（例如，门罗币）的推动下，这类市场快速发展。娱乐和医药是最受欢迎的产品，其次是盗用或欺诈性身份文件，例如身份证、信用卡和银行资信证明，有些网站还提供黑客和技术犯罪服务，包括恶意软件、分布式阻断服务攻击以及雇用黑客。除了这类产品外，很多此类网站还出售其他产品，包括色情和假冒商品。

尽管在暗网上进行的非法交易迅速增长且有具有相当的严重性，应引起各国政府和全球金融机构的关注，但与全球非法商业活动相比，在暗网上交易的商品总量仍微不足道。世界领先的密币支付分析公司 Chainalysis 最近提交的一份报告显示，暗网上的比特币交易从 2012 年的大约 2.5 亿美元增至 2018 年的 8.72 亿美元。该公司预测，暗网上的比特币交易将在 2019 年超过 10 亿美元。如果该预测正确的话，则表明该领域的非法交易将达到历史新高。这份报告同时指出，非法比特币交易的占比一直在下滑，2012 年为 6%，而如今的比例不足所有比特币交易的 1%。更广泛地讲，据联合国估计，全球每年的洗钱金额占全球 GDP 的 2%—5%，介于 1.6 万亿美元至 4 万亿美元之间。

尽管从经济体量而言，非法的暗网活动规模仍相对较小，但是，当今社会所面临的诸多破坏性威胁均受到 Tor 网络的保护，这亟需引起国际监管机构、金融机构和执法机关的关注。

暗网监管

在保护持不同政见者、隐私提倡者及举报者的同时，不应纵容虐童者、武器贩卖者和毒枭。这给监管机构和执法机关带来了挑战：制定双管齐下的方法迫在眉睫，既能在信息管控时代保护自由主义原则，同时能发现并根除暗网上最隐秘的活动。过去几年间，国际社会通过完善信息共享、提高执法机关打击主要非法市场的技术能力以及规范加密货币交易的转移，在应对这些挑战方面取得了重大的进展。

要打击暗网上那些最邪恶的活动，首先要加强执法机关与金融机构之间的信息共享。暗网的全球性使得国际合作势在必行。2018—2019 年，国际刑警组织和欧盟联合 12 个国家的执法机关，锁定了 247 个重要的嫌疑目标，并共享了执法所必要的运营情报。此举的成果令人期待：就在今年，该团队的成员成功逮捕了犯罪嫌疑人，并关闭了 50 个非法暗网网址，包括全球最大的两个贩毒市场——华尔街和瓦尔哈拉。

非法暗网交易的蔓延也促使世界各国政府积极加强国内执法部门——例如，美国联邦调查局（FBI）——的能力，努力打击各类犯罪活动。例如，据报告，FBI 开展了一系列行动，使 Tor 服务器“去匿名化”。FBI 在网络上建立节点，借此来发现非法 Tor 网页的网络号和位置。FBI 第一项重大行动就是捣毁“丝绸之路 2.0”（Silk Road 2.0）网站，这是 2014 年上线的最具影响力的非法暗网市场之一。FBI 的调查显示，在该网站非法运营的两年半中，几千名毒品贩子和其他非法商人通过该网站向 10 万多名客户出售了数百公斤的毒品和其他非法商品及服务。该网站还被用来进行洗钱，从这些非法交易中获得的黑钱达数亿美元。总之，按比特币计算，该网站当时的总销售收入超过了 9500 万美元，约合 12 亿美元。继“丝绸之路”后，2017 年两个最大的市场——AlphaBay 和 Hansa——被成功捣毁。

针对暗网的执法能力正在不断增强。近期，在荷兰的一次执法行动中，执法人员对一家知名的暗网商户匿名追踪了一个月，最后将其成功取缔，接着又利用所收集的信息取缔了其他几十个暗网商户。

建设新的法规势在必行

除了开展打击行动外，各国政府和国际机构正在设法对那些助长暗网市场的加密货币进行直接监管。例如，2019 年 6 月，金融行动特别工作组发布了一份指南，敦促为客户办理加密货币转账的公司要识别转出方和转入方。这份指南主要遵循 2018 年 G20 峰会提出的建议。在 G20 峰会上，与会领导人要求国际监管机构在政策层面对加密资产采取应对措施，尤其是与了解客户、反洗钱和打击恐怖主义融资有关的政策。由兑换、电子钱包和其他加密支付助推因素组成的初创生态系统缺乏必要的基础设施来落实类似金融行业的标准，但监管机构需要着手为强化审查做一些准备。脸书即将上线的加密货币 Libra 只会使这项工作变得更加紧迫，毕竟对 20 多亿的脸书用户而言，使用虚拟资产的门槛将进一步降低。

界限分明

独裁政权将继续屏蔽暗网，并防止暗网因支持异见人士和活跃分子而对合法性产生威胁。面对这种威胁，自由公民社会的自然反应将是主张 Tor 不受监管和管制，以保护言论自由与个人隐私。但暗网的实际情况要复杂得多，这要求监管部门和执法机关采取全新的方法，以挫败那些在自由社会中被视为非法和不道德的活动，同时保护匿名网络的真正利益。FD

阿迪蒂·库马尔（ADITI KUMAR）是哈佛大学约翰·F.肯尼迪政府学院贝尔福科学与国际事务中心执行主任。**埃里克·罗森巴克**（ERIC ROSENBACH）是贝尔福中心的联合主任，前美国国际安全事务国防助理秘书。