The Dark Web is a collection of thousands of websites that use anonymity tools like Tor and I2P to hide their IP address. While it's most famously been used for black market drug sales and even child pornography, the Dark Web also enables anonymous whistleblowing and protects users from surveillance and censorship.

**History of TOR-** The name TOR is derived from the acronym”The Onion Router”.It was developed in the mid-1990s by U.S Navy employees mathematician Paul syverson and the computer scientists Michael G. Reed and David Goldschlag, that enabled them to browse the internet anonymously.DARPA further developed it in 1997.

The alpha version of TOR,developed by Syverson and computer scientists Roger Dingledine and Nick Mathewson and then called the Onion Routing Project or TOR project,launched on 20 september 2002. In 2006 TOR has become a non profit organization and is heavily funded by the U.S Government.

With the rise and fall of the Silk Road—and then its rise again and [fall again](https://www.wired.com/2014/11/operation-onymous-dark-web-arrests/)—the last couple of years have cast new light on the Dark Web. But when a news organization as reputable as [60 Minutes describes the Dark Web](http://www.msn.com/en-au/video/watch/60-minutes-the-dark-web/vp-f9b6d9b5-f5ea-4836-8a65-d61f7b5d8239) as “a vast, secret, cyber underworld” that accounts for “90% of the Internet,” it’s time for a refresher.

The Dark Web isn’t particularly vast, it’s not 90% percent of the Internet, and it’s not even particularly secret. In fact, the Dark Web is a collection of websites that are publicly visible, yet hide the IP addresses of the servers that run them. That means anyone can visit a Dark Web site, but it can be very difficult to figure out where they’re hosted—or by whom.

The majority of Dark Web sites use the anonymity software Tor, though a smaller number also use a similar tool called I2P. Both of those systems encrypt web traffic in layers and bounce it through randomly-chosen computers around the world, each of which removes a single layer of encryption before passing the data on to its next hop in the network. In theory, that prevents any spy—even one who controls one of those computers in the encrypted chain—from matching the traffic’s origin with its destination.

When web users run Tor, for instance, any sites they visit can’t easily see their IP address. But a web site that itself runs Tor—what’s known as a Tor hidden service—can only be visited by Tor users. Traffic from both the user’s computer and the web server takes three hops to a randomly chosen meet-up point in the Tor network, like anonymous bagmen trading briefcases in a parking garage.

Just because the IP addresses of those sites are kept hidden, however, doesn’t mean they’re necessarily secret. Tor hidden services like the drug-selling sites Silk Road, Silk Road 2, Agora and Evolution have had hundreds of thousands of regular users; Anyone who runs Tor and knows a site’s url, which for Tor hidden services ends in ".onion," can easily visit those illegal online marketplaces.

Almost any type of illegal and legally questionable products and services can be found somewhere in the internet's underground.

One of the best examples is the [**Silk Road**](http://en.wikipedia.org/wiki/Silk_Road_(marketplace)), a now-defunct website that, for more than two years, operated as a kind of illicit eBay. The Silk Road was most famous for offering a wide variety of illegal drugs, but it offered other illicit products as well. You could buy fake IDs, pirated DVDs, fireworks, and stolen credit-card numbers.

The Silk Road website was a Tor hidden service, which made it difficult for the authorities to shut the site down. All transactions were conducted using [Bitcoin](http://www.vox.com/cards/bitcoin/what-is-bitcoin), meaning they couldn't be traced the way credit-card transactions can be. But eventually, law enforcement was able to identify the site's alleged operator, who was [**arrested**](http://www.washingtonpost.com/blogs/the-switch/wp/2013/10/02/feds-arrest-the-alleged-founder-of-bitcoins-largest-drug-market/) in 2013.

Almost immediately, copycat sites [**sprang up**](http://arstechnica.com/business/2013/11/just-a-month-after-shutdown-silk-road-2-0-emerges/). A successor site called Silk Road 2 was founded in 2013, but it was infiltrated by law enforcement and [**shut down**](http://arstechnica.com/tech-policy/2014/11/fbi-arrests-blake-defcon-benthall-alleged-operator-of-silk-road-2-0/) in 2014. Currently, one of the largest Silk Road successors is a site called Evolution. Ars Technica recently [**reported**](http://arstechnica.com/business/2014/12/after-two-silk-road-takedowns-dark-web-drug-sites-still-thriving/) that it had 26,000 product listings.

Even these sites had some lines they weren't willing to cross. For example, all three sites barred child pornography listings. But other dark web sites exist to help users find and distribute this kind of material. A recent study by computer scientist Gareth Owen suggested that sites related to child abuse and child pornography could account for as much as [**80 percent of traffic**](http://www.wired.com/2014/12/80-percent-dark-web-visits-relate-pedophilia-study-finds/) to Tor hidden services (though hidden services account for a small fraction of Tor traffic overall).

The government is unlikely to ever fully suppress the dark web for the same reason that law enforcement has never been able to eliminate conventional black markets: there's a lot of demand for the information and products offered on these sites, and there's always going to be someone willing to take the risks involved in meeting that demand.

And these sites can earn a lot of money. Silk Road 2, for example, reportedly [**earned $8 million**](http://arstechnica.com/tech-policy/2014/11/silk-road-2-0-infiltrated-from-the-start-sold-8m-per-month-in-drugs/) in a single month before it was shut down. That kind of money will always attract copycats who believe they can succeed where their predecessors had failed.

Moreover, the government probably can't — and shouldn't — shut down the underlying technologies that make the dark web possible. Tor provides crucial protection to dissidents and whistleblowers around the world. Bitcoin has the potential to [**produce significant innovations**](http://www.vox.com/2014/3/31/5557170/bitcoin-bad-currency-good-network) in the payments business. And shutting down these technologies won't stop people from using the internet for illicit purposes. Most likely, these activities will simply shift overseas, where they will be even harder for American authorities to police.

**Related links-**

<https://www.wired.com/2014/11/hacker-lexicon-whats-dark-web/>

<https://en.wikipedia.org/wiki/Dark_web>

https://www.vox.com/2014/12/31/7470965/dark-web- explained

<https://www.hackersdenabi.net/deep-web-and-dark-web/>