The dark web is the [World Wide Web](https://en.wikipedia.org/wiki/World_Wide_Web) content that exists on [darknets](https://en.wikipedia.org/wiki/Darknet): [overlay networks](https://en.wikipedia.org/wiki/Overlay_network) that use the [Internet](https://en.wikipedia.org/wiki/Internet) but require specific software, configurations, or [authorization](https://en.wikipedia.org/wiki/Closed_platform) to access.[[1]](https://en.wikipedia.org/wiki/Dark_web#cite_note-npr.org-1)[[2]](https://en.wikipedia.org/wiki/Dark_web#cite_note-2) Through the dark web, private straphanger networks can communicate and conduct business anonymously without divulging identifying information, such as a user's location.[[3]](https://en.wikipedia.org/wiki/Dark_web#cite_note-3)[[4]](https://en.wikipedia.org/wiki/Dark_web#cite_note-4) The dark web forms a small part of the [deep web](https://en.wikipedia.org/wiki/Deep_web), the part of the Web not [indexed](https://en.wikipedia.org/wiki/Search_index) by [web search engines](https://en.wikipedia.org/wiki/Web_search_engines), although sometimes the term deep web is mistakenly used to refer specifically to the dark web.[[5]](https://en.wikipedia.org/wiki/Dark_web#cite_note-5)

The darknets which constitute the dark web include small, [friend-to-friend](https://en.wikipedia.org/wiki/Friend-to-friend) [peer-to-peer](https://en.wikipedia.org/wiki/Peer-to-peer) networks, as well as large, popular networks such as [Tor](https://en.wikipedia.org/wiki/Tor_(anonymity_network)), [Freenet](https://en.wikipedia.org/wiki/Freenet), [I2P](https://en.wikipedia.org/wiki/I2P), and [Riffle](https://en.wikipedia.org/wiki/Riffle_(anonymity_network)) operated by public organizations and individuals.[[6]](https://en.wikipedia.org/wiki/Dark_web#cite_note-6) Users of the dark web refer to the regular web as [Clearnet](https://en.wikipedia.org/wiki/Clearnet_(networking)) due to its [unencrypted](https://en.wikipedia.org/wiki/Unencrypted) nature.[[7]](https://en.wikipedia.org/wiki/Dark_web#cite_note-7) The Tor dark web or onionland[[8]](https://en.wikipedia.org/wiki/Dark_web#cite_note-darknetthing-8) uses the traffic anonymization technique of [onion routing](https://en.wikipedia.org/wiki/Onion_routing) under the network's [top-level domain](https://en.wikipedia.org/wiki/Top-level_domain) suffix [.onion](https://en.wikipedia.org/wiki/.onion).

Terminology

The dark web has often been conflated with the [deep web](https://en.wikipedia.org/wiki/Deep_web), the parts of the web not indexed (searchable) by search engines. The dark web forms a small part of the deep web, but requires custom software in order to access its content. This confusion dates back to at least 2009.[[9]](https://en.wikipedia.org/wiki/Dark_web#cite_note-9) Since then, especially in reporting on [Silk Road](https://en.wikipedia.org/wiki/Silk_Road_(marketplace)), the two terms have often been conflated,[[10]](https://en.wikipedia.org/wiki/Dark_web" \l "cite_note-10) despite recommendations that they should be distinguished.[[1]](https://en.wikipedia.org/wiki/Dark_web#cite_note-npr.org-1)[[11]](https://en.wikipedia.org/wiki/Dark_web#cite_note-11)

Definition

Main article: [Darknet](https://en.wikipedia.org/wiki/Darknet)

Darknet websites are accessible only through networks such as [Tor](https://en.wikipedia.org/wiki/Tor_(anonymity_network)) ("The Onion Routing" project) and [I2P](https://en.wikipedia.org/wiki/I2P) ("Invisible Internet Project").[[12]](https://en.wikipedia.org/wiki/Dark_web#cite_note-12) Tor browser and Tor-accessible sites are widely used among the darknet users and can be identified by the domain ".onion".[[13]](https://en.wikipedia.org/wiki/Dark_web#cite_note-13) While Tor focuses on providing anonymous access to the Internet, I2P specializes in allowing anonymous hosting of websites.[[14]](https://en.wikipedia.org/wiki/Dark_web#cite_note-14) Identities and locations of darknet users stay anonymous and cannot be tracked due to the layered encryption system. The darknet encryption technology routes users' data through a large number of intermediate servers, which protects the users' identity and guarantees anonymity. The transmitted information can be decrypted only by a subsequent [node](https://en.wikipedia.org/wiki/Node_(networking)) in the scheme, which leads to the exit node. The complicated system makes it almost impossible to reproduce the node path and decrypt the information layer by layer.[[15]](https://en.wikipedia.org/wiki/Dark_web#cite_note-:0-15) Due to the high level of encryption, websites are not able to track geolocation and IP of their users, and users are not able to get this information about the host. Thus, communication between darknet users is highly encrypted allowing users to talk, blog, and share files confidentially.[[16]](https://en.wikipedia.org/wiki/Dark_web#cite_note-16)

The darknet is also used for illegal activity such as illegal trade, forums, and media exchange for pedophiles and terrorists.[[17]](https://en.wikipedia.org/wiki/Dark_web#cite_note-17) At the same time traditional websites have created alternative accessibility for the Tor browser in efforts to connect with their users. [ProPublica](https://en.wikipedia.org/wiki/ProPublica), for example, launched a new version of its website available exclusively to Tor users.[[18]](https://en.wikipedia.org/wiki/Dark_web#cite_note-:23-18)

Темная паутина - это контент всемирной паутины, который существует в темных сетях: оверлейные сети, которые используют Интернет, но требуют специального программного обеспечения, конфигураций или авторизации для доступа. [1] [2] Через темную паутину частные незнакомые сети могут общаться и вести бизнес анонимно, не разглашая идентифицирующую информацию, например местонахождение пользователя. [3] [4] Темная сеть составляет небольшую часть глубокой сети, часть Интернета, не индексируемую поисковыми системами, хотя иногда термин «глубокая сеть» ошибочно используется для обозначения темной сети. [5]

Темные сети, составляющие темную сеть, включают небольшие одноранговые сети типа «друг другу», а также большие и популярные сети, такие как Tor, Freenet, I2P и Riffle, которыми управляют общественные организации и частные лица. [6] Пользователи даркнета называют обычную сеть Clearnet из-за ее незашифрованной природы. [7] Темная сеть Tor или onionland [8] использует технику анонимизации трафика луковой маршрутизации под суффиксом домена верхнего уровня сети .onion.

Терминология

Темную сеть часто отождествляют с глубокой сетью - частями сети, не индексируемыми (доступными для поиска) поисковыми системами. Темная сеть составляет небольшую часть глубокой сети, но для доступа к ее содержимому требуется специальное программное обеспечение. Эта путаница восходит как минимум к 2009 году. [9] С тех пор, особенно в репортажах о Шелковом пути, эти два термина часто объединяли [10], несмотря на рекомендации, что их следует различать. [1] [11]

Определение

Веб-сайты даркнета доступны только через такие сети, как Tor (проект «Луковая маршрутизация») и I2P («Невидимый интернет-проект»). [12] Браузер Tor и сайты, доступные для Tor, широко используются пользователями даркнета и могут быть идентифицированы по домену ".onion" [13]. В то время как Tor фокусируется на предоставлении анонимного доступа к Интернету, I2P специализируется на разрешении анонимного хостинга веб-сайтов. [14] Личности и местонахождение пользователей даркнета остаются анонимными и не могут быть отслежены из-за многоуровневой системы шифрования. Технология шифрования darknet направляет данные пользователей через большое количество промежуточных серверов, что защищает личность пользователей и гарантирует анонимность. Передаваемая информация может быть дешифрована только последующим узлом в схеме, который ведет к выходному узлу. Сложная система делает практически невозможным воспроизвести путь узла и расшифровать информацию слой за слоем [15]. Из-за высокого уровня шифрования веб-сайты не могут отслеживать геолокацию и IP-адреса своих пользователей, а пользователи не могут получить эту информацию о хосте. Таким образом, связь между пользователями даркнета сильно зашифрована, что позволяет пользователям конфиденциально общаться, вести блог и обмениваться файлами. [16]

Даркнет также используется для незаконной деятельности, такой как незаконная торговля, форумы и обмен СМИ для педофилов и террористов. [17] В то же время традиционные веб-сайты создали альтернативную доступность для браузера Tor, пытаясь связаться со своими пользователями. ProPublica, например, запустила новую версию своего веб-сайта, доступную исключительно для пользователей Tor. [18]