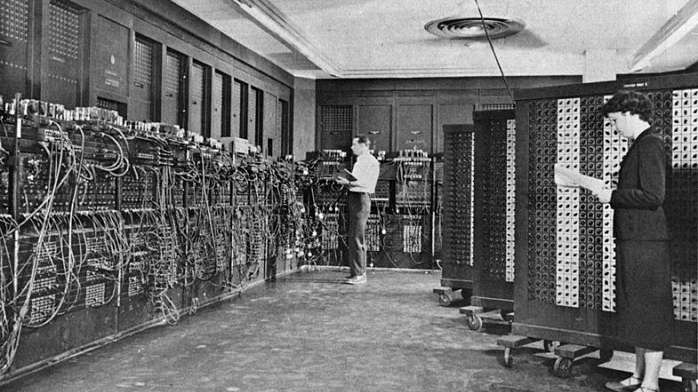
Dark Web History: Where Did It Come From?

The Deep Web and it’s Dark Web subset have been in the public eye more than usual in the past few years. Once the things that happen on the hidden part began having an impact on the “real” world, regular Joes and Janes started to take an interest. That doesn’t mean the hidden part of the internet is a recent development. It’s just about as old as the internet itself!

## **The Early Days**



The history of the hidden web is almost as old as the history of the internet itself. Obviously, the same technology that made the internet and the web possible, also makes the Dark Web possible thanks to its architecture and designs. Which is why it is fair to pin the start of the Dark Web to ARPANET. Which is the direct precursor to the internet of today? While ARPANET may not have had a Dark Web as we know it now from the start, it wouldn’t take long before people started to make use of this technology for things they wanted to keep a secret. It turns out that the first ever online sale happened in the early 70s and was in fact cannabis. Students at Stanford [sold weed](https://www.theguardian.com/science/2013/apr/19/online-high-net-drugs-deal) to students at MIT, using ARPANET. Remember that at this point most people didn’t have personal computers, much less home internet access.

## **The 1980s**



In the 1980s, access to the internet for normal citizens is still a dream. This was the decade when everything needed for a worldwide web would fall into place. In the early 80s, the TCP/IP standard is solidified. By the mid- 80s personal computers and modems are, if not affordable, at least available for anyone to buy. Internet pioneers also invented the domain name system we use to resolve website names during this decade.

[*Data havens*](https://arstechnica.com/tech-policy/2012/03/sealand-and-havenco/) emerge as an idea at this time as well. Since the world was going global, worries about where data should be stored came to the fore. Storing your data in a haven meant sending it out of the country to a territory that had better legal protection against government spying. At the extreme, data havens would be in no country at all. They would be built on structures or vessels out in international waters. A similar idea to [seasteading](https://en.wikipedia.org/wiki/Seasteading" \t "_blank). Actual data havens in the 80s popped up in the Caribbean islands.

## **The 1990s**



The 1990s are without a doubt the time when the World Wide Web went mainstream. Thanks to web technologies like HTTP and FTP along with graphical computers capable of running a web browser, there was a sudden mainstream appeal to this whole internet thing.

Towards the end of the 1990s, there was a real leap in the technologies that allowed large amounts of data, such as multimedia, to be shared online. MP3 technology in particular lead to a massive shakeup of the music industry. Thanks to like the likes of Napster, people could perform illegal peer-to-peer exchanges of ripped and compressed music. This caused a complete meltdown among musicians and music executives. Lars Ulrich famously [sued Napster](http://loudwire.com/metallica-lars-ulrich-we-could-have-educated-ourselves-better-about-napster/) which was really symbolic of the battle between old and new school. Today the music industry has adapted and streaming subscriptions are the norm. Without Dark Web alike peer-to-peer exchanges it’s doubtful we’d have the consumer-friendly online media world of today.

## **The 2000s**



The Dark Web proper really got its start in March of 2000 with the release of [Freenet](https://freenetproject.org/author/freenet-project-inc.html). The service still exists today and provides a censorship-resistant way to use the web. It is a true implementation of the Dark Web and provided a way for plenty of illegal information to pass around. This included illegal pornographic material and pirated content. Of course, actually exchanging money anonymously is still incredibly hard at this point, since you have to use cash. So Freenet doesn’t lead to any black market activity to any significant degree.

A data haven called [HavenCo](https://en.wikipedia.org/wiki/HavenCo" \t "_blank) was established in [Sealand](https://www.sealandgov.org/" \t "_blank) (a seasteading micronation) which promised to store sensitive information in a place where no government could stick its nose. It seemed like a Dark Web dream, but by the early 2010s HavenCo was dead, dead, dead.

The most important Dark Web development of all time happened in 2002, with the release of [TOR](https://www.torproject.org/) or The Onion Router. It was created by non-other than the US government, as a way to help their own operatives remain untraceable. It’s no exaggeration to say that the Dark Web of today could not exist without this technology.

Late in the 2000s came the advent of cryptocurrency in the form of [Bitcoin](https://www.forbes.com/sites/bernardmarr/2017/12/06/a-short-history-of-bitcoin-and-crypto-currency-everyone-should-read/#557663f53f27). The final piece of the puzzle needed to make the Dark Web really click.

## **The 2010s**



The 2010s represent the era where cryptocurrency and TOR met to create the first proper black markets. The pioneer was the [Silk Road, which is now long defunct](https://www.wired.com/2015/12/the-untold-story-of-silk-roads-rise-and-fall/). Despite taking all the important figures out behind the Silk Road, it has seemingly done little to stop the trade of drugs and other illegal goods and services over the Dark Web.

This is the era in which the Dark Web becomes a topic of public concern, rather than just something discussed as cyber security conferences. Many mainstream articles emerge that explain the difference between the massive [Deep Web](https://www.technadu.com/deep-web-vs-dark-web/9480/) and the relatively tiny Dark Web.

It becomes especially scary when it emerges that [terrorists are using the Dark Web](https://www.usatoday.com/story/tech/news/2017/03/27/terrorists-use-dark-web-hide-london-whatsapp-encryption/99698672/) to communicate and coordinate. Ironic, given what the US created TOR for originally. [Research published](https://www.tandfonline.com/doi/full/10.1080/00396338.2016.1142085?scroll=top&needAccess=true&) showing that the Dark Web is mainly being used to commit crimes.

## **Today**



The Dark Web of today is reportedly in decline. Despite this, there is an incredible variety of hidden services and significant information exchange happening out of sight of the mainstream web. It doesn’t really matter that the Dark Web is relatively small compared to the surface web as a whole. Its impact is disproportionately large. Small groups of hackers collaborating on the Dark Web can bring a multi-billion Dollar internet company to its knees. Hackers end up impacting millions of users.

Darknet black markets are also thriving and putting both traditional and new synthetic drugs into the hands of anyone who wants them. Cryptocurrency has been the biggest factor in this maturation of the Dark Web.

## **What the Future Holds**

The technologies and methods that underpin the Dark Web are incredibly sophisticated. While most governments would prefer that something like the Dark Web didn’t exist, they themselves need technologies like encryption and onion routing for their own purposes. As long as powerful anonymization technologies exist and are effective, there will be some sort of Dark Web.

Whether the commercial, black market side of the hidden web has any future is a different question. While I have no doubt that Dark Web information exchanges will always be there, the future of black markets isn’t that clear. It all hinges on cryptocurrency technology and whether it can be made anonymous in a secure way. While Bitcoin was at first thought to be untraceable, the authorities have figured out a few tricks to link specific transactions back to buyers. One stopgap has been Bitcoin tumblers. However, entirely new privacy-focused currencies such as Monero is the medium term solution.

Who will eventually win this arms race remains to be seen. There’s little doubt that there will always be some sort of dark and hidden corner on the internet.

-----------------------------------------------------------------------------------

## What is the dark web?

The internet is actually made up of three different layers: the surface web, the deep web and the dark web.

The top layer, the surface web, are web pages that show up using search engines such as Google - like The Sun website that you're looking at right now.

The deep web are web pages which search engines can't access and are therefore hidden, accessed via passwords and authorisation.

Any time you log into an account you're accessing deep web content that won't show up on a search engine.

[](https://www.thesun.co.uk/tech/2054243/dark-web-kidnap-chloe-ayling-encrypted-network-black-death/)

6

Users of the dark web access websites using special browsers and softwareCredit: Getty Images

For example, work intranets, password-protected areas of online banking and draft blog posts are all stored on the deep web.

This means that if someone was to Google your name, your banking information or Amazon wishlist won't show up in the results.

The dark web is a network of untraceable online activity and websites on the internet. They cannot be found using search engines and to access them you need to use specific software, configurations or have authorisation. They are used by lots of different people to keep their web activity hidden.

## Where did the dark web come from?

The dark web was actually created by the US government to allow spies to exchange information completely anonymously.

US military researchers developed the technology, known as Tor (The Onion Router) in the mid-1990s and released it into the public domain for everyone to use.

The reason was so that they could stay anonymous - it would be harder to distinguish the government's messages between spies if thousands of other people were using the same system for lots of different things. Tor now hosts roughly 30,000 hidden sites.

It's called The Onion Router because it uses the technique of onion routing - making websites anonymous through layers of encryption. Most websites are also hosted on the .onion domain.

## What is the government doing about the dark web?

On April 11, Home Secretary Amber Rudd launched a multi-million pound cyber blitz on criminals selling guns on the dark web.

She announced a £9million fund to ensure every police force in the UK has a dedicated cyber crime unit to bust its "sickening shopping list of services and products".

The extra cash will tackle offenders who are exploiting the anonymity of the dark web - where users use freely available software to avoid being tracked - to trade in guns, drugs and child abuse images.

This anonymity has attracted criminals seeking to avoid detection by law enforcement agencies.

## How does the dark web work?

The best explanation so far has been published by Daniel Prince, Associate Director Security at Lancaster University, on [The Conversation](https://theconversation.com/what-is-the-dark-web-and-how-does-it-work-63613).

Mr Prince says: "So just for a minute imagine that the whole internet is a forest – a vast expanse of luscious green as far as the eye can see. And in the forest are well-worn paths – to get from A to B.

"Think of these paths as popular search engines – like Google – allowing you as the user the option to essentially see the wood from the trees and be connected. But away from these paths – and away from Google – the trees of the forest mask your vision.

"Off the paths it is almost impossible to find anything – unless you know what you’re looking for – so it feels a bit like a treasure hunt. Because really the only way to find anything in this vast forest is to be told where to look.

"This is how the dark web works – and it is essentially the name given to all the hidden places on the internet.

"Just like the forest, the dark web hides things well – it hides actions and it hides identities. The dark web also prevents people from knowing who you are, what you are doing and where you are doing it."

[](https://www.thesun.co.uk/tech/2054243/dark-web-kidnap-chloe-ayling-encrypted-network-black-death/)

6

One of the criminal uses of the dark web is to buy and sell drugsCredit: PA:Press Association

## Who uses the dark web and why?

The dark web is used by all sorts of people for all sorts of reasons  - but it's not surprising that it's [used for illegal activity](https://www.thesun.co.uk/news/1851874/hidden-internet-allows-would-be-jihadists-to-buy-fake-passports-and-even-assault-rifles/).

A study by the University of Portsmouth in 2014 found that the most wanted type of content on Tor was child porn, followed by black markets for goods such as drugs, [personal details](https://www.thesun.co.uk/news/1503297/criminals-are-selling-british-o2-customers-online-identities-on-the-dark-web/) and even guns.

This type of site is regularly busted by police, who compromise them by distributing viruses and malware to users.

The dark web is also used for hiding online activity related to finance, extremism, arms, [hacking](https://www.thesun.co.uk/news/2002311/inside-twitters-dark-markets-where-punters-sell-hacked-sky-accounts-and-put-bounties-on-users/), abuse and fraud.

However, for others the dark web has positive uses. For example, it can be used to avoid a national firewall, such as China, where users are normally blocked from accessing hidden sites.

It can also be used as a tool for whistleblowing - infamous website WikiLeaks is hosted on the dark web, allowing whistleblowers to anonymously upload classified information to the press.

## Do police ever catch people using the dark web?

Yes - although using the dark web makes it easier to evade detection but governments around the world are working to index, sort and catalogue the dark web as well as monitor it as much as they can.

The UK government have a dedicated cybercrime unit to tackle the dark web with a focus on taking down serious crime rings and child porn.

Just earlier this year police caught Richard Huckle['Britain's worst-ever paedophile'](https://www.thesun.co.uk/news/1229829/monster-who-raped-kids-as-young-as-3-volunteered-in-orphanages-and-awarded-himself-points-offences/) by secretly taking over a dark web site dedicated to child abuse.

[](https://www.thesun.co.uk/tech/2054243/dark-web-kidnap-chloe-ayling-encrypted-network-black-death/)

6

Richard Huckle was handed 22 life sentences after pleading guilty to 71 child sex offencesCredit: Getty Images

The online network was made up of over 45,000 people who [swapped sickening videos and images](https://www.thesun.co.uk/news/1232944/britains-worst-paedo-to-be-sentenced-for-horrific-string-of-crimes-we-may-never-know-full-scale-of/) of children on a dark-web forum which was only accessible through a specially encrypted browser.

Another take-down, called Operation Onymous, revealed over 400 "hidden services" in an effort by seventeen different countries co-ordinated by Europol and the FBI.

The operation led to hundreds of pounds worth of Bitcoin being seized and 17 arrests - but only one person was identified and taken into custody.

## What was the Chloe Ayling case?

[Chloe Ayling](https://www.thesun.co.uk/news/4186202/chloe-ayling-british-model-kidnapped-black-death-group-milan/) is a 20-year-old British model who was [kidnapped by a notorious sex trafficking gang](https://www.thesun.co.uk/news/4193233/british-model-chloe-ayling-shared-bed-with-sex-slave-cult-kidnapper/) known as the 'Black Death Group' after being lured to Milan.

The mother-of-one was held captive for six days in a remote Italian farmhouse after being led to Milan by fake promises of a photoshoot.

She was drugged and stuffed inside a bag before being auctioned on the dark web.

The [Black Death Group](https://www.thesun.co.uk/news/4182188/black-death-group-chloe-ayling-kidnap-britsh-model-sex-slave/) is a shadowy online group which has been linked to multiple instances of kidnapping and people trafficking.

Notorious on sections of the internet, it is claimed users of the dark web pay to buy women who have been abducted across Europe.

6

Mum Chloe Ayling, 20, was driven to a remote farmhouse and held captive for six days after being abducted by masked men

## Who is Ross Ulbricht?

Ross Ulbricht was the man behind Silk Road, the internet's biggest market for illegal drugs - which was hosted on the dark web.

Silk Road was reportedly worth $34.5m and had nearly one million anonymous customers. On Silk Road you could buy drugs, services (such as hacking into Facebook accounts), pirated content, fake passports and more. You could even check the reviews and star ratings of each dealer left by other customers.

[](https://www.thesun.co.uk/tech/2054243/dark-web-kidnap-chloe-ayling-encrypted-network-black-death/)

6

Ulbricht is in prison in New York after he was unmasked as the man behind dark web drugs emporium Silk RoadCredit: Reuters

### **MOST READ IN TECH**

[](https://www.thesun.co.uk/tech/11487415/xbox-ps4-nintendo-switch-bundles-cheap-cheapest-price-free-games/)

HOT DEALS

### GAME WINNER

Cheapest Xbox, PS4 and Nintendo Switch bundles you can still buy online

[](https://www.thesun.co.uk/tech/11518595/nintendo-switch-online-free-trial-games-snes-nes/)

### SWITCHED ON

Nintendo is giving away a FREE week of Switch Online – plus over 70 retro games

[](https://www.thesun.co.uk/tech/11519202/how-to-spot-swan-comet-what-time/)

### SPACE TAIL

How to spot 'best comet in YEARS' soaring over Earth for the next month

[](https://www.thesun.co.uk/tech/11495755/popular-google-doodle-games/)

### GOOGLE GAMES

Popular Google Doodle games - from Pac-Man to interactive Rubik's Cube

[](https://www.thesun.co.uk/tech/11506604/xbox-games-with-gold-may-2020-free-download-warhammer-racing/)

HOT DEALS

### PLAY DATE

Xbox owners can get four FREE games this week – including Warhammer 40,000

[](https://www.thesun.co.uk/tech/11509932/iphone-se-voucher-code-ee-save/)

HOT DEALS

### EAS-SE DEAL

iPhone SE voucher code gets you 16GB data, for £28 a month and NOTHING upfront

Ulbricht was caught by the FBI in 2013, who shut down Silk Road and convicted him of money laundering, computer hacking, conspiracy to traffic fraudulent identity documents and conspiracy to traffic narcotics in February 2015.

He was sentenced to life in prison. Ulbricht will also be tried for procuring murder.

FBI indictments claimed he ordered hitmen to kill people he thought would expose the identity of his clients.

But investigators believe none of the six hits took place.