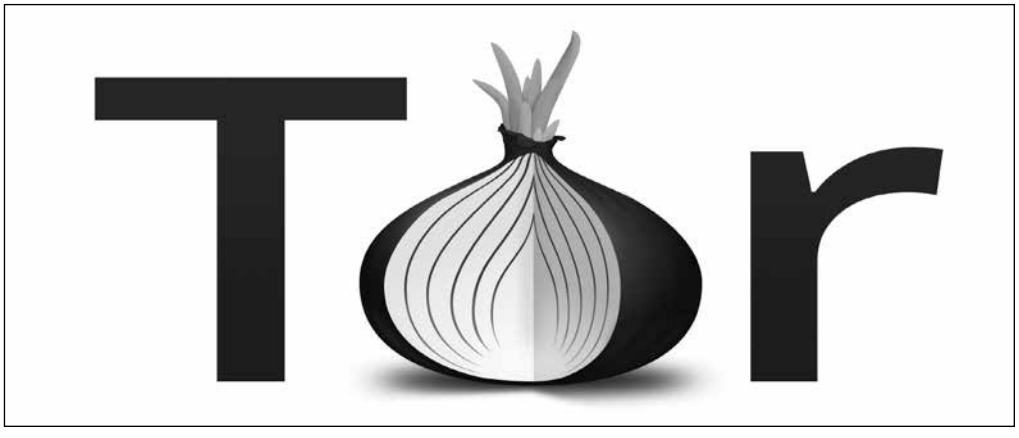
初探暗网
Dark Web 101

杰明·科尔，美国空军少校（Major Jeremy Cole, USAF）



当今互联网有多种网络。首先是明网（surface web），它由谷歌和其它搜索引擎可索引的网站组成，在其中通过各种链接开展索引和查询。本质上，明网就是公开可用索引的总索引网，基于搜索条件和链接来提供搜索结果。明网规模很小，仅占 4%。第二种网络称为深网（deep web），约占 96%，亦即互联网的其余空间。它的组成包括要求用户输入验证数据才能进入的受保护网站（例如电子信箱或网上银行）、未设链接的内容（例如未发表的博客或机构数据库）、专属数据（例如研究成果、财务报告、研发资料），以及个人信息（例如病历档案或法律文件）。这些都属于深网，标准的搜索引擎无法进入这些网站，因此无法搜索。最后一种网络称为暗网（dark web），它是深网的一部分。暗网需要专门的软件、登录名和知识才能进入，那些喜欢躲在暗处的隐蔽网站都在这里安家。

ISP = 互联网服务提供商
IP = 互联网协议

黑客、政府调查机构、欧洲刑警组织、向记者提供消息的匿名来源、言论自由受压制国家的异议人士、毒品交易者、恋童癖者、受雇职业杀手、内部揭发者、隐私窥探狂热者，他们的共同之处是什么？他们都依靠网上匿名获得保护，或为确保隐私和保护个人信息，或为表达言论自由，或为开展与言论自由相悖的言论审查。此外，他们还依靠网上匿名从事非法活动。无论是交流通信，浏览网站，还是托管数据，这些个人和组织都在暗网中从事他们的活动，隐藏在公众视野之外。暗网是什么，它如何运作，主要哪些人在使用，了解这些至关重要，因为暗网代表着由来自社会各方面很多不同性格人物组成的隐藏服务的混合体。

暗网是什么?

有些人称暗网是“互联网肚脐以下见不得人的下腹部，人们在这里能购买毒品、武器、儿童色情，以及雇凶杀人。”[1] 也有人强调其

如何“帮助政治异议人士逃避政府审查。”[2] 无论是哪种情况，暗网是那些难见真容的网站的集聚地，因为暗网“不能够被诸如谷歌等搜索引擎索引，也不容易被标准的网络浏览器找到。”[3] 简要概述一下暗网的技术发展和演变，可为本讨论做出界定。在一般意义上，暗网，亦称黑网，就是让有些人通过互联网交流通信、托管数据，或访问特定的网站，而把他们的这些网上活动遮掩起来。传统上来讲，互联网的使用，取决于互联网服务提供商（ISP）把其用户跟互联网连接。ISP 给其用户和数据宿主分配互联网协议（IP）地址。IP 地址中包含关于 ISP、其地理位置、最近的城市、访问的网站，以及其他确认身份的信息，这称为元数据。暗网能让其用户和数据宿主匿名浏览互联网，托管一个网站，或使用某个隐蔽其用户 IP 地址的全球网络进行通信。这种匿名技术来自美国海军研究实验室（NRL）研发的一套软件。在 2004 年，NRL 发布了第二代“洋葱路由器”，即人们常说的“Tor”。同年 5 月，Tor 有“32 个节点，24 个在美国，8 个在欧洲。”[4] 今天的 Tor 网络超过 6000 个节点，使其成为国际上最大的用于进入暗网的首选工具。[5]

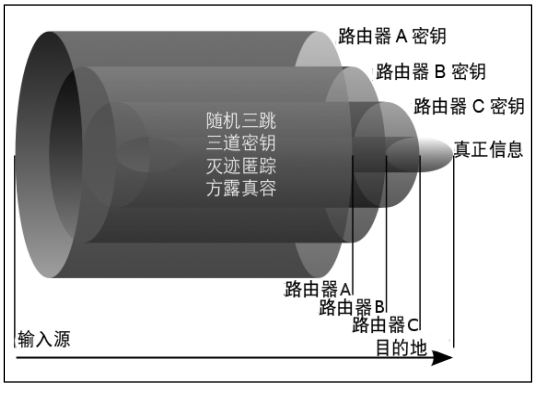
被称为“Tor”的洋葱路由技术为暗网用户匿名曾经发挥过好处，但此后暗网逐步向其他更多用途发展，有些合法，有些非法。Tor 的原始研发者之一迈克尔·里德（Michael Reed）说，Tor 最初用于合法目的，“其‘目的’是供美国国防部和情报部门使用……不是帮助异议人士……和罪犯（或者）‘比特洪流’（bit-torrent）用户……。”[6] 但是，在第二代 Tor 启用 9 年后，使用 Tor 的卢森堡大学研究者评估了近 4 万个隐藏的 Tor 网站。简言之，他们“发现 Tor 隐秘服务的内容非常多样。提供非法内容或专门用于非法活动的隐藏服务的数量，几乎同其他性质的隐藏服务（致力于人权、言论自由、匿名、安全等）的数量相等。”[7] 有趣的是，他们的分析发现，合法的网站（56%）和非法的网站（44%）在数字上几乎是各占一半。[8] 鉴于 Tor 节点在全球的覆盖面如此之广，可以公平地断言，暗网中的内容并非都是坏的。美国政府 2013 年对 Tor 投资大约 180 万美元。[9] 此外，Tor 现在是“由志愿者管理，由活动人士、非营利组织、大学和政府支持的开源项目。”[10] 所有这些因素表明，Tor 和其所寄居的暗网，可能并非像此前人们所认为的完全充斥着犯罪和非法活动。尽管人们的看法不尽相同，暗网的存在让个人，不管他们的意图为何，能够匿名地交流，托管数据或浏览网站。当然，暗网及其所使用的工具已演变到包括范围广泛的各种活动，但始终以匿名为重。

暗网如何运作?

暗网使用加密技术和匿名软件来保护其用户和数据宿主。暗网用户使用加密工具并非鲜见。例如，恐怖组织伊拉克和黎凡特伊斯兰国（ISIL）据报早在 2013 年 11 月就开始实验使用加密工具。[11] 两年后，新的报道说，ISIL 现在拥有一个“全天候的‘服务台’，向不断壮大的圣战者提供加密通信咨询，以便逃避当局的监控”。[12] 关于 ISIL 加密技术细节的公开源报道很少，尤其是涉及到攻击策划。例如，起初人们认为，ISIL 使用加密技术策划了巴黎攻击事件。但是后来的情报证实，所谓 ISIL 使用 PlayStation4 游戏主机加密其行动策划的报道有误。[13] 目前尚无公开信息表明，2015 年 12 月初在美国加州圣贝纳迪诺发生的一起 ISIL 思潮煽动下的攻击事件，在策划中使用了加密手段。[14] 但是，据美国陆军属下打击恐怖主义中心的亚伦 F·布

兰特利（Aaron F. Brantly）说，至少有“120 个不同的(通信)平台,其中很多经过加密……建立一个空间……能不受直接监视地运行。”[15] 虽然这些突出的消极案例可能让人们失望，但是加密技术对保护现今在网上做的各种事情——从支付有线电视帐单，到管理个人财务，浏览喜欢的网站，在社交媒体上发表评论，分享自己认为重要的看法，欣赏在线音乐，等等——有着功大于过的价值，由于加密对于保护个人网上信息，对于只允许授权者访问而言必不可少，匿名软件将继续依靠加密技术。

总体而言，暗网通过加密技术和匿名软件相结合，来隐蔽其用户和数据宿主。虽然互联网中还有其他的选择，如虚拟私用网（VPN）、同行网（P2P）、隐形互联网项目（I2P）等，但 Tor 是暗网中最常用的匿名软件。[16] 用匿名软件来隐藏身份的技术有很多，例如，Tor 以“多层加密网络交通遮掩‘你上网去哪里’过程，并穿过从全球计算机节点（上述提到的 6000 多个可用节点）中随机选取的几个，每经过一个节点像剥洋葱一样剥去一层加密，然后将数据传递给或者说跳跃到网络中的下一个节点。”[17] 这个被称为“跳传”的数据传递过程，把 Tor 用户和数据宿主的私人信息经由随机选取的三个节点传递而使



其 IP 地址隐藏起来，使人很难辨识源头。[18] 在通过 Tor 运行一个网站时，用户的 IP 和网络服务器连跳三次，而 VPN 仅跳一次。[19] 另外一种被称为欺骗的常用技术，让你的 IP 看上去是在其他什么地方。[20] 这很适用于访问那些按照 IP 地址只能在特定物理位置范围才可看到的特定网上资源（电视节目、购物、新闻等）。例如，使用 VPN，人们能进入设在美国的 Netflix 电子影视读物公司，而用户本人则可能住在意大利，使用意大利的互联网服务供应商。VPN 让客户选择世界多个国家的 IP，让他们能匿名读取网上的资源。VPN 由于“免费而且通常比经过 Tor 网络浏览速度更快，更容易使用而受到欢迎。”[21] 匿名软件和加密，向用户和数据宿主提供安全隐藏其真实身份的能力。由于加密能确保只有经过授权才能访问特定的数据，暗网用户依赖加密。如果同能隐藏身份的 Tor 或 VPN 等软件一起使用，能大幅增加保持匿名的程度，因此更能保护用户或数据宿主的身份。

谁使用暗网

这个问题很微妙，因为大多数暗网用户选择匿名，你不知道他们是谁。但是，考虑到互联网用户的数量，可用网站的数量，暗网用户浏览什么，怎么浏览，等等，我们可以知道，暗网使用人数极少，目的也五花八门。例如，全球互联网目前每天用户超过 32 亿，而 Tor 的用户据称仅为 200 万。[22-23] 假设 Tor 的这个数据是准确的，这就等于有 0.0625% 的互联网用户在使用 Tor。那种认为 200 万用户使用 Tor 进入暗网的目的，不外乎贩毒或浏览儿童色情的推论，是无识之见。来自 Tor 的数字称，“在所有流量中……仅有 1.5% 跟隐蔽网站有关。”[24] 互联网上大约有近 10 亿个网站。[25] Tor 估计，暗网数量

在 7000 到 30000 之间。[26] 换言之，Tor 的暗网约占全部网站的 0.003%。[27] 这些数据表明，暗网用户、数据宿主和可用数据组成的群体很小。根据 Tor 项目的说法，这个群体包括极力想保护自身的“一般人”，其中有“不择手段躲避的营销商和偷盗身份的窃贼、无国界记者、美国之音 / 自由欧洲 / 自由亚洲电台、中国的公民记者、执法人员、揭发者、企业高管、博客作者、军方的外勤特工、秘密特工部门、情报部门，等等。”[28] 于是可以想象，这些人通过 Tor 匿名工具使用暗网来隐藏自己的网上踪迹。暗网中还有一些 Tor 项目没有提及的其他使用者，例如，两年前，某人设立了一个暗杀服务市场，以比特币作为支付货币，接单暗杀政治人物。[29] 另一个例子是黑客推销网上黑道服务，这其中颇有些讽刺，因为“为了建立商业关系，黑客必须礼貌待客，及时完成每一单秘密任务，在某些情况甚至要提供退款保证。”[30] 另一方面，还有一些黑客义士，例如一位被称为“Intangir”的黑客，“他在 2014 年侵入暗黑维基网站，删除了所有儿童色情网站的链接，使他成为暗亦有道的暗网捍卫者。”[31] 再一个例子是 X 医生，他是一名训练有素的内科医生，有志帮助人们减少对毒品的依赖，于是设立了一个网站，帮助毒品市场上的使用者。他说，“人们向我询问各种不同药物混合的真正危险和副作用（非法的和处方的），以及糖尿病或神经疾病患者等不同身体状况的人如何使用相关药物。”[32] 这些利他行为提供了人的尊严能存在于匿名之中的希望。

鉴于暗网用户和网上提供的服务数量很少，通过审视热门浏览内容来获取统计数据和了解暗网用户，得到的调研结果各各不同。例如，互联网观察基金（IWF）的报告发现，“31,266 个 URL（统一资源定位符或网上资源链接）含有儿童色情图片。”[33] IWF 称，其中，“在 2014 年，我们确认出 51 个此前未曾发现的隐蔽服务，散布儿童性虐待内容，比 2013 年增长 55%。”[34] 这些隐蔽的非法内容，仅占 0.002%，更令人不安的，是这些隐秘服务的使用者在增长，推动着儿童色情市场的发展。这意味着通过暗网提供儿童色情服务的团伙在增加。再举第二个例子，可了解暗网中毒品商贩的习惯。2014 年 11 月，17 个国家的司法当局在一次代号为“署名行动”的合作中，对暗网中的毒品市场进行打击。[35] 这次行动逮捕了 17 人，吊销了（Tor 托管的）414 个“.onion”（洋葱）域名，“没收了超过 100 万比特币（网上使用的数字货币，没有任何合法银行机构参与），和 25 万美元现金，”并查封了其他资产和多个网上毒品市场。[36] 这次行动获得成功，但是继“暗网中最受欢迎的毒品网站‘丝绸之路’被查封”，又有其他网站取而代之。[37] 像 Agora 之类的网站应运而生，提供“超过 16,000 种大部分为非法的产品。”[38] 在 6 个月后，2015 年 4 月 24 日的数字证实，暗网中较小规模的毒品网站“在过去一个月出现了大幅度的增长。”[39] 似乎，由于“丝绸之路”被取缔出现的真空，反而促使毒品市场事实上得以扩展。这种现象意味着，毒品市场在“署名行动”后继续生存，甚至扩大了在暗网中的存在。耐人寻味的是，暗网中的毒品大网站 Agora，最近因担心“Tor 的隐蔽服务中含有可能致使其服务器被发现的漏洞，”因而关闭了网站运作。[40] 基于这些例子，以及此前提及的卢森堡大学研究的结论，我们可以认定，暗网群体很小，仍在继续推进非法活动；尽管执法机构不断打击，暗网群体依靠最新的技术趋势，尽各种努力保持隐身保护自己。

暗网的手段各异，要辨识出暗网的用户或数据宿主相当困难。例如，英国朴茨茅斯大学教授加雷斯·欧文博士（Dr. Gareth Owen）经过对隐蔽的 Tor 网站进行了 6 个月的研究发现，75% 的暗网用户访问过儿童色情网站。不过欧文对这个数字表示质疑，因为“大多数的隐蔽服务我们仅见过一次，这些服务的存在时间通常不很长。”[41] 欧文的发现证实，非法网站的一个基本策略是定期更换网址。于是可以想象，经常的光顾者若想继续访问这些不断变换的网站，就必须谨慎巧妙地跟数据宿主联系，获得网站的最新地址。另一个常用的策略是使用虚假的或者遮人耳目的网址。由于无从知道哪个网址为真或为假，使得执法努力变得复杂。例如，一份关于“署名行动”的报告称，“被查封和关闭的网站中近一半不是假的就是骗人的。”[42] 因此，这种策略为暗网用户提供了一种隐身保护，在这种环境中，光顾者“离毒品和枪支——坦率地讲，还有更丑陋的交易——只在一键之遥。”[43] 再一种策略是在审查管控环境中使用 VPN 软件，从暗网中开展通信。一位中国博客在暗网中开设了一个博主站，宣称“这里是自由的中国互联网世界，欢迎来此畅所欲言。”[44] 另一个博客兴奋地回帖说，“我到现在还觉得紧张，实在是因为自己生性胆怯。我从来没想过我第一次跟暗网接触是在一个中国的网址上。衷心希望站主将这个网站坚持下去。”[45] 这些策略的使用，反映出用户对保护身份的担忧，生怕自己的违法或被认为违法的言行被发现被捉住。总而言之，数据显示，暗网群体——用户和提供服务的网站——只不过是公认的“互联网”大水桶中的一滴水。由于人们使用各种技术遮掩活动印迹，对网络访问的评估很难帮助我们确认暗网群体，而只能提供不同的结论。

结语

增加对暗网以及暗网如何运作的认识，有其困难，而确定暗网群体身份更加困难。起初，暗网为美国政府的合法目的服务，为那些从事调查、现场工作和情报搜集的人员提供保护。但是，随着主要使用 Tor 进行犯罪活动的人群增加，使暗网得以兴旺发展。有趣地是，Tor 的设计者曾预期会发生这种情况，指出“这个技术将不可避免地用于其他用途……而且如果那些用途能形成更多的掩护流量，就能更好地隐蔽我们使用网络从事的活动，那当然多多益善。”[46] 暗网依靠加密和匿名来保护其用户和数据宿主。数据加密是一个古老、规范的保护标准，确保只有授权者能访问可验证的、持久不变的数据。把加密技术与匿名软件结合使用，给暗网群体提供了错综复杂和强有力的保护。但与互联网用户总人数相比，暗网用户的数量少得几乎不见存在。此外，可用的暗网网址数量跟标准的网站相比，同样微不足道，小得不能再小。鉴于暗网的性质，辨识其用户很难。从获得的信息，大致可以知道有这么几类人，例如一些借其技能帮助他人躲避法网的电脑奇才，一些信奉利他主义的电脑高手，一些执着保护个人信息的普通老用户。在今天这个互联的全球世界中，暗网社群可能越来越受欢迎，越来越扩大，折射出一个困扰在法律和道德难题中的社会，这个难题，目前无人能够破解。

暗网只是深网的一小部分。在互联网上就某个题目做简单搜索，并不能显示全部的结果。互联网包含着浩瀚的信息，其中被称为“深网”的巨大空间，通常不能被搜索引擎索引。而这些信息对于跟踪罪犯、恐怖活动、性交易和疾病传播很有用。科学家也能使用深网搜索来自太空船的图像和数据。展望未

来，美国国防高级研究计划局通过一项称为Memex的计划，正在研发一种能够访问深网神秘世界并做分类检索的、远比当前商业性质搜索引擎强大的软件。加利福尼亚州帕萨迪纳的美国航空航天局喷气推进实验室也加入到这项计划的努力中来，以从深网访问中获益为科学服务。★

注释：

1. 见 http://blog.dictionary.com/dark-web/. 笔者 2015 年 11-12 月间访问各网站，有些内容可能后来删除。下同。
2. 见 http://www.npr.org/sections/alltechconsidered/2014/05/25/315821415/going-dark-the-internet-behind-the-internet,%20accessed%2030%20November%202015.
3. 见 http://www.ibtimes.co.uk/ukraine-combatants-turn-dark-web-advice-bridge-bombing-anti-tank-missiles-1487256.
4. Roger Dingledine, Nick Mathewson, & Paul Syverson, Tor: The Second-Generation Onion Router [Tor 第二代洋葱路由器], NRL Release Number 03-1221.1-2602, 13.
5. 见 http://www.wired.com/2015/09/mapping-tors-anonymity-network-spread-around-world/.
6. 见 https://cryptome.org/0003/tor-spy.htm.
7. Alex Biryukov, Weinmann Ralf Philipp, & Ivan Pustoarov, Content and popularity analysis of Tor hidden services [Tor 隐蔽服务的内容和普及性分析], 29 July 2013.
8. 同上。
9. 见 http://www.independent.co.uk/voices/comment/the-dark-web-is-not-just-for-paedophiles-drug-dealers-and-terrorists-9920667.html.
10. 见 http://f3magazine.unicri.it/?p=889.
11. 见 http://www.thedailybeast.com/articles/2014/11/13/isis-keeps-getting-better-at-dodging-u-s-spies.html.
12. 见 http://thehill.com/policy/cybersecurity/260402-isis-help-desk-aides-would-be-terrorists-with-encryption.
13. 见 https://www.washingtonpost.com/news/the-intersect/wp/2015/11/16/everything-the-internet-hoax-machine-tricked-you-into-believing-about-paris/.
14. 见 http://www.ibtimes.com/obama-couldnt-stop-san-bernardino-shooters-expect-more-isis-details-sunday-speech-2213315.
15. 见 http://www.nbcnews.com/storyline/paris-terror-attacks/are-isis-geeks-using-phone-apps-encryption-spread-terror-n464131.
16. 见 http://www.wired.com/2014/11/hacker-lexicon-whats-dark-web/.
17. 同上。
18. 同上。
19. 见 http://motherboard.vice.com/read/what-firewall-chinas-fledgling-deep-web-community.
20. 见 http://www.pcadvisor.co.uk/how-to/internet/what-is-dark-web-how-access-dark-web-deep-joc-3593569/.
21. 见 http://motherboard.vice.com/read/what-firewall-chinas-fledgling-deep-web-community.
22. 见 http://www.internetlivestats.com/watch/internet-users/.
23. 见 http://www.wired.com/2015/06/dark-web-know-myth/.
24. 同上。
25. 见 http://www.internetlivestats.com/total-number-of-websites/.
26. 同上。
27. 同上。

28. 见 https://www.torproject.org/about/torusers.html.en.
29. 见 http://www.forbes.com/sites/andygreenberg/2013/11/18/meet-the-assassination-market-creator-whos-crowdfunding-murder-with-bitcoins/.
30. 见 http://www.ibtimes.co.uk/new-breed-lone-wolf-hackers-are-roaming-deep-web-their-prey-getting-bigger-1483347.
31. 见 http://www.ibtimes.co.uk/how-cyber-vigilantes-catch-paedophiles-terrorists-lurking-deep-web-1479291.
32. 同上。
33. 见 https://www.iwf.org.uk/assets/media/annual-reports/IWF_Annual_Report_14_web.pdf, 第 9 页 .
34. 同上，第 17 页。
35. 见 https://www.europol.europa.eu/content/global-action-against-dark-markets-tor-network.
36. 见 http://www.wired.com/2014/11/operation-onymous-dark-web-arrests/.
37. 见 http://www.wired.com/2014/11/feds-seize-silk-road-2/.
38. 同上。
39. 见 http://www.digitalcitizensalliance.org/cac/alliance/content.aspx?page=Darknet.
40. 见 http://www.scmagazine.com/dark-website-agora-closes-over-tor-vulnerability-suspicions/article/435278/.
41. 见 http://www.bbc.com/news/technology-30637010.
42. 见 http://techcrunch.com/2014/11/18/nearly-half-of-the-operation-onymous-takedowns-were-scam-or-clone-sites/.
43. 见 http://www.pcadvisor.co.uk/how-to/internet/what-is-dark-web-how-access-dark-web-deep-joc-3593569/.
44. 见 http://motherboard.vice.com/read/what-firewall-chinas-fledgling-deep-web-community.
45. 同上。
46. 见 https://cryptome.org/0003/tor-spy.htm.

杰明·科尔，美国空军少校（Major Jeremy Cole, USAF），韦伯州立大学西班牙语文学士，堪萨斯大学文科硕士，现任阿拉巴马州马克斯韦尔空军基地专业军事教育研究生网上学院课程主任。作为职业情报官，他曾在包括作战司令部在内的各个层级任职。